



Submission to the Electoral Matters Committee of the Parliament of Victoria's Inquiry into Elections and Social Media

Prof. Axel Bruns, A/Prof. Daniel Angus, Dr Timothy Graham, Dr Sofya Glazunova, Tegan Cohen
QUT Digital Media Research Centre
Building Z9, Creative Industries Precinct
Kelvin Grove, QLD, 4059

How is social media changing elections?

Social media has rapidly and radically changed our communication landscape with regards to how citizens engage with each other, with politicians, political parties, government departments, and other institutions. Among other changes, social media has provided us with more immediacy in our daily communication and media consumption, and increased the proximity between citizens, institutions and institutional actors.

Social media platforms themselves are a key part of the shift in the broader communication landscape as they largely determine the conditions for interaction (affordances), what speech is permitted (via their own moderation guidelines), who is permitted to be part of their platform, whether communication is public, private, or semi-private in nature, what advertising is permitted and how it is served, among a host of other conditions.

A result of this rapid uptake of social media as a de facto communication mechanism is that politicians, political parties, lobbyists, unions, industry groups, civil society, and domestic and foreign third parties have adapted their communication tactics around political elections. These various political actors utilise social media (Twitter, Facebook, Instagram, SnapChat, WhatsApp, Youtube, TikTok, etc.) for a variety of purposes including:

- Publishing policy materials and responses to specific issues;
- Organising 'on the ground' activities such as meetings, candidate drop-ins, doorknocking, protests and activations, etc.;
- Publishing advertising, including authorised and unauthorised material;
- Engaging in online discussion and debate.

These social media-enabled activities present a combination of new possibilities and challenges to liberal democracy. They offer possibilities for increased engagement and participation by citizens and political actors, but there is also the possibility that weaponised mis/disinformation or other tactics may be used to influence public opinion and election outcomes. We discuss these issues throughout the remainder of our submission.

What problems have you seen with social media and online advertising around elections?

1. Mis/disinformation

Misinformation refers to false information that is spread, regardless of its intent to knowingly deceive. Disinformation is false or biased information that is spread with an intention to harm, mislead, deceive or subvert a discussion. Both mis- and disinformation are problematic in their own right, particularly when they are weaponised in the context of elections. Specific problems include:

- Differential speed of information transmission, where rumours, mis- and disinformation can travel quickly through a social network. Some studies have revealed that under certain conditions false information can spread faster than truthful information;
- Gaming of information visibility through astroturfing and sockpuppeting, by both human users (e.g. party operatives or lobbyists) and bots;
- Groups of newly created, anonymous accounts gaming the trending topics lists of sites like Twitter in order to make certain hashtags and key terms nationally visible and steer media coverage and discourse towards these topics;
- Celebrities and influencers acting as ‘superspreaders’ of mis- and disinformation, thereby boosting fringe, hyperpartisan, and other problematic content ‘up the chain’ to mainstream media coverage.

Further, many mis- and disinformation activities are increasingly shifting to semi-private social media groups and pages, including those that disguise underlying political affiliations and intentions. This decreases the visibility of such political campaigns and makes it difficult to accurately observe coordinated activities, including sockpuppeting and astroturfing activities aimed at encouraging and engaging in disinformation campaigns. This lack of independent scrutability harms our ability to counter mis/disinformation.

2. Platform moderation

Platforms impose their own moderation principles on online speech, replacing state regulation of what is and isn't allowed. This can lead to problematic content (i.e. racist, misogynistic, homophobic, ableist, ageist, etc.) being permitted, or to legitimate political discussion and expression being silenced. There are few mechanisms to challenge decisions made by platforms on what is or isn't moderated, and there is a complete lack of transparency on how and why moderation decisions are made.

Platforms also operate an uneven playing-field, where there is potential for platforms to self-preference their own political campaigning messages, such as by giving themselves advertising options which are not available to other campaigners – Google's #AFairCode banners on its search engine pages, challenging the ACCC proposals on sharing advertising revenue, are an obvious example for this.

