Digital Rights Watch

Submission to Joint Standing Committee on Electoral Matters - Inquiry into and report on all aspects of the conduct of the 2016 Federal Election: Cyber manipulation of elections

06 August 2018

Who is Digital Rights Watch?

Digital Rights Watch (DRW) is an Australian national non-profit charity that supports, fosters, promotes and highlights the work of Australians standing up for their digital rights. digitalrightswatch.org.au

This submission is provided by Digital Rights Watch and endorsed by the following organisations:

- Australian Privacy Foundation
- Future Wise
- Human Rights Law Centre

For more information about this submission please contact Tim Singleton Norton, Chair - tim@digitalrightswatch.org.au

Context

As representatives of civil society in Australia, we recognise the important role which social media has come to play in facilitating and empowering grassroots political engagement. Like any powerful tool, however, social media is also vulnerable to misuse. We are pleased by the Joint Standing Committee's interest in this issue and welcome the opportunity to make a submission to this inquiry.

At the Australian Human Rights Commission's Human Rights and Tech conference in July 2018, Australia's Ambassador for Cyber Affairs Dr Tobias Feakin said *"[Digital influence on elections] is a constant threat, and we have been engaged in this area for months. We have pushed out training to political parties to educate them on how to protect themselves. We are looking at strengthening the cyber security of voting systems. The government is acutely aware of it, and the impacts on a liberal democracy. It's our job to combat this and respond if we see potential influence such as what has been witnessed in the US. We haven't seen it here, but we must prepare."*

The four major political parties have received funding to protect their online systems and infrastructure from attack.[1] As the controversy over the US 2016 presidential election has shown, however, there are many ways besides hacking to interfere in a country's election.
In addition to shoring up their cybersecurity, parties also need to play a role in safeguarding voters and social media users against potential abuses of personal data for targeted political advertising. This should instituting an "ethical pause" as recommended by the recent findings of the UK Information Commissioner, and bringing political parties, and their contractors and volunteers, under the Privacy Act.

Setting the tone from the top: political parties, disinformation campaigns and the sources of social media manipulation in Australia

A July 2018 report by the Oxford Internet Institute found that political parties are major sources of social media manipulation.[2]

[1] Hendry, Justin. 'Political parties to get cyber subsidy for electoral databases'. Itnews, 10th July 2018.

[2] Bradshaw, Samantha and Philip N. Howard, "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation." Working Paper .1. Oxford, UK: Project on Computational Propaganda, 2018

Research author Samantha Bradshaw observed that *"The number of countries where formally organised social media manipulation occurs has greatly increased, from 28 to 48 countries globally. The majority of growth comes from political parties who spread disinformation and junk news around election periods. There are more political parties learning from the strategies deployed during Brexit and the US 2016 Presidential election: more campaigns are using bots, junk news, and disinformation to polarise and manipulate voters."*[3]

The research found that in Australia as of 2013, automated accounts (also known as bot accounts) were being used to spread pro-government messages and attacks on the opposition by at least two politicians or parties.[4] The researchers note that "With each passing election, there is a growing body of evidence that national leaders, political parties, and individual political candidates are using social media platforms to spread disinformation... In emerging and Western democracies, sophisticated data analytics and political bots are being used to poison the information environment, promote skepticism and distrust, polarize voting constituencies, and undermine the integrity of democratic processes."[5]

At the same time, however, it is important to remember that social media plays a crucial role in enabling and informing legitimate political debate. It is precisely because of the power of social media as a tool for engaging the public in the political debate which makes misuse of it so concerning.

Both the benefits and the risks of social media are magnified by the collection and use of data to target specific groups or individuals with tailored messages. Used responsibly, this can contribute to creating an informed and empowered public; misused, this can lead to the spread of disinformation, the fracturing of the public sphere and ultimately even undermine public trust in the legitimacy of the democratic process.

Like most technologies, social media is neither good nor bad but rather a reflection of those who use it. As those seeking to win the trust of the public, and to steer the nation’s course into the future, political parties need to set the tone from the top by behaving ethically and transparently in their use of social media for political communication.

[3] ‘Social media manipulation rising globally, new report warns' [Press release]. Oxford Internet Institute, 20th July 2018.

[4] Bradshaw, Samantha and Philip N. Howard, “Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation.” Working Paper .1. Oxford, UK: Project on Computational Propaganda, 2018,, Table 2, pp.14.

[5] Ibid, pp.5.

Who uses social media to influence the political debate?

