EMC Submission No. 89
Received 30 September 2020

Office of the Victorian Information Commissioner

t 1300 00 6842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

D20/16367

30 September 2020

Lee Tarlamis OAM MP
Chair
Electoral Matters Committee
Parliament House, Spring Street
EAST MELBOURNE VIC 3002

***By email only**: emc@parliament.vic.gov.au*

Dear Mr Tarlamis,

Inquiry into the impact of social media on elections and electoral administration

Thank you for your invitation of 11 August 2020 to make a submission to the Electoral Matters Committee of the Parliament of Victoria's (**the Committee**) inquiry into the impact of social media on elections and electoral administration (**inquiry**).

My office, the Office of the Victorian Information Commissioner (**OVIC**) is the primary regulator for information privacy, information security and freedom of information in Victoria, administering both the *Privacy and Data Protection Act 2014* (**PDP Act**) and the *Freedom of Information Act 1982*. Relevant to this inquiry, my office also has a function under the *Electoral Act 2002* and the *City of Melbourne Act 2001* to consider whether the public interest in the protection of privacy outweighs requests for access to electoral information received under those Acts.

In preparing this submission, my office has considered the points you specifically raised in your invitation, as well as the terms of reference of the inquiry. We have responded to the points that relate most directly to OVIC's jurisdiction.

My office's submission raises the following key points:

- The increasing use of targeted political advertising in modern elections highlights a current lack of privacy regulation for registered political parties in Australia;
- Using targeted political advertising to influence certain demographics within the community – through the incremental misuse of individuals' personal information – not only diminishes the right to privacy but also limits potential for informed and meaningful political debate ahead of elections;
- The over-collection of voters' personal information by political parties can increase cyber security threats, as well as the potential for misuse of information to negatively impact election outcomes; and
- Amendments to the PDP Act to protect publicly available personal information may go some way to addressing the ability for political parties to unfairly influence the community via targeted political advertising.

How are candidates, political parties and others using social media and online advertising in Victorian elections?

1. Recent reports suggest that Australian political parties routinely combine the personal information of voters from various sources to better target campaigning.[1] Reports also suggest the use of 'email trackers' by political parties, "potentially letting the sender know a range of details about the recipient."[2] Email tracking is a surveillance technique, widely-used by marketers and newsletter services, usually involving a small 1x1 pixel image that is the same colour as the email background (and therefore difficult to detect), embedded into the body of an email.[3] When the recipient opens the email, the tracking client recognises that pixel has been called from a server by the email client, as well as where and on what device.[4]

2. The practices detailed in these reports highlight a larger issue, in the current lack of privacy regulation for registered political parties in Australia. Registered political parties are exempt from the federal *Privacy Act 1988*. In Victoria, Members of Parliament are exempt from the obligations under the Information Privacy Principles (**IPPs**).[5]

3. Given this lack of regulation, it is difficult to clearly establish the online practices of political parties particularly in relation to their collection, use and disclosure of voters' personal information for online political campaigning.

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

Rise of targeted political advertising

4. Commentary around the influence of social media on elections, primarily through Facebook, has increased markedly since the 2016 US Presidential election.

5. Targeted advertising is effective at reaching its intended audience, leading to the growth in use of social media by political campaigns,[6] over traditional broadcast or print media – which by its nature can only be broadly targeted to demographics.

6. Recent commentary describes Facebook as a "narrowcaster…(deriving) its power in the marketplace from its ability to acquire tremendous amounts of data about people (they don't have to be Facebook users), which it then uses to sell targeted ads based on people's personalities, affiliations, demographics, and other very specific attributes."[7] OVIC considers this type of consumer profiling an incremental misuse of individuals' personal information, posing both individual and societal consequences.

