Mitigating microtargeting: Political microtargeting law in Australia and New Zealand

Melissa-Ellen Dowling
Jeff Bleich Centre, College of Business, Government and Law, Flinders University, Adelaide, South Australia, Australia

Abstract
To the detriment of liberal democracy, governments have struggled to prevent the exploitation of personal data for voter manipulation in the digital era. Laws pertaining to political microtargeting are often piecemeal and tend to derive from a combination of laws on electoral advertising and privacy. Evidence indicates that this approach is insufficient to curtail microtargeting. However, little is known about the regulation of microtargeting outside of the European and US contexts within which the bulk of anti-microtargeting research has been undertaken. Accordingly, this paper aims to shed light on the preparedness of the law in Australia and New Zealand to mitigate the potential harms of political microtargeting. A comparative analysis of legislation pertaining to microtargeting is therefore undertaken using a blended approach of comparative law and content analysis. This paper: (1) identifies current legislation relevant to microtargeting in Australia and New Zealand; (2) assesses patterns of similarity and difference between each country’s laws in relation to microtargeting; and (3) evaluates the preparedness of current legislation to curtail microtargeting in an evolving social media landscape. It finds that in both countries, legislation is sufficiently robust to mitigate microtargeting in some limited circumstances, but a cohesive regulatory approach is needed to constrain the most insidious microtargeting operations.

Keywords: comparative law, data-driven campaigning, digital regulation, political microtargeting, social media.

1. Introduction
Microtargeting has been a fixture of political campaigning for decades, yet, to the detriment of liberal democracy, governments and industry have struggled to pre-empt and prevent the exploitation of personal data for voter manipulation (Barocas, 2012). As researchers point out, laws pertaining to political microtargeting are often “piecemeal” and tend to derive from a combination of laws on electoral campaigning, data protection, and privacy (Cavaliere et al., 2021, p. 4). This haphazard regulation leaves “gaps and loopholes” that microtargeters can leverage (Cavaliere et al., 2021, p. 4). Others note that policymakers have been “slow” to acknowledge the array of challenges that data-driven campaigning poses for democracies (Bennett & Lyon, 2019, p. 8).

Algorithms, cookies, invisible pixels, and data mining tools are just some of the digital implements that enable online political microtargeting: the power to use data to identify and persuade voters to alter their political preferences and/or election conduct (Information Commissioner’s Office, 2022). This technology is advancing rapidly which is making it easier to analyze and connect multiple data points on individuals using big data. The computational techniques deployed in analyzing online discourse through natural language processing techniques are also becoming more sensitive and sophisticated in their ability to detect human emotion and contextual meaning (Zad et al., 2021). These techniques have already been applied to large datasets in other contexts (e.g., health research) (Stewart & Velupillai, 2021) and therefore have clear potential to be applied for microtargeting to identify vulnerable targets as well as generate automated messages.

Correspondence: Melissa-Ellen Dowling, Flinders University, Sturt Rd, Bedford Park, Adelaide, SA 5042, Australia. Email: melissaellen.dowling@flinders.edu.au
* Conflict of interest: The author has no conflict of interest to disclose.
† An alternative version of this paper titled, “Next Generation Political Microtargeting: Pre-Emptive and Preventative Policy Imperatives” was presented at the National Security College’s Surprise Tech Forum 2022 (Futures Hub, Australian National University).

Accepted for publication 10 November 2023.

© 2023 The Authors. Regulation & Governance published by John Wiley & Sons Australia, Ltd.
This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.
Immersive technologies are predicted to evolve and deepen users’ digital experience. In doing so, greater opportunities are likely to emerge for a variety of actors to surreptitiously exert political influence on voters within these immersive environments. Digitization has already afforded additional scope to a broader range of actors to conduct anonymous, illegal, or unethical microtargeting campaigns with a lowered possibility of attribution. The types of actors that either have deployed or could potentially deploy microtargeting include political parties, companies, individuals (e.g., wealthy party donors), interest-groups (e.g., climate change, anti-abortion), and state actors (e.g., foreign governments).