3. Online abuse, doxing, harassment directed towards candidates and party members

Abuse and trolling *of* candidates as well as *by* candidates is commonplace online, and often reflects and works to reinforce existing longstanding discrimination towards women, people of colour, Indigenous peoples, and other minority groups. There are cases of candidates having personal details leaked online, so called 'doxing' incidents, and instances of deliberate and coordinated harassment.

Abuse is often targeted based on inferred 'vulnerabilities', and platforms are also at risk of engaging in discriminatory practices, e.g. 'political redlining' (Howard, 2005; IDEA, 2018) through the ability to micro-target advertising (further discussed below).

Divisive and emotionally charged hashtags are often used as part of orchestrated campaigns which attempt to push these hashtags onto the trending topics list and whip up an online frenzy. Psychologically, such events have been explained through a process of deindividuation (McKenna & Bargh, 2000), where otherwise rational actors may engage in mob-like cyberbullying activities due to a weakened ability to regulate their own behaviour, reduced ability to engage in rational, long-term planning, and a tendency to react to immediate cues or based largely on their current emotional state.

4. Old media laws are incompatible with new media practices

Electoral laws have not kept pace with the realities of digital campaigning. For instance, the blackout period for election ads in the lead up to the Federal and State elections only applies to television and radio broadcasters, and not to social media and other digital platforms (*Broadcasting Services Act 1992* (Cth), sch 2 s 3A). The arbitrary nature of this distinction was underlined during the 2019 Federal election, when the major commercial free-to-air TV networks instead screened election ads on their streaming platforms during the blackout period (Duke, 2019). Related issues also include:

- Increased difficulty in enforcing authorisation of official campaign materials as required by electoral laws, especially when such material is created at hoc and posted to micro-targeted groups;
- Undeclared influence campaigns by domestic and foreign third parties;
- Lack of timely response and takedown of mis/disinformation and (increasingly) deep fakes, which have the potential to substantially affect election results;
- Circulation of disinformation pretending to represent electoral commission advice.

5. Political micro-targeting

The tailoring and targeting of messages to voter segments is not a new phenomenon. In some ways, micro-targeting is a contemporary iteration of older techniques such as direct mail, but "with exponentially more data, new tools and more precision" (Tufekci, 2014, 9), and – owing to the ubiquity of social media platforms – performed at unprecedented scale.

Contemporary forms of political micro-targeting on social media platforms have the potential to adversely impact informed voter choice and public deliberation. When an individual receives a targeted

political message on Facebook, they are provided with very little information about the grounds upon which they have been targeted. This lack of transparency arguably deprives voters of information which is pertinent to their assessment of political messages (Ward, 2018).

A related concern is the reduced public visibility of targeted advertising on social media. Whereas political ads disseminated via mass media are able to be evaluated, critiqued, and rebutted through public discussion, targeted political advertising on social media largely deprives recipients of the benefit of diverse viewpoints and collective scrutiny. Tools such as the Facebook Ad Library, touted as providing greater transparency about how political actors use micro-targeting, still fail to offer comprehensive information about how and by whom specific groups of voters are targeted.

6. Voter privacy and transparency

The collection and mining of social media data to build highly detailed and up-to-date voter profiles has significant and largely unaddressed privacy implications. Social media platforms are a rich source of data for political campaigners. While Australian political parties began compiling voter profiles long before the advent of social media, the ubiquity of platforms have significantly increased the volume and variety of data about voters which is readily available to political campaigners. Using campaign software solutions, political campaigners are able to synchronise their voter records with matching social media profiles, constructing highly detailed and up-to-date dossiers. NationBuilder, whose software is utilised by a number of Australian political organisations, describes its sync feature as follows:

Social media data can help you learn about your supporters' interests and influence.

Shortly after an email enters your database, NationBuilder Match will append corresponding social media accounts along with any info visible to the public — their Twitter bio or LinkedIn headline, profile images, follower counts and more.