Social media is playing an increasingly significant role in shaping the national political debate both online and offline. Social media platforms such as Facebook and Twitter have emerged as key spaces in which the relatively unfiltered opinions of ordinary Australians are shared, debates of varying degrees of robustness are had and grassroots political movements can be mobilised.

Social media is also a crucial source of daily information for many Australians. As of 2018, 52% of Australians use social media as a source of news.[6] Discussions and trends on social media also often both reflect and drive the traditional media cycle,[7] making it a key battleground for groups seeking to inform, influence or shape political and policy debates. This includes:

- Federal, state and local governments
- Government departments and bodies
- Individual politicians
- Political parties and their associated entities
- Corporations
- Media
- Interest groups (including industry bodies, civil society groups, NGOs, informal social media groups and communities)
- Foreign actors

Each of these groups may have legitimate and valuable contributions to make to Australia's online political discussion. At times, however, the use of social media for sharing information and engaging with the public tips over into manipulation or undue interference in the political process.

When does the use of social media to influence the political debate become a problem?

This is a complex question which cannot be fully answered in a few pages. Broadly, however, the use of social media to influence political discussions becomes a problem when it involves:

- **Deception** – for example, the intentional dissemination of false information (AKA 'fake

[6] Reuters Digital News Report 2018, Reuters Institute for the Study of Journalism, University of Oxford, 2018.

[7] Sauter, Theresa and Axel Bruns, Social Media in the Media: How Australian Media Perceive Social Media as Political Tools. ARC Centre of Excellence for Creative Industries and Innovation, Brisbane, 2013.

news') or presenting true information out of context or in such a way as to create a misleading impression. Another example of deceptive social media practices is to deliberately misrepresent who is behind the information or the purposes for which it is being communicated.

- **Distortion** – for example, the use of bot accounts to 'amplify' a particular political message and create an impression that there is greater public support for that message than actually exists. This method of manipulation is becoming more difficult to detect as bots become more sophisticated and thus more difficult to distinguish from real social media users.
- **Lack of transparency** – for example, when it is not clear to social media users targeted by an influence or advertising campaign whether they are being targeted, who is targeting them, what personal data is being used to target them and why. This lack of transparency makes it difficult for users to evaluate the information they are being presented with, including understanding the potential biases or agendas which may be driving the campaign.

Case Study: Facebook's "dark ads" and the same-sex marriage postal vote

Facebook enables groups and organisations to run tailored advertising campaigns which will only be seen by the particular groups and individuals being targeted. The lack of transparency makes it extremely difficult for outside observers to know what messages and information these so-called "dark ads" are spreading. Such ads are used widely by actors seeking to influence the political debate – in fact, in the UK they have even been used by political parties against their own candidates.[8]

Dark ads are also playing an increasingly prominent role in the Australian political context. In the lead up to the 2017 postal vote on same-sex marriage, the federal parliament passed a law intended to safeguard against vilification or intimidation, including requiring paid advertisements to be authorised. However during the months and weeks before the vote, sponsored Facebook posts (i.e. paid advertising) which were openly homophobic and were clearly targeting Australian Facebook users with the intention of influencing their vote continued to appear without authorisation. At least one such ad took more than a month to be blocked, despite the direct intervention of the Australian Election Commission and Special Minister of State with Facebook.[9]

[8] Busby, Mattha. 'Corbyn supporters attack Labour moderates for 'using targeted Facebook ads to trick him about own general election campaign', The Independent, 15th July 2018.

[9] Evershed, Nick. 'Facebook took month to remove page that violated same-sex marriage safeguard laws', Guardian Australia, 2nd November 2017.

The fact that these unauthorised ads were able to target Australian voters with more or less complete impunity despite the safeguards law, and the difficulty in identifying who was behind the campaigns and who was exposed to them, should be a matter of serious concern for the parliament.

Facebook has recently taken steps to improve the transparency of dark ads, including launching an archive for ads with political content, and allowing Facebook users to see the advertising campaigns a page has run in the previous week even if they are not in the targeted group. This is a significant improvement, but is not sufficient to resolve the problem of transparency.

For one thing, the tool does not show what Facebook calls “dynamic creative” ads. These are ads which are partially automatically generated by Facebook to optimise the combination of images, videos, titles and descriptions for each user. In the case of the archive, it is not clear exactly how Facebook is defining and identifying ‘political content.’

The tool also does not allow users to see which groups are being targeted by which advertising campaign. This is of particular concern due to the close link between the misuse of social media and the invasive and irresponsible use of personal data for microtargeting.