7. The collection of the individuals' data allows advertisers to narrowly segment users by a diverse range of criteria. This ability extends to political advertising and social media posts, which have

[1] See, Byron Kaye et al., 'Political parties combine social media data with electoral roll information' (6 May 2019), (Reuters (Computerworld), online) available at: https://www.arnnet.com.au/article/661237/political-parties-combine-social-media-data-electoral-roll-information/.
[2] Ariel Bogle, 'How the Australian federal election invaded your inbox with email tracking tools' (2 May 2019), (ABC Science, online), available at: https://www.abc.net.au/news/science/2019-05-02/email-tracking-parties-lobby-groups-australian-federal-election/11056186.
[3] Brian Merchant, 'How Email Open Tracking Quietly Took Over the Web' (12 November 2017), (Wired, online), available at: https://www.wired.com/story/how-email-open-tracking-quietly-took-over-the-web/.
[4] Ibid.
[5] Under section 13(g) of the PDP Act.
[6] Wan-Shiou Yang et al., 'Mining Social Networks for Targeted Advertising,' (4 January 2006),in *Proc. 39th Annual Hawaii International Conference on System Sciences (HICSS'06),* available at: https://ieeexplore.ieee.org/abstract/document/1579567.
[7] Sue Halpern, 'The Problem of Political Advertising on Social Media' (24 October 2020), (The New Yorker, online), available here: https://www.newyorker.com/tech/annals-of-technology/the-problem-of-political-advertising-on-social-media.

been ever-narrowly targeted. Former Facebook executives have admitted that this has enabled misinformation to spread widely on the platform,[8] with increasingly tragic consequences.[9]

8. When information is shown to some and not all online (whether it is misinformation or not), this can have the effect of limiting meaningful political debate among citizens, and of freedom of thought and freedom of expression. This can also lead to a phenomenon often referred to as *cyberbalkanisation*, whereby "people seek out only like-minded others and thereby close themselves off from ideological opposition, alternative understandings, and uncomfortable discussions."[10] *Cyberbalkanisation* can lead to an online environment in which there is no collective body public, but rather a disparate set of interest groups without the shared sense of community representative democracy relies upon for peaceful exchange of views.[11]

9. From a Victorian perspective, a report into the results of the 2018 Victorian State Election noted that the "unfiltered nature of social media also made it easier to disseminate misinformation. In one instance, online video footage was edited in a way that misrepresented (an election candidate's) stance on the issue of fracking, with the edited footage posted on Facebook and Twitter."[12]

Manipulation and management of content on social media

10. In the United States, legislation has had the effect of shielding most social media platforms from liability for publication of content.[13] Many experts believe it has led to adverse unforeseen consequences since the growth of social media.[14] Comparatively, major social media platforms agreed to a voluntary code of conduct in the EU, to limit the spread of hate speech by reviewing notifications received within 24 hours.[15]

11. To address the spread of hate speech and misinformation, Facebook and other social media platforms rely heavily on automated tools to manage content posted by advertisers and other users. These tools, layered upon one another over time, have led to a confusing network of automated decision-making that even the platforms themselves do not understand well.[16] Attempts to moderate inflammatory and vile content on social media both by algorithms[17] and

---

[8] See, Alison Durkee, 'Facebook Engineer Resigns, Says Company On 'Wrong Side Of History' As Internal Dissent Grows' (8 September 2020), (Forbes, online) available at: https://www.forbes.com/sites/alisondurkee/2020/09/08/facebook-engineer-resigns-company-on-wrong-side-of-history-internal-employee-dissent-grows/#702919343794. See also, James Vincent, 'Former Facebook exec says social media is ripping apart society' (11 December 2017), (The Verge, online) available at: https://www.theverge.com/2017/12/11/16761016/former-facebook-exec-ripping-apart-society.

[9] Paul Mozur, 'A Genocide Incited on Facebook, With Posts From Myanmar's Military,' (15 October 2018), (The New York Times, online), available here: https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.

[10] Lori A. Brainard, 'Cyber-communities' (2009), 598, in Helmut K. Anheier & Stephan K. Toepler (Eds.), *International encyclopedia of civil society* (New York, NY: Springer Science & Business Media), available at: https://www.springer.com/gp/book/9780387939940.

