Response to Call for Evidence –

Select Committee on Democracy and Digital Technologies

Data collection by private companies: a threat to human rights? Rights to Privacy (Article 8) and the Digital Revolution

Written evidence submitted by Prof. Derek McAuley, Dr. Ansgar Koene and Dr. Jiahong Chen of the Horizon Digital Economy Research Institute, University of Nottingham.

20 September 2019.

1. Horizon[1] is a Research Institute at The University of Nottingham and a Research Hub within the UKRI Digital Economy programme[2]. Horizon brings together researchers from a broad range of disciplines to investigate the opportunities and challenges arising from the increased use of digital technology in our everyday lives. Prof. McAuley is Director of Horizon and was principal investigator on the ESRC funded CaSMa[3] (Citizen-centric approaches to Social Media analysis) project to promote ways for individuals to control their data and online privacy, and the EPSRC funded UnBias[4] (Emancipating Users Against Algorithmic Biases for a Trusted Digital Economy) project for raising user awareness and agency when using algorithmic services. Dr Koene was a lead researcher of the CaSMa and UnBias projects, is Research co-Investigator on the EPSRC funded ReEnTrust[5] (Rebuilding and Enhancing Trust in Algorithms) project and chairs the working group for developing the IEEE P7003 Standard for Algorithm Bias Considerations. Dr Jiahong Chen is a Researcher Fellow of Horizon, with his completed doctoral research focusing on the legal and societal implications of online advertising.

Questions

General

1. How has digital technology changed the way that democracy works in the UK and has this been a net positive or negative effect?

2. The implications of digital technologies on democracy in the UK are multi-dimensional. On the one hand, the popularity of online services and platforms has enabled the government, political parties, individual politicians, and civil society organisations to reach out to the general public in highly effective manners. These include the use of online government portals, electronic archives, social media channels and direct communications. On the other hand, the press, watchdogs, and rights groups have gained better access to information whereby public bodies can be subject to closer oversight and greater transparency. Members of the public are also empowered to engage in public debates more easily, and can even hold public officials accountable by means of "citizen journalism" on social media.
3. However, digital technologies have also posed unprecedented challenges to the discourse of

[1] http://www.horizon.ac.uk
[2] https://epsrc.ukri.org/research/ourportfolio/themes/digitaleconomy/
[3] http://casma.wp.horizon.ac.uk
[4] http://unbias.wp.horizon.ac.uk
[5] https://ReEnTrust.org

democracy. As further explained in the responses below, new forms of communications may be exploited to undermine the functioning of democracy, notably hampering public debates, manipulating voters, and creating cyber-polarisation. While it is hard to measure the net effect of digital technologies, appropriate regulatory efforts can minimise the potential harms of such technologies.

2. How have the design of algorithms used by social media platforms shaped democratic debate? To what extent should there be greater accountability for the design of these algorithms?

4. The design of algorithms used by social media platforms has, at least until recently, not been guided by any direct considerations regarding democratic debate. The primary guiding principle has been to increase the competitive market share of the platforms as measured in size of user-base, time spent on the platforms, number of interactions ("likes", "shares", "ad-clicks" etc). In order to achieve competitive advantage, the algorithms have been built to play on same basic human behavioural and emotional triggers that tabloid journalism and political propaganda have traditionally prayed on, sensationalism, outrage, and strong emotions. An unintended by-product of this development has been an increased visibility in confrontational media content focusing on polarisation of democratic debate.
5. In the absence of laws or regulations governing the quality or tone of online discourse, platforms have tended to want to protect the neutrality of their own political position, to avoid alienating any part of their potential user base, by appealing to crowd based mechanisms (e.g. user driven "like" counts) for identifying which content to promote. As is well know from many studies of crowd behaviour however, nobody is morally responsible or accountable for the behaviour of a crowd.
6. In order to mitigate against unacceptable behaviour on online platforms it is vital to establish clear lines of accountability that cannot vanish in the crowd. Since the platform provider is the only party with the capacity to know what is happening on the platform, accountability must lie with the platform provider.