How does the use of personal data for microtargeting increase the risk of misuse of social media in the political debate?

As the Cambridge Analytica scandal has made abundantly clear, the exploitation of personal data of social media users for political purposes can have wide-ranging consequences from the level of nation states right down to its impact on individuals.

This includes therisk to the security of the data itself, but it also includes associated risks of negligent, irresponsible or inappropriate use of citizens’ and voters’ data, such as loss of public trust in political parties and institutions. The exemption of political parties from the Privacy Act is therefore highly consequential.

In a recent report[10] connected to a 14 month investigation into Cambridge Analytica, the UK’s Information Commissioner’s Office said that *“one of the most concerning findings from the investigation was a significant shortfall in transparency and provision of fair processing information.”*

[10] Information Commissioner’s Office, ‘Democracy Disrupted? Personal information and political influence’, London, 2018.

The Information Commissioner is now calling for an 'ethical pause' in the further expansion of data collection and targeting in order to allow government, Parliament, regulators, political parties, online platforms and citizens time to reflect on their responsibilities in relation to these new technologies.

The Commissioner observes that in order to *"retain the trust and confidence of electorates and the integrity of the elections themselves, all of the organisations involved in political campaigning must use personal information and these techniques in ways that are transparent, understood by people and lawful."*

This is every bit as true of Australia as it is of the UK. Australians' trust in the political system and in their political representatives has plummeted in recent years. A 2018 study by the Museum of Australian Democracy and the University of Canberra's Institute for Governance and Policy Analysis found that Australians' trust in governments and politicians is at the lowest it has been since 1993. Levels of satisfaction with how Australia's democracy is functioning have likewise plunged over the past several years.[11]

The exemption of political parties, and their contractors, sub-contractors and volunteers, from the Privacy Act therefore poses not only a data security risk, but also a major reputational risk for political parties themselves.

If political parties are not absolutely sure where their contractors and all of their contractors' sub-contractors have acquired data from; whether it was collected with the full knowledge and consent of the people the data belongs to (as opposed to hidden in the fine print of Terms and Conditions agreements which no one has read); exactly how it is being analysed, shared and used; and whether those uses will be accepted by the public at large, then it is very possible that a data scandal similar to the Cambridge Analytica episode could occur in Australia.

The backlash from such an incident would not be limited to the particular political party responsible – the low trust in politicians generally makes it likely that all political parties would face public outrage. This means that political parties should consider not only how confident they are in their own data practices, but how much faith they have in the practices of their opponents.

Maintaining public faith in the legitimacy of the democratic process is not a partisan issue. Public trust in how our democracy functions is a crucial part of the bedrock of Australian society and the Australian way of life, and its erosion eats away at support for all actors in the political process. Bringing political parties and their associated entities under the Privacy Act is not just

[11] Evans, Mark, Max Halupka and Gerry Stoker, 'Who Do You Trust to Run the Country? Democracy, Trust and Politics in Australia'. Museum of Australian Democracy and the University of Canberra's Institute for Governance and Policy Analysis, Canberra 2018.

about managing risk; it is also an opportunity to demonstrate leadership, build trust and prove to the public that they are serious about protecting the privacy rights of voters.

What should be done to reduce the risk of misuse of social media, personal data and microtargeting to interfere in Australia’s political debate?

We are at an inflection point. The way in which Australian society, and particularly our political leaders, respond to the challenges posed by new technologies today will shape our nation for years to come.

The clear risks which the misuse of social media pose to the integrity of our elections and public trust in our democratic systems means that political leaders should seize this moment as an opportunity to set the tone from the top. This should include:

- Removing the exemption for political parties, their contractors, sub-contractors and volunteers from the Privacy Act, both to reduce the risk of misuse of data and social media and to send a clear signal to the public that the parliament is taking this issue seriously.

- Implementing an “ethical pause” similar to what has been suggested by the UK Information Commissioner.

- Using this pause to develop a code of conduct for the ethical use of social media for political communication, including the use of data for targeting, the use of automated (bot) accounts and transparency in relationships with contractors, sub-contractors and other third parties.

- Following Germany, Austria, Switzerland and other nations in requiring an “Impressum” section for Facebook pages including details such as the name of the business or organisation, name of the owner or manager of the organisation, relevant registration or license numbers and contact information.

- Consider potential options to empower the AEC in the social media space. This could include requiring Facebook to respond to AEC enquiries within a set period of time and increased resources for the AEC to handle digital and social media-related issues.