You can use that data to find out what a donor cares about before you reach out. Are they a doctor? A space enthusiast? Do they have a massive following they could tap to help amplify your campaign to a wider audience? (Stevens, 2017)

The opacity surrounding the data collection activities of political parties means that Australian voters are generally unaware of the full nature and extent of information collected about them for political purposes. Due to exemptions in the *Privacy Act 1988* (Cth) and *Privacy and Data Protection Act 2014* (Vic), political parties and Victorian MPs do not have the same transparency obligations as entities subject to those laws. Furthermore, voters do not have rights to prevent political parties from harvesting their sensitive information, nor to obtain access or correction of records about them held by political parties.

What actions have you seen governments take in relation to social media/online advertising and elections? What results have been achieved by these actions?

1. Transparency - Political Ad Archives / Tracking

Various legislatures have introduced or proposed a range of measures to increase transparency in relation to social media operations and procedures with respect to elections, including advertising, content moderation and complaints handling. One popular initiative has been the mandating of political advertisement archives, though with varying approaches to the level of disclosure required. Since 2018, most of the dominant digital platforms have established advertisement registries. However, some have refused to comply with the specific legislative requirements for registries in certain jurisdictions, including Canada (Leerson et al, 2019).

Canada

In 2018, the Canadian Government passed legislation which requires certain online platforms to maintain public registries of 'partisan' and election advertising messages published on the platform, including a copy of each ad and the authorising entities (*Elections Modernization Act* s 325.1(2)). The Canadian legislation only targets platforms with a large reach, which is determined by reference to the average number of monthly site visits by Canadians.¹

United States

The *Honest Ads Act*, a bill proposed in the US Senate, would compel online platforms to maintain an online public record of any requests to purchase political advertisements (*Honest Ads Act* s 8(1)). The record must contain (among other things) a copy of the ad, a description of the audience targeted, number of views, average rate charged for the ad and details of the entity who purchased or authorised the ad (*Honest Ads Act* s 8(2)). Similarly to the Canadian law, the bill only extends to platforms with a certain number of monthly US visitors during a 12 month period (*Honest Ads Act* s 8(3)). As at the time of writing, the Bill has yet to be passed.

European Union

Ahead of the 2019 European Parliament elections, the EU recommended parties and other campaigners publish details about their online expenditure and advertising targeting criteria, and that Member States require such disclosure (EC, 2018)

¹ Platforms that receive average monthly visits in a specified 12 month period of at least '(a) 3,000,000 times, if the content of the online platform is available mainly in English; (b) 1,000,000 times, if the content of the online platform is available mainly in French; or (c) 100,000 times, if the content of the online platform is available mainly in a language other than English or French' (*Elections Modernization Act* s 325.1(1)).

2. Little or no regulation

Netherlands

Dutch legislation is not specifically regulating online advertising during elections and referenda in the country (Dobber et al., 2019). Though, recently, the Dutch government took actions to increase the transparency of parties' online advertising proposing the Political Parties Act (Van Hoboken et al., 2019).

United Kingdom

In the UK, paid political advertising is not specifically restricted online through regulation (Dobber et al., 2019), and the UK Electoral Commission has recommended a number of changes to online political advertising during elections. They include that (a) election and referendum adverts on social media platforms should be labelled to make the source clear; and (b) campaigners should be required to provide more detailed and meaningful invoices from their digital suppliers to improve transparency (Dobber et al., 2019).

3. Moderate government regulation

Spain

The Spanish Data Protection Agency issued criteria for the use of personal data for political purposes, including restrictions on obtaining social media data from private messaging groups (e.g. WhatsApp) or only shared with limited people (e.g. 'friends only') (OxTec, 2019). It also restricts individual-level profiling.