The dangers of democratic erosion through microtargeting are well-documented (see e.g., Bennett & Lyon, 2019; Borgesius et al., 2018; Dawson, 2021; Dobber et al., 2019; Dowling, 2022; Endres & Kelly, 2018; Lavigne, 2021; Witzleb & Paterson, 2021), and this growing threat signals the need for strong regulatory mechanisms and capabilities to protect democracies from political microtargeting.

One possible barrier to microtargeting is data protection law, which has become increasingly robust around the globe. The European Union’s General Data Protection Regulation (GDPR) was a hallmark step toward regulating microtargeting through increasing data controllers’ responsibilities to protect data (Buttarelli, 2016; Mantelero, 2021). If microtargeters cannot freely access users’ data, then presumably microtargeting—a practice that is reliant on user data—cannot be sustained.

Research on political microtargeting in the European context highlights that privacy law, namely the GDPR, provides data subjects with more power to control who collects their data and how it is used, and it has strict rules protecting political opinions as a form of personal data. It is typically more difficult to acquire political data on individuals without their consent, but there are exceptions for political parties in some circumstances (Borgesius et al., 2018). However, there are no specific laws about political microtargeting in the GDPR. Even where GDPR protections might theoretically curtail data collection for the purposes of microtargeting, compliance with, and enforcement of, the law is not guaranteed (Dobber et al., 2019). Further, protection of democracy is but a tangential possibility of the GDPR, and is, as Brkan (2022, p. 355) explains, merely “incidental.” Though, EU policymakers are, at the time of writing, debating new regulatory measures to improve transparency in elections and protect democracy from political microtargeting. It also remains unclear to what extent political microtargeting is protected by the European Convention on Human Rights, with scholars suggesting that perhaps it could be treated as a form of political communication and therefore a highly protected form of expression (Dobber et al., 2019). Thus, evidence from the European case indicates that data protection regulation may not be enough to curtail microtargeting due to tension between free political speech and privacy wherein freedom of expression is sacrosanct (Cavaliere et al., 2021; Dobber et al., 2019). Similarly, in the United States, the First Amendment is cited as a barrier to enacting effective federal data protection policy (Balkin, 2017; Bulka, 2022; Rhum, 2020) which, by extension, limits controls on microtargeting.

While research on the regulation of political microtargeting in the European context is well underway, we do not yet know enough about the regulation of political microtargeting in other liberal democracies (Blasi Casagran & Vermeulen, 2021; Borgesius et al., 2018; Dobber et al., 2019; King, 2022; Kruschinski & Haller, 2017; Nenadić, 2019; Papakyriakopoulos et al., 2018; Witzleb & Paterson, 2021). Furthermore, while studies of data-driven campaigning give insight into the dynamics of the scope and risks of microtargeting (see e.g., Anstead, 2017; Bennett & Gordon, 2021; Borgesius et al., 2018; Ferrer, 2020; Kefford, 2021; Witzleb et al., 2020), there is a dearth of insight into the potential impact of changing trends in social media use on anti-microtargeting measures.

Accordingly, this paper aims to shed light on the preparedness of current law in Australia and New Zealand to mitigate political microtargeting. This article’s research questions are: what national legislation is in place in Australia and New Zealand that has a significant bearing on political microtargeting? And, how equipped is the existing legislation to mitigate microtargeting? A comparative analysis of legislation pertaining to microtargeting is therefore undertaken. After providing background on the nature of the microtargeting threat, the paper will: (1) identify current legislation relevant to microtargeting in Australia and New Zealand and describe the paper’s research methods; (2) assess patterns of similarity and difference between each country’s laws in relation to microtargeting; and (3) evaluate the preparedness of current legislation to curtail microtargeting in an evolving social media landscape.
1.1. Political microtargeting and democracy

To understand the legal barriers to microtargeting, it is necessary to appreciate the procedural and normative contexts that shape the regulatory environment on data protection and elections. The practice of elections creates conditions within which political microtargeting is incentivized, yet there is an ostensible normative shift toward protecting individuals’ privacy which signals that microtargeting is not an acceptable practice.

