Wilton Park

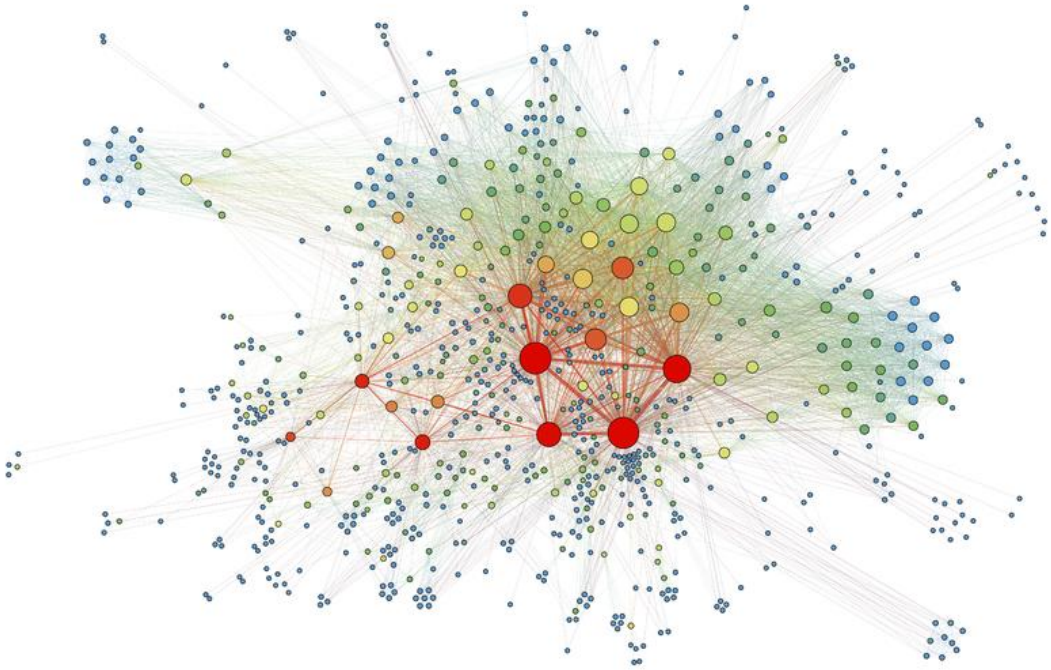

Image: : Martin Grandjean

Report

Digital interference in democratic processes: use and misuse of personal data

Monday 8 – Wednesday 10 April 2019 | WP1682

Wilton Park

Report

Digital interference in democratic processes: use and misuse of personal data

Monday 8 – Wednesday 10 April 2019 | WP1682

With support from Open Society Foundations (OSF) and in association with Tactical Technology Collective.

Executive summary

- There is a window of opportunity for different actors to work together to set new minimum standards around the use of personal data in democratic processes. In the wake of recent elections, referenda and digital platform scandals there is increased public interest in the use and misuse of their personal data. This has created an opportune moment to build a more digitally literate population and put in place the right kind of societal responses.
- Digital interference by foreign and domestic actors poses a threat to democratic processes. Public attitudes can be manipulated through hacking and cyber-security attacks or disinformation operations that can start years ahead of elections. These are often hard to identify and are likely to become even more sophisticated. The wide array of digital interference tools and techniques that have been used are only just starting to be understood in depth. Cambridge Analytica's use of psychometric profiling represents just one technique used by a single player in a vast political influence industry.
- While public faith in democracy was challenged long before social media disinformation campaigns, these campaigns are effective largely because they exploit these existing societal divisions. Social media has helped to accelerate fractious discourses and seems to have encouraged campaigns to become more negative and single issue based.
- The digital space is developing at such a speed that it has been challenging for those attempting to take action to get their responses right. Effective regulation of digital interference in the democratic process requires a balance that maintains civil liberties and ensures effective systems of public protection.
- With governments, independent regulators and some technology companies considering regulation, there is an important opportunity for cross-sector actors including the media, civil society and the public to influence the debate. Recommendations for ways to move forward include:
    - The development of a code of conduct to determine a minimum global standard for how political parties and digital advertising can use digital tools, techniques and personal data during elections.
    - Encouraging companies to engage with civil society groups early in the design process of tools and platforms to highlight potential problems and encourage more ethical design.