4. Excessive government regulation

Russia

In Russia, online political ads during elections are regulated by Federal Laws, Central Electoral Commission, censorship, and regulatory bodies. As a part of a wider strategy of regulating the Net, international and domestic social media platforms are forced to satisfy most of the government's requests to remove content, including political ads. Large international companies such as Google and Facebook in some cases can resist political pressure. In 2020, YouTube deleted the agitation video for the Russian Constitution Reform Voting due to the presence of discriminating statements (Meduza, 2020). However, domestic social media platforms such as VKontakte are more regulated by authorities, which also imply self-censorship. VKontakte allows political advertising on the platform only during the period of electoral campaigning and only by registered candidates (VKontakte, n.d.). This prevents the challengers of the political regime who are often barred from elections from competing with the establishment in the digital public sphere.

What are the most effective ways to address any problems with social media and online advertising around elections?

First and foremost, more transparency is required.

We require greatly enhanced access to the Facebook Ad Library, including full searchability and details on microtargeting strategies of specific ad campaigns; plus similar ad library functionality for other platforms – cf. the Illuminating 2020 (<https://illuminating.ischool.syr.edu/>) and Ryerson ad spend projects (<https://socialmedialab.ca/2020/08/17/who-is-running-facebook-political-ads-during-the-pandemic-in-canada-update-july-2020/>) for the United States and Canada, respectively.

The Facebook Ad Library as it is currently designed enables users to search for the ad campaigns run by known actors (e.g. the accounts and pages of political parties). This is welcome in principle, but inherently encourages unscrupulous political campaigners to outsource their rogue political advertising activities to new and apparently independent accounts that were created solely for this purpose. Election authorities, researchers, and others scrutinising campaigns would not be able to detect these ads through the Ad Library unless they happened upon them in day-to-day Facebook use.

Similarly, the Ad Library allows searches only by who is running campaigns, not by who is targeted. This prevents the detection of mis- and disinformation campaigns that specifically address vulnerable communities – for instance by providing false voting information to migrant communities in their languages of origin, or by directing fear and smear campaigns that discredit candidates at specific electoral demographics.

For everyday users of social media platforms, existing features that explain why they encounter specific ads (e.g. Facebook's 'Why Am I Seeing This Ad?') are welcome, but far too limited at this stage; they provide little detailed information. There should be greater obligations for platforms to supply prescribed details about the *actual* grounds for targeting users with each ad, listing the specific targeting categories chosen by the advertiser in scheduling the ad. Similarly, both through the Ad Library and information directed at everyday users, platforms should provide real-time disclosure of online advertising expenditure – with itemisation down to the level of the individual ad (i.e., 'You are seeing this advertisement because your profile says you are a [personal attributes]. [Advertiser] has spent A\$[value] on this campaign to date.')

To track not only official advertising, but also rogue or 'below the line' advertising activities, astroturfing and sockpuppeting campaigns, and other coordinated inauthentic activities that are designed to influence public opinion and electoral choices, we also require generally enhanced access for researchers to social media data, across all major platforms, via research-specific Application Programming Interfaces (APIs). Such access has been much reduced in recent years: the Facebook API has been severely curtailed; the Instagram API has been discontinued; platforms like WhatsApp provide no API functionality whatsoever. This undermines critical, independent, third-party scrutiny, and means that there is no chance to verify whether the measures against mis- and disinformation that platforms announce from time to time are indeed effective (Bruns, 2019).

Other changes should strengthen institutional and regulatory mechanisms.

At an institutional level, there is a need for substantially increased funding for state and federal electoral commissions, focussing especially on extending their social media campaign monitoring and enforcement activities, and on enabling rapid intervention in case of improper social media campaigning. This must necessarily include additional skills development, ideally in collaboration with Australian research leaders in the field; as the online campaigning activities of legitimate political actors, lobby groups, and fringe activists have evolved rapidly, electoral commissions have struggled to keep up, and it may be necessary to develop dedicated social media monitoring and mitigation teams.