Although profiling groups of voters has been common practice in political campaigning for decades, social media has enabled political campaigning firms to acquire greater access to voters through political microtargeting (Bennett & Lyon, 2019; Borgesius et al., 2018; Dawson, 2021; Dobber et al., 2019; Endres & Kelly, 2018; Lavigne, 2021; Witzleb & Paterson, 2021). By harvesting data from social media platforms and acquiring identifiable data from other sources such as data brokers, microtargeting firms can deploy machine learning to build profiles of individual voters which they can then use to generate and share tailored material to influence those users. Data-driven microtargeting has three broad stages: (1) data collection; (2) segmentation and profiling; and (3) tailored messaging (Hersh, 2015). It is therefore a more personalized and individual-based approach to political influence than analogue or demographic campaigning.

Stage one of microtargeting involves collecting information about voters (Brkan, 2022). In liberal democracies which enshrine individual rights and liberties, data collection must be balanced with individuals’ privacy. Data can be collected in many different ways and from a wide range of sources. For example, it can be obtained from data brokers, acquired through social media tracking, online quizzes, and records of consumer behavior. During stage two, microtargeters segment the data and profile users. While population segmentation into demographics is common in political campaigning and is not unique to microtargeting, a microtargeting operation relies on more personal information specific to individual voters. Such information can be used to profile voters in ways that potentially enable their messaging to be more effective. For example, Cambridge Analytica profiled individuals using a psychographic framework and segmented individuals into categories based on personality type. Individuals with different psychological profiles received different political messages designed to target their perceived sensitivities (CA, 2016; Hinds et al., 2020; Wylie, 2019). Thus, stage three of microtargeting entails designing and communicating tailored messages that play on targets’ political preferences, moral views, consumer habits, family life, and so on.

However, not all data-driven campaigning is as individualized as microtargeting. As Glenn Kefford et al. (2022) point out, political parties use data-driven campaigning, but most campaigns stop short of microtargeting. Instead, their empirical research finds that party campaigns tend to focus more on geographic or demographic categories of voters through “narrowcasting” (Kefford et al., 2022). In another study, Kefford (2021) identifies funding limitations as a barrier to party microtargeting in the Australian context. Likewise, in their research on microtargeting in Canada, Bennett and Gordon (2021) find that most Canadian political parties lack the resources to fund “precise content-creation” that separates microtargeting from other forms of campaigning. The distinction is important because microtargeting, as a form of data-driven campaigning, has greater potential to harm democracy than other forms of digital campaigning.

Part of this greater potential for harm stems from the ways in which microtargeting has the capacity to diminish individuals’ agency, reduce trust in democracy, fragment political discourse, spread disinformation, and jeopardize electors’ privacy (Bakir, 2020; Bayer, 2020; Bennett & Lyon, 2019; Borgesius et al., 2018; Burkell & Regan, 2019; Gorton, 2016; Matthes et al., 2022; Witzleb & Paterson, 2021). Yet, these are symptoms of a broader systemic challenge: interference in the electoral process jeopardizes the fundamental structures responsible for societal stability in liberal democracies; the structures of representative and responsible government. If powerful actors can clandestinely manipulate democratic processes at scale, then the target political community effectively cedes sovereignty over its governance. In such scenarios, election outcomes are not organically generated through public political debate and discourse, but engineered by actors external to the political community, or, by domestic actors exerting illegitimate influence over political outcomes.

Public knowledge of such operations thus has the potential to undermine public trust and legitimacy of government and governance to an extent which could generate disorder and induce a conflict or latent conflict social order. As civil war expert Barbara Walter (2022) explains in her research on how civil wars start, hovering between a consolidated democracy and an autocracy (as Walter describes it, an “anocracy”) positions societies in a risk zone for civil war.