- Improving digital literacy amongst the public, civil society, media, international institutions and politicians.
- Creating more transparency and access for the media, researchers and civil society so that they can observe how digital platforms and political parties are using personal data.
- Increased cross-sector collaboration between policy makers, technologists and civil society experts to create independent and well informed responses.

Introduction

Against a backdrop of concerns over recent election processes and referenda and in the run up to the 2019 EU elections, this expert round table provided an opportunity to explore the interface between technology and politics. Building on previous Wilton Park conferences #FakeNews: innocuous or intolerable? and Safeguarding rights in the big data revolution, over three days participants from a range of disciplinary backgrounds examined ways in which personal data is used and misused in campaigning and elections and the implications for democracies.

The dialogue included representatives from regional and multi-lateral bodies, policy makers, information and disinformation experts, election specialists, think tanks, academics, and companies from selected countries in Europe, Africa, North America and Latin America. Discussions focused on generating a deeper understanding of election interference and disinformation, as well as exploring strategies for oversight, monitoring and policy interventions to mitigate risks, build resilience and maintain public trust in democratic processes.

It is challenging to take stock of such a fast moving issue, but there is increasing acknowledgement of the hidden costs of an internet ecosystem dominated by a small number of companies. With governments and some technology companies considering regulation, an important opportunity has been created for cross-sector actors as well as the wider public to influence the debate.

The scope and scale of digital interference in democratic processes

"Digital interference by foreign and domestic actors poses a threat to elections and democratic systems around the world."

1. Digital interference by foreign and domestic actors poses a threat to elections and democratic systems around the world. The scope and scale of this threat is likely to continue to increase as more people access the internet, important public discussions move online and states choose to digitalise aspects of their electoral systems.
2. Threats to public information flows during the US Presidential elections and the UK Brexit referendum in 2016 shifted concerns regarding 'uninformed' voters to concerns about voters being 'misinformed' by malicious foreign influence operations. Some forms of coordinated foreign digital interference can be seen as information warfare.

"Public faith in democracy was challenged long before social media disinformation campaigns."

3. Public attitudes and election results can be manipulated through hacking attacks or influence operations. Hacking can target parties to steal and leak sensitive information during campaigns. It can also target election infrastructure including voting machines and voter registration databases, as well as non-election infrastructure. An attack that shuts down power or the internet on polling day could depress turnout and undermine public trust in the process. The Hillary Clinton 2016 campaign took this threat seriously and produced contingency plans for a polling day without the internet.
4. Foreign state interference has also included covert influence operations. These can start years ahead of elections, with states experimenting with methods to spread distrust in democratic institutions and fuel social dissent. In 2016, troll farms and bot networks were used to artificially boost anti-establishment voices, attack candidates and stoke social conflict. False accounts targeted both sides of emotive debates (e.g. 'Black Lives Matter' campaign and separatism in Canada) and sent abusive messages to silence Hillary Clinton supporters.

5. These efforts are often very hard to identify and are likely to become more sophisticated. Governments should consider how to confront the problem of 'deep fake' videos (convincing false videos of world leaders) and explore in depth whether influence operations are likely to become bolder, and escalate in the lead up to polling day.

6. The current debate focuses heavily on foreign states, but there are also many individual consultants such as Steve Bannon who have assisted domestic campaigns to mount opaque influence operations. Candidates seeking to undermine rivals or target disillusioned voters have hired micro-targeting companies, paid popular bloggers for their support and shared misleading stories on WhatsApp. Harvesting from huge social media databases, micro-targeting companies such as Cambridge Analytica, have created political profiles for voters based on thousands of data points. These could be used to target the most persuadable voters with adverts that would mobilise them or stoke their fears. Domestic political use of influence operations has politicised the issue and made it more difficult for state bureaucracies to address.

7. The January 2019 court case against Cambridge Analytica ruled that if data is processed by a UK company, UK data protection laws apply. The case also raised issues of whether profiling based on political belief or race during campaigning is lawful.