But regulatory settings must also be adjusted. Current blanket prohibitions on paid and targeted online advertising are ill-conceived due to the difficulties of drawing a line between political and non-political content, which leads to uneven and unintended consequences (Kreiss and Perault, 2019). Perversely, this also removes possible tools for countering disinformation. However, consideration should be given to *limiting grounds* for targeting or mandating opt-outs for certain types of profiling and targeting (e.g. on the basis of inferred personality traits).

Finally, we also strongly recommend the introduction of transparency obligations for political campaigners, regarding their data harvesting, matching, and handling activities. At present, political parties and sitting members are exempt from federal and state privacy legislation, which would otherwise impose transparency notice and access obligations. In the interest of citizens' rights, these exemptions should be reconsidered.

References

Broadcasting Services Act 1992 (Cth).

Bruns, A. (2019). After the 'APIcalypse': Social Media Platforms and Their Fight against Critical Scholarly Research. *Information, Communication & Society*, 22(11), 1544–1566.

<https://doi.org/10.1080/1369118X.2019.1637447>

Dobber, T., Ó Fathaigh, R., & Zuiderveen Borgesius, F. (2019). The regulation of online political micro-targeting in Europe. *Internet Policy Review*, 8(4).

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3533232

Duke, J. (2019, May 12) TV networks to run election ads on streaming apps during blackout. The Sydney Morning Herald. <https://www.smh.com.au/business/companies/tv-networks-to-run-election-ads-on-streaming-apps-during-blackout-20190512-p51mkb.html>

Elections Modernization Act, SC 2018, c 31.

Honest Ads Act, S 1989, 115th Congress (2017-2018).

Leerssen, P., Ausloos, J., Zarouali, B., Helberger, N., de Vreese, C.H., (2019), Platform Ad Archives: Promises and Pitfalls. *Internet Policy Review*, 8(4).

McKenna, K. Y., & Bargh, J. A. (2000). Plan 9 from cyberspace: The implications of the Internet for personality and social psychology. *Personality and social psychology review*, 4(1), 57-75.

Meduza. (2020, June 4). YouTube deletes homophobic campaign video created by media organization linked to 'Russian troll factory'. <https://meduza.io/en/news/2020/06/04/youtube-deletes-homophobic-campaign-video-created-by-media-organization-linked-to-russian-troll-factory>

Privacy Act 1988 (Cth).

Privacy and Data Protection Act 2014 (Vic).

Stevens, A. (2017, August 2). Personalization is King! Gather These 5 Types of Data and Take the Throne. *Nationbuilder.com*. https://nationbuilder.com/personalization_is_king_gather_these_5_types_of_data_and_take_the_throne

Tufekci, Z. (2014). Engineering the Public: Big Data, Surveillance and Computational Politics. *First Monday*, 19(7), 1-14.

Vkontakte. (N.d.) Requirements on Election Campaign Materials.

https://vk.com/ads?act=office_help&id=53516181&oid=-19542789&terms=1

Van Hoboken, J., Appelman, N., Ó Fathaigh, R., Leerssen P., McGonagle, T., van Eijk, N., & Helberger, N. (2019). De verspreiding van desinformatie via internetdiensten en de regulering van politieke advertenties [The dissemination of disinformation via internet services and the regulation of political advertisements] [Report]. <https://www.rijksoverheid.nl/documenten/rapporten/2019/10/18/de-verspreiding-van-desinformatie-via-internetdiensten-en-de-regulering-van-politieke-advertenties>

Ward, K. (2018). Social Networks, the 2016 US Presidential Election, and Kantian Ethics: Applying the Categorical Imperative to Cambridge Analytica's Behavioral Microtargeting. *Journal of Media Ethics*, 33(3), 133-148.