© 2023 The Authors. Regulation & Governance published by John Wiley & Sons Australia, Ltd.
More specifically, there are two core and interrelated ways in which political microtargeting can damage liberal democracy: (1) skewed preference formation and articulation and (2) legitimacy erosion (Dowling, 2022). Preference formation is shaped by information environments, and the political preferences electors form are critical to political outcomes since preferences inform political actions. As Jacquelyn Burkell and Priscilla M. Regan (2019, p. 16) observe, microtargeting has the potential to restrict free choice by manipulating electors’ “decisionmaking capacity.” Manipulation of the preference formation process runs counter to aspirational features of liberal democracy of electors being able to develop “enlightened understanding” through which to construct political preferences (Dahl, 2008). However, as I argue elsewhere, tangible changes to preferences rely on an assumption that microtargeting is effective (Dowling, 2022). Yet, the evidence is unclear as to whether political microtargeting is effective in persuading voters to alter their preferences, with studies producing mixed results (Baldwin-Philippi, 2019; Dobber et al., 2021; Endres & Kelly, 2018; Zarouali et al., 2022).

The biggest danger that can arise does not depend on effective persuasion: it just needs to raise doubt over the legitimacy of processes of political participation (such as voting, petitioning, and protesting) and participatory outcomes (such as who is elected). Civil and political destabilization can arise from widespread societal perception at the possibility of influence: trust in government and political processes can be easily undermined even without microtargeting actually altering political outcomes.

2. Methodology

This paper conducts a comparative content analysis of Australia’s and New Zealand’s legislation that is relevant to political microtargeting. I determine relevance based on the extent to which policies concern core aspects of the stages of political microtargeting. The criterion for determining relevance therefore includes the extent to which laws concern privacy and data protection as connected to microtargeting’s data collection phase, and the extent to which legislation concerns the creation and sharing of political material as connected to the tailored messaging phase of microtargeting. Table 1 maps the relevant legislation for microtargeting in Australia and New Zealand. From here, I discuss in more detail the laws that have the most direct relationship to microtargeting: privacy law and electoral law.

Table 1 Legislation most relevant to political microtargeting in AU and NZ

<table>
<thead>
<tr>
<th>Country</th>
<th>Legislation</th>
<th>Purpose</th>
<th>Relevance to microtargeting stages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>Privacy Act (1988)</td>
<td>“An Act to make provision to protect the privacy of individuals and for related purposes.”</td>
<td>Data collection and use</td>
</tr>
<tr>
<td>Australia</td>
<td>Commonwealth Electoral Act (1918)</td>
<td>“An Act to consolidate and amend the law relating to parliamentary elections and for other purposes.”</td>
<td>Tailored political messaging</td>
</tr>
<tr>
<td>Australia</td>
<td>Commonwealth Electoral (Authorisation of Voter Communication) Determination (2021) (CED)</td>
<td>“This instrument sets out: requirements for notifying particulars in relation to a communication for the purposes of the Electoral Act …” (Electoral Commissioner, 2021).</td>
<td>Tailored political messaging</td>
</tr>
<tr>
<td>Australia</td>
<td>National Security Legislation Amendment (Espionage and Foreign Interference) Act (2018)</td>
<td>“An Act to amend the criminal law and to provide for certain matters in relation to the foreign influence transparency scheme, and for related purposes.”</td>
<td>Data collection and use</td>
</tr>
<tr>
<td>New Zealand</td>
<td>Privacy Act (2020)</td>
<td>“The purpose of this Act is to promote and protect individual privacy …”</td>
<td>Tailored political messaging</td>
</tr>
<tr>
<td>New Zealand</td>
<td>Electoral Act (1993)</td>
<td>“An Act to reform the electoral system …”</td>
<td>Data collection and use</td>
</tr>
</tbody>
</table>

© 2023 The Authors. Regulation & Governance published by John Wiley & Sons Australia, Ltd.
Methods of comparative law and content analysis guide the analysis. The paper deploys methods of comparative law to identify “similarities and differences between multiple legal data points” by analyzing the “content, meaning, and application” of the laws under assessment (Eberle, 2011, p. 61). Both comparative law and sociology’s content analysis approaches recognize the intersubjectivity of texts and the symbiotic role of culture in text creation and interpretation (Krippendorff, 2004). Note too, that aligning with the critical approach of content analysis, that the qualitative data are unavoidably infused with researcher bias as a reflection of the researcher’s enculturation and worldview. This does not invalidate the study, but rather adds another layer of complexity to the embeddedness of texts within cultures as part of an interactive and interpretive system.