8. Public faith in democracy was challenged long before social media disinformation campaigns. Controversial elections (eg. the US Presidential race in 2000), corruption scandals, politicised media, the restriction of rights, and repeated attempts to disenfranchise groups of voters have all had an impact. Influence operations are largely effective because they attempt to exploit these existing societal divisions which governments have not addressed. Social media has been instrumental in accelerating fractious discourses and has brought conspiracy theories and fringe ideas into the mainstream debates. But it is important to remember that the vast majority of sensationalist pieces that people read on social media originate from mainstream media institutions.

9. Voting machines are often presented as a way to prevent fraud, but have further undermined public faith in democracy in some countries where they are thought to have been controlled by a partisan electoral commission. Some politicians have allegedly 'hacked' their own infrastructure to alter counts and produce false results. In close contests, where the public suspect that a voting machine in a swing area was compromised, the 'winning' candidate's legitimacy may be questioned. Registration databases are also thought to have been compromised. A hack that deleted potential opposition supporters based on their ethnicity or location could lead to people being turned away at the polling station, systematic bias and potential unrest.

10. There is a growing trend of politicians questioning the impartiality of Election Commissions and making allegations of rigging before election day. They may do this because they are behind in the polls, or because they want to amplify their victory. Election Commissions often find it hard to respond as they lack good public relations teams and are cautious to avoid accusations of bias.

The tools and techniques of digital interference

11. There is still a limited understanding of the wide array of digital interference tools and techniques in use. Whilst there was widespread global attention on Cambridge Analytica's use of psychometric profiling, a range of techniques were used, and they were not the only player in a vast industry of influence. Beyond the more widely covered services of Facebook that enable political parties to target users based on their personal data, there are lesser known but equally widespread techniques that use personal data for political campaigning. These include geotargeting, campaign apps, third-party tracking, digital listening, robocalls and mobile texting and psychometric profiling.

"there are lesser known but equally widespread techniques that use personal data for political campaigning. These include geotargeting, campaign apps, third-party tracking, digital listening, robocalls and mobile texting and psychometric profiling"

12. While Facebook remains a powerful tool for political campaigns in the United Kingdom and the United States, the past few years have seen WhatsApp become an increasingly powerful campaigning tool in the Global South. In Kenya for example, during the 2017 election campaign WhatsApp was used by 12 million people. It helped to broaden the political discussion to include participants from urban and rural regions. Because communication via WhatsApp relies on senders having access to recipients' phone numbers, databases of phone numbers are a crucial asset for campaigners. However, this extended reach has also meant that misinformation, disinformation or defamatory information is more easily spread.

13. It is important to note that social media apps such as WhatsApp are not stand-alone tools to spread misinformation and disinformation. Rather, they are part of an ecosystem of techniques used to influence populations not only during election cycles, but all of the time. In recent elections in Kenya, Nigeria and Senegal it has been clear that politicians are using personal data to target people with disinformation through a range of tools, consequently having significant impact on the narrative. In the 2014 Indian elections Facebook was the main tool used to influence and manipulate voters, whereas in the 2019 elections it was WhatsApp. The contextual variations in different countries and the speed at which the usage of tools shifts makes it difficult to create regulation that addresses all different players and technologies.

"social media apps such as WhatsApp are not stand-alone tools to spread misinformation and disinformation. Rather, they are part of an ecosystem of techniques used to influence populations"

14. Increased digital security is also necessary to counter disinformation campaigns that come from both external and internal actors. In the current digital environment malicious individuals are fairly easily able to take over an account and target political figures from one or many compromised accounts. It used to be much simpler to discern whether a Twitter or Facebook account was fake, but today a fake account can often look 'real' with followers, friends, photos and a history of activity. In the 2018 Georgian elections, numerous false news outlet pages were used to influence voters and discredit candidates through a mixture of fake and real content. The difficulty in stopping the spread of disinformation and sentiment that these fake accounts encourage is that platforms and regulators are more reactive, than proactive. Currently not enough is being done to counter bot net operators who are spreading disinformation and the big platforms do not have enough people working to identify which accounts are fake. Identifying the perpetrators behind fake accounts and holding them to account is often just a matter of time. But it requires platforms to provide as much information as they can and more resource to combat it.