Bios

Prof. Axel Bruns is a Professor in the Digital Media Research Centre at Queensland University of Technology in Brisbane, Australia, and a Chief Investigator in the ARC Centre of Excellence for Automated Decision-Making and Society. His books include *Are Filter Bubbles Real?* (2019) and *Gatewatching and News Curation: Journalism, Social Media, and the Public Sphere* (2018), and the edited collections *Digitizing Democracy* (2019), the *Routledge Companion to Social Media and Politics* (2016), and *Twitter and Society* (2014). His current work focusses on the study of user participation in social media spaces such as Twitter, and its implications for our understanding of the contemporary public sphere, drawing especially on innovative new methods for analysing 'big social data'. He served as President of the Association of Internet Researchers in 2017–19. His research blog is at <http://snurb.info/>, and he tweets at @snurb_dot_info.

A/Prof. Daniel Angus is Associate Professor of Digital Communication in the Digital Media Research Centre at Queensland University of Technology in Brisbane, Australia, and an Associate Investigator in the ARC Centre of Excellence for Automated Decision-Making and Society. His research focuses on the development of visual computational analysis methods for communication data, with a specific focus on interactional data. His novel computational methods have improved our understanding of the nature of communication in medical consultations, conversations in aged care settings, television broadcast, social media, and newspaper reporting. Daniel has been involved in computer science research for 15 years and contributes regularly to media and industry on the impact of technology on society.

Dr. Timothy Graham is Senior Lecturer in Digital Media at the Queensland University of Technology. His research combines computational methods with social theory to study online networks and platforms, with a particular interest in online bots and trolls, disinformation, and online ratings and rankings devices. He is a Chief Investigator of an ARC Discovery Project that utilises large-scale hyperlink network analysis and web experiments to comparatively assess the web presence of 10 countries. He develops open source software tools for social media data analysis, and has published in journals such as *Information, Communication & Society*, *Information Polity*, *Big Data & Society*, and *Critical Social Policy*.

Dr. Sofya Glazunova is a postdoctoral research fellow at the Digital Media Research Centre at Queensland University of Technology, Brisbane, Australia. Sofya is specialising on digital political communication with the emphasis on activists' resistances online, investigative journalism, and propaganda in the digital public sphere in Russia and beyond. Her recent publications include "Four populisms of Alexey Navalny. An analysis of Russian non-systemic opposition discourse on YouTube" (2020). Her current research looks at Russia's digital information warfare and how Russian pro-government television channels use social media affordances to disseminate and engage digital publics in strategic government discourses.

Tegan Cohen is a PhD candidate in the Queensland University of Technology Faculty of Law, in Brisbane, Australia. Her current research looks at privacy in the context of democratic processes, with a particular focus on the implications of current and emerging data-driven campaigning practices for voter privacy. Before commencing a PhD, Tegan practised law in Australia and the UK, specialising in privacy, intellectual property and technology law.

QUT Digital Media Research Centre

The QUT Digital Media Research Centre (DMRC) conducts world-leading communication, media, and law research for a flourishing digital society. One of only nine University Research Centres established at QUT in 2019, it is one of the top Australian centres for media and communication research, areas in which QUT has achieved the highest possible rankings in the national research quality assessment exercise ERA, and it is closely linked with the School of Communication.

The Centre incorporates the QUT node of the Australian Research Council (ARC) Centre of Excellence for Automated Decision-Making & Society (ADM+S), and participates in the ARC Centre of Excellence for the Digital Child, headquartered in the Faculty of Education.

Working across five new programs and drawing together people from five Schools and three Faculties, the DMRC investigates the digital transformation of the media industries, the challenges of digital inclusion and governance, the growing role of AI and automation in the information environment, and the role of social media in political polarisation. The DMRC has an international reputation for both critical and computational methods, and has access to cutting-edge research infrastructure and capabilities in areas such as social media analytics and critical simulation.

We actively engage with industry and international partners in Australia, Europe, Asia, the US, and South America; and we are especially proud of the dynamic and supportive research training environment we provide to our many local and international graduate students.

The DMRC is also a member of the global Network of Centres – a group of academic institutions with a focus on interdisciplinary research on the development, social impact, policy implications, and legal concerning the Internet.

For further information, see: <http://research.qut.edu.au/dmrc>