Australia and New Zealand were chosen for this comparative study due to their shared socio-political traditions and lack of research on their microtargeting laws. As common law systems, Commonwealth states, liberal democracies, and parliamentary democracies, the countries share legal traditions and socio-political values that enable comparison without exploration of markedly different contextual variables. They also form part of the Anglosphere which has a historical and ongoing pattern of cooperation on mutual challenges (Legrand, 2015, 2016; Vucetic, 2011). Since the countries form part of the Anglosphere, understanding potential opportunities for cooperation and knowledge-sharing has the potential to strengthen the Anglosphere and enhance liberal democratic protections more broadly. Patterns identified in this study might reflect common regulatory gaps, similar legal approaches, shared societal values, or reveal differences that could facilitate mutual learning across the Anglosphere network. To also reduce variation in variables, this study analyses top-level legislation. This means that for Australia, only federal legislation is analyzed, which allows direct comparison with New Zealand’s unitary system. This does not materially distort the analysis for the Australian case, since, in Australia, federal elections and referendums are regulated by federal legislation. This federal focus limits the discussion in this article to microtargeting that could occur in relation to federal elections and referendums. However, where there is a prominent deviation in state law from federal law, it will be noted.

This paper analyses legislation but acknowledges the pivotal contribution of case law in the common law countries studied to shaping the overall preparedness of “the law” more broadly in mitigating microtargeting. The legislation referred to throughout this paper has and is subject to the court’s interpretation. Many social media platforms also enact initiatives to limit the spread of misinformation and disinformation which may assist in curtailing online microtargeting (see e.g., Tan, 2022). Yet, limiting this study to analysis of legislation enables an initial broad scoping of relevant law to support future studies that can then go on to subsequently assess how the provisions identified here have been implemented.

3. Discussion

Political microtargeting lacks coherent and direct regulation in Australia and New Zealand. Instead, constraints on political microtargeting must stem from piecemeal provisions that tend to manifest most prominently in privacy legislation and political advertising law. Significantly, none of the relevant legislation refers to microtargeting, although Australia’s Privacy Act provides some guidance with respect to “direct marketing” which is related to microtargeting. While the privacy and advertising provisions identified in this article can theoretically limit microtargeting in some circumstances, the legislation is not designed with mitigating microtargeting in mind. Consequently, the piecemeal approach lacks sufficient tailoring to the political microtargeting problem within a digital world, but fortunately still has some power to limit the ill effects of microtargeting.

3.1. Stage one: Data collection

The first stage of a microtargeting operation typically involves collecting data on the potential targets. For microtargeting, some of the most valuable data is personal information about individuals’ beliefs, ethnicity, income, family life, and association membership. Crucially, without personal information on voters, microtargeting cannot occur at the fine-grained level that makes it microtargeting. Law regulating the collection of individuals’ personal information is therefore highly relevant in the context of microtargeting. In Australia and New Zealand, privacy protection laws regulate entities’ collection of personal information. The laws are designed in the spirit of protecting individuals’ information and they confer an array of obligations on entities that collect, store, and use
personal information. Privacy protection legislation is comparably robust in Australia and New Zealand. Likewise, the content of the legislation demonstrates a high degree of homogeneity across the countries. However, some key differences distinguish the laws in ways that potentially have a bearing on the mitigation of microtargeting, particularly regarding exempt entities and the circumstances of consent.