"today a fake account can often look 'real' with followers, friends, photos and a history of activity."

15. The broad range of online tools has also helped ordinary citizens and civil society organisations to play a part in the narratives and the spread of information in their respective countries. This has proven a positive way to counter negative messages and has enabled citizens to act in the face of unresponsive online platforms.

The long term effects of digital interference on social cohesion

16. Assumptions about how democracies work have been challenged. It is clear that long-term democracies are still in a state of transition. Individual experiences have changed significantly and there is a sense of nostalgia for the erosion of identity forming institutions. The effect of their decline is not clear, but could make it difficult to find shared stories around which to reunite.

"Some populist politicians are promoting a version of democracy in which majorities represent the absolute will of the people and minorities are silenced, ignored or considered enemies."

17. Focus group discussions suggest that public attitudes in the UK have changed in the past two years. Citizens feel they are living in a time of crisis. They are more likely to take risks, are less likely to look for consensus and some say they would be open to alternative forms of government. Similar patterns have been seen in other parts of the world, reflecting existing distrust in the democratic system but also the arrival of new populist actors. In Latin America and the Caribbean support for democracy decreased by 9% from 2014 to 2017.

18. Some populist politicians are promoting a version of democracy in which majorities represent the absolute will of the people and minorities are silenced, ignored or considered enemies. Their polarised narratives have encouraged people to separate by race or other socio-cultural factors, and to identify around a shared adversary rather than in shared values. In some countries, polarisation has been so great that opposing sides can no longer agree on a shared reality. This makes it very difficult to engage people with commonly shared and accepted information sources.

The challenges of digital political campaigning and what is being done to counter the harmful narratives.

"Parties have always 'pushed the envelope' during campaigns, but digitalisation has made some politically unethical practices easier"

19. Parties have always 'pushed the envelope' during campaigns, but digitalisation has made some politically unethical practices easier. In the same way, voter suppression campaigns have always existed, but now make use of mass text messages and social media. The internet also seems to have changed the focus and tone of campaigns. Just a few years ago, many parties focused on physical leaflets, but social media advertising has given access to cheap targeting and can deliver hundreds of communications at the same cost.

20. The tone of campaigns has become more negative and single-issue based. While politicians formerly tried to make national policy debates relevant to local voters, social media and a shorter news cycle means that they are often more interested in political insults. In many Latin American countries hate speech and violent attacks have become more common.

21. Governments, technology companies, journalists and civil society all have a stake in combating digital interference and harmful narratives. There is consensus that governments and technology companies should do more, but society is divided about perceived trade-offs between civil liberties and public protection. It is important for all actors to consider the costs of any potential action and inaction. A technological solution without addressing the root causes of social fragmentation, or without political backing, will not protect democracies.

"There is consensus that governments and technology companies should do more"

22. Government efforts to understand the origins of disinformation campaigns that worked a year ago are no longer effective. As disinformation campaigns become increasingly sophisticated but easier to implement, governments should consider how to reduce incentives to those considering running them. They should also consider penalties for companies with a record of spreading disinformation.

23. Governments could also consider improving information flows with allies and companies. The G7 now has a rapid response mechanism to help states quickly share concerns amongst government agencies and leading academics.

24. Some of the same people who campaigned against large technology companies acting as gatekeepers of the internet are now calling on them to introduce new tools to fight disinformation. Similarly, technology companies that initially aimed to be the antithesis of government have started to think they should act more like governments, which are good at mapping social harm and incentives. But it is important to consider safeguards and how tools to fight disinformation might be used in the future. In semi-authoritarian countries these tools might be used to suppress free speech or target opposition supporters.

"companies could consider encouraging their product teams to engage in open debates about the problems of disinformation to help inform better designed products"

25. Companies are well placed to see real time information flows and could be more proactive about what they share. They initially claimed to lack resources to tackle disinformation, but there is a growing consensus that they should play more of a role. Many Silicon Valley companies were overly optimistic about how people might use their tools. They often prioritised maximising user bases over consideration of potential risks. But the 2016 US elections, the Cambridge Analytica scandal, and 'Facebook Live' broadcasts of violent attacks encouraged Facebook to think more about potential problems when designing and launching products. It has improved automated reporting tools to remove fake accounts and has started working with fact-

checkers, promoting media literacy and making its reporting tools more robust. It has increased transparency of some of its adverts and group pages and has made some of its standards documents public. It is working to establish a panel to suggest what should and should not be allowed on the platform. These are welcome steps, but companies could consider encouraging their product teams to engage in open debates about the problems of disinformation to help inform better designed products.

