Dr Felipe Romero-Moreno – written evidence (DAD0059)

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?**

1.1 The democratization of information and the way in which user data is weaponized by social media platforms, has permitted hostile players to exert excessive power over the public interest.[1] If this is not tackled, there is an actual threat of cross-contamination among all sources, with public confidence and trust in society decreasing further, whatever the news source or its dissemination platform. As the situation worsens, simple allegations will hamper the accuracy of facts that are real.[2] Indeed, the UK government regards this problem as 'fourth generation espionage'.[3]

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?**

2.1 In 2017 in the US over 125 million people were specifically targeted using 'divisive' information such as, ads and messages coming from cloned accounts.[4] In 2018 the Facebook-Cambridge Analytica scandal also revealed unlawful access to, and data use, from 50 million Facebook profiles, affecting both the US presidential election and the Brexit referendum.[5] In terms of accountability, individual States should ensure that human rights are essential to corporate design, use and adoption of algorithms, requiring companies to conduct impact assessments and AI audits, as well as guaranteeing adequate external accountability processes.[6]

Education

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

3.1 Algorithm transparency does not have to be complex, since even refined accounts of policies, reasons, outputs and inputs of AI can contribute to efforts in the increase public of education and debate, through technology at every stage. Rather than struggling with the onerous task of making convoluted algorithmic systems comprehensible to the public, corporations should attempt

[1] https://perma.cc/7FVT-3PFL see page 34.
[2] https://perma.cc/KQM7-JMFF
[3] https://perma.cc/9GUH-C2VC
[4] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf see page 9.
[5] See for example https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf; https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf
[6] https://undocs.org/A/73/348 see page 21.

to promote transparency without demanding technical skills in AI procedures. Thus, the focus should be upon educating users about an AI's rationale, nature, presence and effect, instead of scrutinizing the training data, source code, outputs and inputs.[7] Moreover, aggregate data showing trends in the display of information should also be accessible for users to examine, along with case studies, which exemplify why specific information is displayed first in favour of other information, and education on political profiling. Additionally, companies should also ensure that users are wholly informed about how AI decision-making can affect them, for instance, through education campaigns, just-in-time notices, and other ways to signal whether AI technology is shaping an individual's enjoyment of a site, service or platform.[8]

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?

4.1 Reports handed in by political groups specifying their campaign spending and electoral authorities' investigations, could offer vital information to the data protection authorities, concerning political campaigns data gathering and processing practices. Notably, this might also feed into the compatibility assessment with the GDPR, including transparency, accountability, legality and fairness of data processing. Thus, all State authorities and regulators involved must understand to what extent political groups carry out user targeting and profiling, what sources of personal data are utilized, and what profiling and targeting techniques are deployed.[9]

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?

5.1 Of significant concern is the fact that technology such as, Deep Packet Inspection (DPI), which is essential for micro-targeted advertising, also enables the *modification of internet content* as it passes through the network. Yet, while packet modification has been used for behavioural advertising,[10] worryingly, in the future, this DPI feature could also result in a political party's or contender's website, manipulating its content according to the established user political leanings.[11] Thus, part of the solution to the manipulation problem is to properly enforce existing GDPR provisions along with rules for media pluralism and elections.[12]

---

[7] https://www.omidyar.com/sites/default/files/file_archive/Public%20Scrutiny%20of%20Automated%20Decisions.pdf
[8] https://undocs.org/A/73/348 see pages 19, 22.
[9] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf see pages 19, 20.
[10] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2621410 see pages 9, 10.
[11] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf see page 11.
[12] *Ibid* at page 22.

Privacy and anonymity

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

6.1. In recent years, user privacy and anonymity are playing an increasingly important role in preserving democracy, and encrypted communication apps such as WhatsApp, Telegram or Signal, alongside private groups like Chatcrypt,[13] are just one of the techniques users can rely upon to better safeguard not only their personal data, but also themselves.[14] As Google explains, HTTPS connections protect against man-in-the-middle attacks, snoopers and criminals who try to deceive a trusted site. End-to-end encryption specifically prevents interception of user data and protects the integrity of content, which is communicated and received.[15]

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

7.1 On the one hand, anonymity and encryption, which are fundamental aspects of security, offer everyone a mechanism for safeguarding their privacy, enabling them to search, learn, develop and exchange views and content without restricting the right to freedom of expression. Intelligence services and law enforcement authorities, on the other, frequently claim that encrypted or anonymous information exchange make it hard to scrutinize drug dealing, economic crimes, terrorism and child sexual abuse. Moreover, individuals also raise valid concerns regarding how offenders and bullies deploy modern technology to carry out harassment.[16]

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?