3.1.1. What data to collect?

3.1.1.1. Personal information. Australia and New Zealand’s privacy laws apply to “personal information,” and the legislation in each country defines personal information similarly. Australia’s Privacy Act (1988) (Cth)(s 6) defines personal information as “information or an opinion about an identified individual, or an individual who is reasonably identifiable.” An individual is deemed by the Act to be a “natural person.” The explanatory material for the provisions notes that personal information can include a vast array of information such as a person’s address, occupation, physical description, religious beliefs, political beliefs, and asset holdings (Explanatory Memorandum to the Privacy Bill 1988 (Cth)). To be reasonably identifiable means that personal information can include information wherein the person is not identified by name but could otherwise be identified based on the information.

According to New Zealand’s Privacy Act (2020) (s 7(1)), personal information is “information about an identifiable individual.” This means “any information that relates to a living, identifiable being,” which aligns with the Australian definition’s focus on natural persons. Also similar to the Australian legislation, is the stipulation that the individual does not necessarily need to be named in order to be identifiable, “as long as they are identifiable in other ways … or if their identity could be pieced together” (Privacy Commissioner, 2020).

The laws that deem identifiable information as personal information have the potential to either enable or constrain microtargeting, depending on how fine-grained the campaign is. Information that is not about an identifiable individual is not regulated by the Australian privacy law (see s 6(1)), which means that information about individuals which is “de-identified” is fair game for microtargeters. While this limits how fine-grained profiling and messaging can be in the subsequent stages of an operation, technology allows for online tailored messaging without identifying an individual. This means that a less personalized (yet more tailored than demographic targeting) form of microtargeting is still possible without information that is regulated by the Privacy Act (1988) (Cth). While New Zealand’s Privacy Act (2020) does not refer to de-identified information explicitly, it nonetheless encourages organizations to ensure that individuals are “not identified” where possible (privacy principle 10). This is consistent with the legislation’s aims of reducing the amount of personal identifiable information held by organizations and corresponds with a potential shrinking of the “identifiable data pool” that micro-targeters could otherwise draw from.

3.1.1.2. Sensitive information. In Australia, under the broader umbrella of personal information, is “sensitive information,” for which the Act provides more stringent protections. It defines sensitive information as “information or an opinion about an individual’s racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record, health information, genetic information, biometric information … or biometric templates” (Privacy Act, 1988 (Cth)(s 6)). Unlike the Australian legislation, New Zealand’s Privacy Act, 2020 does not make explicit provisions for sensitive information. However, an in-practice distinction is still made, and sensitive information must be treated with extra precautions.

New Zealand’s approach to what constitutes sensitive information aligns with Australia’s approach. It encapsulates information about “a person’s race, ethnicity, gender or sexual orientation, sex life, health, disability, age, religious, cultural or political beliefs.” Likewise, the Privacy Commissioner (2020) notes that there are circumstances wherein a person’s “activities or memberships can be sensitive” if it shows “insights into an individual’s personal opinions” (Privacy Commissioner, 2020). It provides the example that membership of a union or political party is typically sensitive and asserts that there is a “higher standard of protection for sensitive personal information” that depends on each particular case (Privacy Commissioner, 2020). Where there are common types of sensitive information, New Zealand legislation is supplemented with industry-specific codes to protect individuals’ information, for example, the Credit Information Privacy Code 2020.

The Australian and New Zealand privacy acts both seek to protect personal information, and they construct personal information as an umbrella category under which sensitive information can be treated differently. While
the Australian Privacy Act explicitly protects sensitive information, the New Zealand legislation does not, but the special situation of sensitive information is nevertheless highlighted by supporting and explanatory commentary on the information privacy principles. In short, both countries treat sensitive information differently from other personal information. This distinction has implications for political microtargeting because information such as purchasing histories, political beliefs, religious beliefs, and so forth can be highly useful for targeting individuals to influence party or issue preferences. Awareness of these different categories of information is therefore important because restrictions on the collection of personal information vary depending on the category of information under collection and can thus have implications for the data collection stage of a microtargeting campaign.