Education

3. What role should every stage of education play in helping to create a healthy, active, digitally literate democracy?

7. Helping to create a healthy, active democracy is a core function of the educational system that should include every stage of education and must go beyond the focus on digital literacy. The focus of concerns about mis-information and dis-information is on digital platforms because digital is the main conduit through which information is disseminated. Fundamental skills of critical analysis and distinguishing serious democratic debate from populist crowd baiting, however are not specific to the medium through which the information is carried. Digital literacy can help educate people to understand the process that channelled certain information to them. Being able to engage in a healthy democratic discussion, to listen to opposing points of view and evaluate the positions based on their merits, however requires an education focusing on human social dynamics, not technology.

Online campaigning

4. Would greater transparency in the online spending and campaigning of political groups improve the electoral process in the UK by ensuring accountability, and if so what should this transparency look like?

8. Greater transparency on online campaigning by political groups would help address some of the threats to democracy in the UK. To effectively hold political campaigns to account, however, future

regulation should not only focus on spending, but also the use of targeting technologies and personal data of the electorate. In fact, restrictions on the use of personal data – including data revealing one's political opinions – are already in place under data protection law.[6] Policymakers should further investigate how data protection principles should apply to political campaigning. For example, further legislation may be introduced to empower electoral regulators to issue a code of practice to define what constitutes a legitimate interest by campaign groups (and is thus permissible even without securing individual consent) and what constitutes unfair practices (and is thus prohibited regardless of individual consent).

9. An effective regime designed to enhance transparency in online political campaigning should cover at least the following areas: (1) a requirement of a detailed statement on the political group's spend on different online platforms and the marketing methods employed; (2) a compulsory, publicly accessible archive of any online political advertisements and direct-marking messages to internet users and the criteria of targeting; (3) a platform-specific – or ideally, cross-platform – portal to allow internet users to review when and how they have been targeted with political messages and by which political groups.

5. What effect does online targeted advertising have on the political process, and what effects could it have in the future? Should there be additional regulation of political advertising?

10. Online targeted advertising may exhibit its negative effects on the political process at least in the following three ways:

11. First, it may create chilling effects on internet users who are conscious of online tracking enabled by online advertising practices, and thus subject to "self-censorship" when expressing their opinions online.[7]

12. Second, political campaigners may gain unfair advantages through opaque targeting practices, which can be highly powerful yet hard to trace.[8] This may include using protected characteristics to identify and influence susceptible groups or disseminating false claims about opposition groups that are hard to noticed and corrected by the latter.

13. Third, targeted advertising may also deepen social division by generating "filter bubbles" that polarise voters. There is a substantial risk that voters may be exposed to political messages from limited sources and thus lose sight of the full landscape of the political discourse.[9]

Privacy and anonymity

6. To what extent does increasing use of encrypted messaging and private groups present a challenge to the democratic process?

14. Encrypted messaging and private groups are sometimes considered to have facilitated the dissemination of harmful content and mis-/disinformation by making such abuses more difficult to regulate. However, strong encryption also plays an important role in improving confidentiality of communications and has a positive impact on user trust, which forms an important part of the foundation of a democratic society.[10]

---

[6] See DPA 2018, sec 10; sch 1, para 22; GDPR, art 9(1).

[7] For empirical evidence, see https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092

[8] Cambridge Analytica, for example, has been accused of unduly influencing voters in the UK's Brexit Referendum. See https://www.bbc.co.uk/news/uk-politics-43558876

[9] See, for example, http://www.europarl.europa.eu/RegData/etudes/STUD/2019/634414/EPRS_STU(2019)634414_EN.pdf; https://www.theverge.com/2017/10/11/16449976/facebook-political-ads-trump-russia-election-news-feed; https://greatergood.berkeley.edu/article/item/is_social_media_driving_political_polarization

[10] https://www.computerweekly.com/news/252469043/Security-pros-reiterate-warning-against-encryption-backdoors