26. Journalists and civil society have been key in exposing problems around digital campaigning and privacy. Any efforts to counter harmful narratives online should be accompanied by offline training to help more journalists and election monitors understand the issue. There should be more debate about how journalists cover information known to come from malicious foreign hacking efforts. Awareness raising and model responses could be part of the discussion.

27. There are an increasing number of civil society fact checking groups, but responses disproving misleading stories are often less engaging than the initial photo-shopped or video rumours. Tools such as 'Media Cloud' have helped some voters see how major public debates have been amplified. But simpler, more accessible real time tools might help voters understand how they are being influenced.

"responses disproving misleading stories are often less engaging than the initial photo-shopped or video rumours"

28. Fact checking plays an important role in responding to digital influence. It helps citizens and civil society to verify information. Fact checking organisations have found that names, statistics or estimates can often be mistaken or misquoted in the media, or by politicians. But it is important to determine whether this spread of disinformation is intentional or a genuine mistake. There is a real need to classify the type of disinformation and examine what level of harm it can do. To do this, platforms need to be more aware of the country specific nuances, understanding what behaviours could be triggered; fact checking needs to be scaled up to identify sources of reliable information; a news literacy curricula should be developed; and more funding is needed for fact checking practices in newsrooms.

29. Civil society groups have used social media to expose government efforts to hack election infrastructure and spread disinformation. Some groups have even managed to overcome state internet shutdowns and to expose state abuses. Civil society groups have also worked with the private sector to produce national voter information systems where no government information was available.

Monitoring, oversight and regulation in an increasingly fast paced environment

"For electoral regulators, the impact of digital interference on elections is one of the biggest democratic challenges"

30. There is often an expectation that the government and independent regulators should be responsible for monitoring, oversight and regulation in the digital space. While it is important for these more traditional actors to play a role, it is equally important to involve the digital platforms, as well as civil society and the public. Effective regulation of digital interference in the democratic process requires a fine balance to ensure fair and transparent elections, including freedom of speech, and a system whereby effective controls are in place to prevent abuses.

31. For electoral regulators, the impact of digital interference on elections is one of the biggest democratic challenges. The UK Electoral Commission will continue to work within their existing frameworks to: monitor and ensure that elections run smoothly; regulate political finance and political activity; and consider how electoral processes could be improved. While it is possible to put in place increased regulation and legislation around elections in the UK, so far there has been minimal government time or capacity to do so.

32. It is vital that civil society and electoral observers work with and support government departments and electoral commissions. Three main questions should be applied as a point of reference for civil society electoral observers: what has the biggest impact and proves the biggest threat to electoral integrity? what is technically feasible? what

issues are already regulated in the specific context? Civil society groups who report on elections have identified the need to understand the cycle of how people tend to form their political beliefs and voting choices pre and post elections in order to effectively observe and monitor elections.

33. It is important to note that monitoring and oversight do not mean the same thing in all country contexts. In some semi-authoritarian countries in Africa regulation of social media seems designed to prevent criticism of incumbents and oversight has often meant punishment of opponents. The close connections between the executive and regulatory bodies in some countries makes it difficult to create blanket global regulation to deal with digital interference in democratic processes. Despite these challenges, countries such as the UK with independent electoral regulators could encourage digital platforms to comply with certain minimum standards.

"monitoring and oversight do not mean the same thing in all country contexts"

34. Therefore, strategies to counter harmful narratives will have to be context specific. Companies based in the US should partner with local organisations in different continents to better understand nuanced social and political sensitivities. In countries where there is already a deep distrust in democratic processes, the introduction of electronic voting machines or vote transmission could be detrimental. Some digital systems have proved vulnerable and close connections between incumbent governments and their election commissions who control procurement raise questions about impartiality. The 'black box' nature of some digital infrastructure makes electoral processes difficult for voters to understand, making it more likely that they will believe rigging allegations. Where electronic voting or transmission is introduced, it is important to have back up paper trails.