3.1.2. What to collect data for?

The purposes for which personal information may be collected reflect the sentiment of data minimization. In both jurisdictions, there is a need for the information to be related or connected to the entities’ “functions” or “activities” and each law also includes a necessity requirement. For example, according to Australian Privacy Principle 3, an agency or an organization entity “must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities.” The bar for collecting sensitive information is higher, and an entity “must not collect sensitive information about an individual unless: the individual consents to the collection of the information” and “the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities” or, if an exception applies (relevant exceptions will be discussed shortly). New Zealand’s first privacy principle sets out that organizations “must only collect personal information if it is for a lawful purpose connected with their functions or activities, and the information is necessary for that purpose.”

In the context of political microtargeting, one could argue that if a political party were to collect data for the purpose of microtargeting it might meet this principle as an activity which is reasonably necessary for its functions—to gain support and increase votes. Yet, it is also possible to argue that it is not reasonably necessary since there can be other, less effective, means of achieving their goals and performing their functions without acquiring personal information. In a liberal democratic system, balancing free political communication with privacy rights and expectations can be a challenge. And, as this article will explain in the next section, Australia’s way of addressing this is to exempt political parties from the obligations of the Privacy Act (1988) (Cth). Nonetheless, parties are not the only entities who partake in political microtargeting, so it remains important to consider the Privacy Act since it can, theoretically, constrain the data collection of other entities such as campaigning firms or other businesses with an interest in particular political issues or outcomes.

The Australian Privacy Act also includes the need for consent for collecting sensitive information. Sensitive information, as mentioned, is of high value for microtargeters. It is unlikely that in instances where consent is required, many individuals would relinquish their information while cognizant of the manipulative use to which the information will be put.

3.1.3. How to collect information?

In both Australia and New Zealand, personal information generally needs to be collected from the individual whose information it is. The Australian Privacy Act states that an entity, “must collect personal information about an individual only from the individual,” unless exceptions apply. None of the stipulated exceptions are relevant for political microtargeting. Note that this provision applies to “soliciting” personal information. In the legislation, an entity solicits information “if the entity requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included” (Privacy Act, 1988 (Cth) s 6(1)). A request, in this instance, refers to an “active step” to obtain personal information. These provisions reduce the scope for third-party microtargeting operations by limiting the circumstances in which campaigners can recruit microtargeting firms or data brokers to collect personal information about constituents.

Similarly to the Australian legislation, New Zealand’s privacy principle 2 stipulates that personal information “must be collected from the individual concerned.” However, the Act acknowledges that this is not always possible, thus in certain situations, the law allows information to come from other parties. The Privacy Commissioner’s Office (2020) states that, “sometimes there may be good reasons for not letting a person know about the collection – for example, if it would undermine the purpose of the collection to protect law enforcement investigations, or it’s just not possible to tell the person.”
However, none of the situations within which this is permissible apply in a context of political microtargeting practices.

The Act also mandates that if collecting personal information from the individual, then the agency must take steps that are “reasonable” to ensure that the person knows that the information is being collected, why it is being collected and who the “intended recipients” are of the information.

In Australia, an individual’s consent is required to collect their sensitive information unless exceptions apply. Consent can be implied or express. The Australian Privacy Principle guidelines stipulate that several conditions need to exist for consent to be valid. For example, consent must be informed and voluntary and that “the individual has the capacity to understand and communicate their consent” (OAIC, 2022, p. 10). Consent cannot be inferred if the entity merely provided notice of collection, and the guidelines point out that “it will be difficult for an entity to establish that an individual’s silence can be taken as consent” (OAIC, 2022, p. 10). Under these provisions, it appears difficult for microtargeters to obtain consent without targets becoming aware of the microtargeting activity. In this case, the success of the operation would be compromised. In New Zealand, “authorization” from the relevant individual is required if the information is collected from a third party, if the information will be used for a different purpose than it was collected for, or if the information will be disclosed outside of New Zealand.