15. Private groups (like WhatsApp), that are not already politically homogenous, tend to have a more discourse-oriented character compared to the more information-dissemination focused character of open platforms (like Twitter). The quality of debate on private group platforms therefore depends on the general (technology-independent) capacity towards democratic discourse. The use of encrypted messaging and private groups by political groups tends to focus on organising of their followers. Political campaigning is not directly done on these platforms.
16. In most widely available end-to-end encrypted systems, the platform provider also supplies the app that decrypts the data and presents it to the user. It is often overlooked, yet entirely reasonable, that such apps could be implementing some of controls mandated on "the platform" after the data has been decrypted, and in a manner that limits the privacy impact.

7. What are the positive or negative effects of anonymity on online democratic discourse?

17. Online anonymity has the positive effect of encouraging individual participation in the public discussion in the online forum, potentially facilitating public engagement in a democratic process. However, anonymity also means lower costs for publishing inappropriate, manipulative, offensive or even illegal content, and higher costs for enforcement against such behaviour.[11]
18. Despite the potential downsides of maintaining full anonymity online, policymakers should take additional caution when considering any "real-name" policy or the like. Such an approach may present significant threats to confidentiality of electronic communications, and create substantial chilling effects to the use of online services.[12] Bad-actors are likely to circumvent the "real-name" policy with false identities, whereas the "real-name" policy could potentially expose vulnerable groups to harmful retaliation if they speak out against certain groups.

Democratic debate

8. To what extent does social media negatively shape public debate, either through encouraging polarisation or through abuse deterring individuals from engaging in public life?

19. See response to Q2.

9. To what extent do you think that there are those who are using social media to attempt to undermine trust in the democratic process and in democratic institutions; and what might be the best ways to combat this and strengthen faith in democracy?

20. See work by Carole Cadwalladr, extensively published in *The Observer* and *The Guardian* for evidence regarding the use of social media to attempt to undermine trust in the democratic process.

    The best ways to combat this and strengthen faith in democracy are for actual politicians and serious journalists to refrain from engaging in the same disingenuous activities.

Misinformation

10. What might be the best ways of reducing the effects of misinformation on social media platforms?

21. See response to Q3.

[11] https://www.bbc.com/worklife/article/20150309-the-danger-of-online-anonymity
[12] https://www.theguardian.com/commentisfree/2015/jun/03/facebook-real-name-policy-hurts-people-creates-new-digital-divide

Moderation

11. How could the moderation processes of large technology companies be improved to better tackle abuse and misinformation, as well as helping public debate flourish?

22. No response.

Technology and democratic engagement

12. How could the Government better support the positive work of civil society organisations using technology to facilitate engagement with democratic processes?

23. Government departments could support civil society organisations by further streamlining and accelerating the response process to freedom of information requests and provide access to (public) government data in standardised and compatible formats.

13. How can elected representatives use technology to engage with the public in local and national decision making? What can Parliament and Government do to better use technology to support democratic engagement and ensure the efficacy of the democratic process?

24. No platform provides a representative sample of the population (for example, few privacy advocates will be found on Facebook), and care should be taken in extrapolating policy from such biased statistical samples. The introduction of any technological engagement means must be accompanied by a suitable impact assessment to ensure inclusivity, and that it does not systematically favour some demographic groups over others. Much evidence has previously been received on this topic in the previous 2014 Select Committee inquiry into "Social media data and real time analytics".[13]

14. What positive examples are there of technology being used to enhance democracy?

25. Audrey Tang's work as Digital Minister in Taiwan has introduced a series of technological innovations to increase citizen engagement with government, including direct citizen stakeholder engagement in shaping the policy that affects particular population groups.[14]

[13] https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/news/report-responsible-use-of-data/

[14] See https://en.wikipedia.org/wiki/G0v; https://apolitical.co/solution_article/reprogramming-power-audrey-tang-is-bringing-hacker-culture-to-the-state/