35. The digital space is developing at such a speed that it has been challenging for those taking action to get their responses right, whilst keeping up to date on the most recent developments. In recent years, this has been demonstrated by a dramatic increase in spending by political parties on digital campaigns which use personal data to target existing and potential voters. This rapid escalation makes it more difficult for electoral regulators to put in place the right measures to track exact spending on political digital campaigns. Despite the requirement of political parties to publish their detailed election expenditure, it is challenging to obtain the exact constituency level break down of digital campaign expenses. It is hard to track online spend, with abuses only being followed up after elections. Fining or imprisoning low-level campaign staff for exceeding expense limits is unlikely to stop this. Countries could consider better ways of holding campaigns to account if they were found to have won on the basis of false information or online campaigns that far exceed spending limits.

"The launch of the Online Harms White Paper in the UK represents an attempt to regulate in a fast paced environment"

36. Governments or companies could also consider regulating auctioning principles around the sale of data. Current well-funded campaigns can pay to be heard on social media, but advocacy groups short of funds struggle to be part of the conversation. Companies could consider distributing a limited number of credits to each party to be used during campaigns. This could work in a similar way to broadcast media rules.

37. There is already a consensus that UK regulations for print and broadcast media should be extended into the online space. The UK government is also considering the ethics of micro-targeting in political campaigns and is preparing requirements for online materials to be published in line with print regulations.

"Companies would be held to account with regard to a set of online harms, ranging from illegal activity and content to behaviours which are harmful but not necessarily illegal"

38. The use of voter information to build political profiles and target campaigns is not new and is not necessarily unethical. But governments should try to understand concerns around opaque data supply chains used by micro-targeting companies – what data is being used, which groups are using it and for what purpose? Any regulation should consider the relative power of different users (at a ground level campaigns are often still relatively unsophisticated). Suggestions for regulation include asking companies to share parts of their data with government to be able to work in certain sectors.

39. The launch of the Online Harms White Paper in the UK represents an attempt to regulate in a fast paced environment. The debate around online harms and the use of personal data is rapidly moving, vast and complex. While there is not yet a complete understanding of the issue, the UK government recognises the need to take action to deal with the challenges. The White Paper sets out plans for a package of online safety measures to make companies more responsible for their users' safety online, especially children and other vulnerable groups. It proposes establishing in law a new duty of care towards users, which will be overseen by an independent regulator. Companies would be held to account with regard to a set of online harms, ranging from illegal activity and content to behaviours which are harmful but not necessarily illegal.

40. In the EU, personal privacy and data privacy are considered fundamental rights and vital components of a sustainable democracy. Political beliefs fall under these privacy rules. The EU's General Data Protection Regulation (GDPR) says that users should be in charge and able to secure how their data is used. It applies to any organisation or company around the world that offers goods or services to people in the EU or monitors their behaviour. The GDPR represents an important step, but is still inconsistent in its application: further work is needed to communicate the practical implications for the public, businesses and governments.

A proposal for the way forward

The development of a code of conduct

"Existing international human rights law presents a solid and widely shared framework which can be used as an effective base"

- A code of conduct should be developed to determine a minimum global standard for how digital tools, techniques and personal data can be used in the democratic process. This would provide clear guidelines for political parties, political campaigners, digital platforms and those in the digital influence industry. It could also include a cap on political party spending on digital campaigning alongside greater transparency about how voters have been targeted. This cap and increased transparency would create a more equal playing field between political parties in spreading their political messages and increased transparency for the public and observers to know how money is being spent.
- Legislation or regulation must be highly contextual. It is clear that the specific use of online tools and techniques by each population is unique and no blanket solution can be implemented globally to address digital interference in democratic processes. Regulation should be nuanced and detailed, rather than generalised at a global level.
- With contextual development and implementation in mind, it is important for countries such as the US, Canada, the UK and international bodies and regional bodies such as the European Union to leverage their global standing and encourage the development of minimum global standards. The EU's GDPR and the new UK Online Harms White Paper go some way to doing this. Because the nature of the discussion varies across countries, it is also important to involve a range of civil society groups and governments in order to create a more level playing field of understanding and action.
- Existing international human rights law presents a solid and widely shared framework which can be used as an effective base. To build on this, strategic litigation at both the national and international levels would be an effective way to identify and pursue legal cases as part of a strategy to promote a more fair, open and honest use of personal data in the democratic process. By focusing on individual cases it would help to bring about broader social change in this space.