8.1 The problem of utilizing personal data and content to manipulate politics and individuals, obviously surpasses users' right to privacy and protection of their personal data. An individualized, microtargeted digital domain generates 'filter-bubbles' in which individuals are subject to 'more-of-the-same' like-minded content and come across less viewpoints, leading to expanded ideological and political polarisation.[17] This in turn intensifies the prevalence and power of fabricated news and conspiracy theories.[18] Moreover, importantly, there is also

[13] https://www.chatcrypt.com/
[14] https://www.techradar.com/best/best-encrypted-messaging-app-android
[15] https://transparencyreport.google.com/https/overview?hl=en
[16] https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx see page 3.
[17] See for instance https://www.economist.com/printedition/2017-11-04 at pages 21-24.

evidence that the manipulation of users' search results and newsfeeds can determine their voting decision.[19]

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?

9.1 Please refer to general questions above and the misinformation question below.

Misinformation

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

10.1 Using the example of Google as a case study, the search engine recently made global ranking updates to better identify original reporting, showing it more clearly in searches and guaranteeing that it remains there longer. While users interested in the most recent stories can locate the news, which initiated it all, publishers can also take advantage of having their original reporting more broadly viewed. It is therefore arguable that providing everyone with better access to original journalism might well reduce the impact of fake-news on social media platforms.[20] Similarly, the Rapid Response Unit, which is the executive branch of the UK Government, has created a system with the acronym FACT (find, assess, create and target), to help it identify and tackle the misinformation problem.[21] FACT particularly concentrates on analysing trends in story sources, and if specific search terms reflect a bias in search results, it is designed to enhance government pages to show higher in results or activate user-generated content, to help readjust the story and convince the most engaged users of the content.[22]

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?

11.1 To enhance their moderation systems, intermediaries should: (i) implement, where possible after consulting their users, clear, pre-established

---

[18] https://web.stanford.edu/~gentzkow/research/fakenews.pdf at page 219.
[19] See for example https://web.stanford.edu/~gentzkow/research/fakenews.pdf at pages 211-236; https://policyreview.info/articles/analysis/should-we-worry-about-filter-bubbles at page 9.
[20] https://www-blog-google.cdn.ampproject.org/c/s/www.blog.google/products/search/original-reporting/amp/
[21] https://perma.cc/4BDP-JTRN see page 7.
[22] https://perma.cc/837J-UF2U

policies premised upon objectively reasonable principles instead of political or ideological aims; (ii) adopt effective mechanisms to guarantee that users can easily comprehend and access any practices and policies, including platform terms and conditions, as well as comprehensive information about enforcement measures by publishing explanatory notes or outlines of these practices and policies; (iii) notify users quickly if material that they host, generated or uploaded could be subject to a restriction and provide the user with an opportunity to challenge such restriction; (iv) rely on automated procedures (whether or not based on AI) regarding their own or third party material only for legitimate operational or competitive purposes; (v) support the creation and research of adequate technical solutions to the fake news problem that users might voluntarily apply; and (vi) take part in initiatives, which provide fact-checking systems to users, as well as revising advertising practices to guarantee that diverse ideas and opinions are not negatively impacted.[23]

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?

12.1 As tools developed by D-CENT and My society show, it would be advisable to support the creation of open source systems. The idea is to create a multi-tool online repository, which city governments can deploy when carrying out new citizen engagement operations. Moreover, for instance, platforms such as, BetterReykjavic also contain a debate feature for any proposal, which is suggested. After receiving feedback, the individual who suggested the proposal, can then rewrite it, before public voting.[24]

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?

13.1 Technology can also provide elected representatives with the power to make decisions directly to individuals utilizing collaborative budgeting. This entails permitting citizens to choose how a proportion of the city budget is used. For example, 'Madame Mayor, I have an idea' is a collaborative budgeting procedure, which allows individuals to vote and suggest project proposals in Paris. In 2016, its pilot stage received more than 5000 submissions and over 20000 citizens subscribed to the platform.[25]

[23] https://www.osce.org/fom/302796 see page 4.
[24] https://www.nesta.org.uk/blog/power-to-the-people-how-cities-can-use-digital-technology-to-engage-and-empower-citizens/
[25] *Ibid*.

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

14.1 Taking Nesta as an example, the foundation has developed several distributed, privacy-aware, open source mechanisms for direct democracy, which permit individuals to receive relevant notifications in real-time, work cooperatively to suggest and write policies, vote and agree proposals, and assign resources using communal budgeting processes. For instance, Objective8 is an online crowdsourcing mechanism utilized for participatory policy writing, Mooncake offers a newsfeed bringing together notifications, comments and content, and Agora Voting software opens the ballot boxes and calculates the election results whilst protecting privacy.[26]

[26] https://www.nesta.org.uk/blog/digital-democracy-where-next/