[11] A related concept was developed by Timur Kuran and Cass Sunstain called 'availability cascades,' whereby a new idea or insight gains rapid currency on social media through its simplicity and its apparent insightfulness, setting up a self-reinforcing cycle because other people within the network have adopted it and it seems – superficially at least – to make sense. Kuran and Sunstein argue this is impossible without social media. Such cascades facilitate the spread of misinformation and increase the spread of populist messaging online. See, Timur Kuran and Cass Sunstain, 'Availability Cascades and Risk Regulation,' (1999) *Stanford Law Review*, 5(4), available at: https://papers.ssrn.com/sol3/papers cfm?abstract_id=138144.

[12] Bella Lesman et al., *The 2018 Victorian State Election*, (June 2019) Department of Parliamentary Services, Research and Inquiries Unit, Research Paper No. 2, 5, available here: https://www.parliament.vic.gov.au/publications/research-papers/summary/36-research-papers/13892-an-analysis-of-the-victorian-state-election.

[13] See, Daisuke Wakabayashi, 'Legal Shield for Social Media Is Targeted by Trump,' (28 May 2020), (The New York Times, online) available at: https://www.nytimes.com/2020/05/28/business/section-230-internet-speech.html.

[14] Ibid.

[15] Alex Hern, 'Facebook, YouTube, Twitter and Microsoft sign EU hate speech code'(31 May 2016), (The Guardian, online), available at: https://www.theguardian.com/technology/2016/may/31/facebook-youtube-twitter-microsoft-eu-hate-speech-code.

[16] See, for example, Thomas Macaulay, 'Facebook again admits to wrongly sharing user data with third-party apps' (2 July 2020), (The Next Web, online), available at: https://thenextweb com/neural/2020/07/02/facebook-again-admits-to-wrongly-sharing-user-data-with-third-party-apps/.

[17] See, for example, Markena Kelly, 'Facebook proves Elizabeth Warren's point by deleting her ads about breaking up Facebook,' (11 March 2019), (The Verge, online), available at: https://www.theverge.com/2019/3/11/18260857/facebook-senator-elizabeth-warren-campaign-ads-removal-tech-break-up-regulation.

humans have thus far been mixed. Research suggests that the manual moderation of hateful content on social media exposes humans to unacceptable psychological risks.[18]

12. Even where moderation exists, the pace of moderation in comparison to the 'viral' nature of some content means that the content spreads widely, and quickly. Some progress has been reported following the introduction of the voluntary EU code of practice, with Facebook assessing notifications of hateful content in less than 24 hours in 58 per cent of cases.[19] However, in the context of the modern election campaigning and the demonstrated potential for an entire demographic of voters to be influenced by targeted political advertising on social media, 24 hours can seem a very long time indeed.

Increasing use of data breaches and cyber-attacks

13. The low-cost of targeting on social media platforms, combined with the increased sophistication of adversary nation-states, has also led to foreign interference in elections. Researchers from Oxford University determined that half of the political 'news' stories shared by legitimate social media users during the 2016 US Presidential Election originated from bots or 'junk' sources, most of which were orchestrated by foreign agencies.[20]

14. Since this time, research on artificially generated language has made extraordinary advances, suggesting that in future elections, foreign regimes may not need to rely on humans to directly implement this interference but instead will use swarms of AI-generated 'personalities.' These personalities are expected to reflect the identities of particular community groups, to offer targeted messages to those groups, undetectable from the messages they get from actual community members.[21]

15. Given that political parties in Victoria have access to a significant amount of voters' personal information made up of data from the electoral roll, social media, and third-party data brokers, there is the increasing potential for inappropriate uses of that information, whether by accident or design. In Australia, there have been instances of systems operated or used by Australian political parties exposing personal information, or failing to implement appropriate information security measures, given the cyber-security risks attached to large troves of voters' personal information.[22]

16. As well as the risk of personal information held by political parties being accessed by unauthorised third parties, such as foreign states, and used to manipulate elections,[23] political parties have been victim to cyber-attacks in the recent past.[24] Without appropriate information security measures in place, this risk may lead to significant issues in future elections and online political campaigning. While political parties are likely to rely on consultants to assist them with security, the resources of