"Increased transparency of how digital platforms and political campaigners use personal data should be accompanied by the promotion of increased digital literacy"

Creating more ethical design for digital platforms

- More work needs to be done with technology companies and digital platforms in the early stages of their design process. This could help educate tech developers, engineers and designers and support them to create more ethical products. Awareness raising and education regarding the ethics of design would help to ensure a more proactive approach.
- Awareness raising around the ethics of design should also be widened to include venture capitalists who invest in the initial technologies. Their understanding of the social implications of badly designed products could assist to minimise negative consequences further down the path.
- Algorithmic regulation to increase transparency could be considered. An independent audit system or auditing body could be developed to keep digital platforms in check and ensure that they are adhering to set standards and regulations in their algorithm and product design.

Creating more digital literacy amongst the public, civil society, media, international institutions and governments

- Digital literacy needs to be increased amongst younger and older generations. This could enable better public understanding of the impact of their online behaviour and the way in which personal data is used in the democratic process. However, it is important to consider that there is already a lot of information pushed onto overwhelmed users and it is often hard for the general public to understand this fast moving topic. There should be careful consideration about ways in which to make information more accessible, and less technical and intimidating to the public.
- Policy makers and legislators also need to improve their digital literacy to be able to take a proactive approach. Building up their capacity and confidence would lead to more effective, context specific regulation.

Creating more transparency and access

- The media, researchers and civil society could play an important role as watch dogs of how digital platforms and political parties are using personal data in democratic processes. This would require digital platforms and political campaigners to provide greater access to the nature of personal data used, how it is processed, how much is spent, and on what. It would further enable cross-sector actors to reassure the public about the conduct of digital campaigns, to the benefit of both digital platforms and political parties.
- Increased transparency of how digital platforms and political campaigners use personal data should be accompanied by the promotion of increased digital literacy for the general public. Without this there is a risk of further voter disengagement and distrust in democratic systems.

Increased cross-sector collaboration

- It is important to impress upon policy makers that they need to engage more with technologists and civil society experts who are willing to give independent and well informed advice. Their technological perspectives, alongside their focus on ethics and the public-good, are vital for the development of effective regulation and legislation. It is not enough for policy makers to engage solely with big companies.

Conclusion

There is a need for governments, civil society and digital platforms to take a more continuous, proactive and preventative stance to address digital interference in the democratic process. A shift from current reactive responses will be difficult in this fast paced environment. But it is a necessary step to take to maintain trust in democratic systems and in the growing use of our personal data.

It is important that this task does not fall on the shoulders of one actor alone. The responsibility must be shared amongst governments and companies, as well as civil society, media, international institutions and the public. There is currently a window of opportunity to work together and coordinate between different actors in setting new minimum standards around the use of personal data in democratic processes. In the wake of recent elections, referenda and digital platform scandals there is increased public interest in the use and misuse of their personal data, thus creating an opportune moment to educate and build a more digitally literate population.

A key point of consideration when moving into the next phase of work is to realise that there is a whole ecosystem of tactics and techniques already at play, as well as a wide variety of actors. It is important to shift away from the fixation solely on Facebook and Cambridge Analytica and to recognise that other digital platforms and companies are using personal data to influence democratic processes.

In this fast paced environment finding solutions that will stand the test of time while also being detailed enough and context specific is a tough balancing act. A coordinated and collaborative cross-sector approach is necessary to ensure that the use of data in the democratic process is appropriate and that future digital interference does not diminish the integrity of our modern day democracies further.

Authors:

Nicole Ayo von Thun
Executive Assistant, Tactical Technology Collective.

Chris Day
Senior Research Analyst, Africa Research Group, Foreign and Commonwealth Office

Wilton Park | May 2019