[18] Andrew Arsht and Daniel Etcovitch, 'The Human Cost of Online Content Moderation,' (2 March 2018), (*Harvard Journal of Law and Technology*, synopsis available via The Jolt, online), available at: https://jolt.law.harvard.edu/digest/the-human-cost-of-online-content-moderation.
[19] Alistair Macdonald and Julia Fioretti, 'Social media firms have increased removals of online hate speech: EU,' (1 June 2017), (Reuters, online), available at: https://www.reuters.com/article/us-eu-hatespeech-idUSKBN18S3FO.
[20] Philip N. Howard, *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives*, (2020) (Yale University Press), 12.
[21] See, Jonathan Freedland, 'Disinformed to Death,' (20 August 2020), (The New York Review of Books, online), available here: https://www.nybooks.com/articles/2020/08/20/fake-news-disinformed-to-death/.
[22] Jackson Gothe-Snape, 'Labor's voter-tracking practices exposed by a simple Google search,' (23 October 2018), (ABC News, online), available at: https://www.abc.net.au/news/2018-10-23/labor-campaign-central-database/10338998. See also, Richard Willingham, 'Private data of thousands of Victorian Liberal Party members 'leaked and misused',' (17 April 2016), (ABC News, online) available at: https://www.abc.net.au/news/2018-04-17/private-details-of-liberal-party-members-used-in-internal-fight/9663968 and Amy Remeikis, 'Australian security services investigate attempted cyber-attack on parliament,' (8 February 2019), (The Guardian, online), available at: https://www.theguardian.com/australia-news/2019/feb/08/asio-australian-security-services-hack-data-breach-investigate-attempted-cyber-attack-parliament.
[23] David Wroe, 'Democracy at stake': Parties warned Australia at risk of US-style cyber manipulation (25 April 2019) (Sydney Morning Herald, online), available at: https://www.smh.com.au/federal-election-2019/democracy-at-stake-parties-warned-australia-at-risk-of-us-style-cyber-manipulation-20190424-p51gu3.html
[24] Ibid.

nation-states with an interest in influencing elections are very sophisticated, increasing the risk of foreign interference in future elections.

Should the Victorian Government introduce more regulation in this area? Are there other things the government should be doing?

17. In 2010, the Australian Law Reform Commission (**ALRC**) considered the exemption for registered political parties, political acts and practices in their inquiry into Australian privacy law and practice.[25] The ALRC took the view that:

    "*(u)nless there is a sound policy reason to the contrary, political parties and agencies and organisations engaging in political acts and practices should be required to handle personal information in accordance with the requirements of the Privacy Act 1988 (Cth).*"[26]

18. The Office of the Australian Information Commissioner, which administers the federal *Privacy Act 1988*, has recently commented that the exemption for political parties "came into operation in a world before social media, digital communications and the internet had really taken off."[27]

Protecting information collected from social media

19. OVIC is of the view that the personal information of Victorians collected from public social media accounts should be subject to the privacy and information security protections under the PDP Act.

20. Currently, section 12 of the PDP Act excludes 'publicly available information' from either privacy or information security regulation. Social media has increased the volume of public information online and available to potentially be collected for the purposes of better targeting political advertising. Protecting publicly available information under the PDP Act may go some way to addressing the ability for political parties to unfairly influence the community via targeted political advertising and increase potential for wider meaningful debate around election priorities in the public sphere.

I thank you again for the opportunity to make a submission to the Committee's inquiry. I have no issues with my submission being published on the Committee's website without further reference to me.

If you have any concerns regarding the above, please don't hesitate to get in touch with me directly at [redacted], or my colleague, Emily Arians, Senior Policy Officer at [redacted]

Yours sincerely

[redacted]

Sven Bluemmel
Information Commissioner

[25] ALRC, For Your Information: Australian Privacy Law and Practice (ALRC Report 108), available here: https://www alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/.
[26] Ibid, at 41 54.
[27] Angelene Falk, '2020 Vision: Challenges and opportunities for privacy regulation' (Keynote address by Australian Information and Privacy Commissioner, at the International Association of Privacy Professionals Australia and New Zealand 2019 Summit in Sydney), available here: https://www.oaic.gov.au/updates/speeches/2020-vision-challenges-and-opportunities-for-privacy-regulation/.