The provisions that regulate the means of collection of personal information are similar in both countries insofar as they each require the individual to supply the information which would likely restrict the value of the information for a microtargeting purpose. Yet, in Australia, there have been situations wherein collection of personal information may not have complied with privacy law, signaling that perhaps a deterrent effect of the legislation is not enough to ensure compliance in all situations. One of the most prominent examples of this is Australian Information Commission v Facebook Inc [2020] FCA 531, wherein the Office of the Australian Information Commission initiated proceedings against Facebook for claimed violations of the Privacy Act which occurred within the context of Cambridge Analytica’s infamous political microtargeting operations. As of 2023, the matter remains unresolved and mired in preliminary determinations regarding jurisdiction. While the outcome on the substantive matters of the case will enable a more fruitful analysis, the case highlights the potential limits of privacy law when it comes to large corporations for whom legal barriers may not deter or prohibit actions.

Importantly, in the Australian system, political parties are exempt from the Privacy Act (see s 6C for parties and s 7C for other limited political exemptions). The exemption is rooted in the recognition of the unique role that political parties play in democratic processes, including their need to engage in political communication, campaign activities, and constituent engagement. While this exemption allows political parties to collect, use, and disclose personal information without being subject to the Privacy Act’s requirements, it also raises important discussions about the balance between safeguarding individuals’ privacy rights and enabling robust political discourse. Critics argue that this exemption could potentially lead to concerns regarding data protection, transparency, and the potential misuse of personal information for political purposes (Attorney-General’s Department, 2023). Since political parties have clear incentives to engage in microtargeting, their exemption from the restrictions of privacy law is likely to limit the potential effect of privacy law on curtailing microtargeting.

Overall, the strength of privacy protections indicates that microtargeters may face a high hurdle at the outset of their campaigns because access to voters’ data is tightly controlled in Australia and New Zealand. Not only might microtargeters encounter obstacles relating to accessing data but they are also likely limited to data that may not be particularly useful for mounting sophisticated microtargeted campaigns. Yet, political parties are likely to be one of the key types of actor to benefit from political microtargeting operations and, in Australia, they are not restricted by the Privacy Act and can thus procure and use personal information unencumbered by the legislation. Further, microtargeting is a covert business that depends on and exploits targets’ ignorance. Consequently, while privacy legislation is well-equipped to mitigate microtargeting in some instances where all actors and platforms are committed to legally legitimate conduct, the reality is that this is not likely to be the norm given the range of actors capable of engaging in microtargeting.
3.2. Stage two: Segmentation and profiling

3.2.1. How to use information?

Both countries’ laws limit the disclosure of personal information (analyzed here as a type of use) and limit information’s use beyond its original purpose. Under the Australian Privacy Act, if an entity holds personal information “collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose)” unless “the individual has consented to the use or disclosure of the information” or the individual “would reasonably expect” the entity to “use or disclose the information for the secondary purpose,” providing that purpose is “directly related” to the original purpose (if sensitive information) or “related” (if regular personal information). Likewise, in New Zealand’s Privacy Act, other uses of information and disclosure are restricted by Principle 10. For example, the Act stipulates that “an agency that holds personal information that was obtained in connection with one purpose may not use the information for any other purpose” unless the information is “used in a form in which the individual concerned is not identified” or if “the use of the information for that other purpose is authorised by the individual concerned,” or if the information is public. The Act also limits disclosure, providing that agencies “must not disclose the information to any other agency or to any person” unless it is for the primary purpose or directly related to the primary purpose, or, if the individual authorizes it.

The closest reference to microtargeting in the legislation is in Australia’s privacy principle 7, which limits the sharing of personal information for the purpose of “direct marketing” (see Privacy Act, 1988, Schedule 1, s 7). However, a range of exceptions are provided which appear to allow for direct marketing unless the information is sensitive, and even when it is sensitive, information can be shared for direct marketing with the individual’s consent. It is also unclear whether microtargeting would be captured by “direct marketing.” The implications of the direct marketing principles for microtargeting do not appear to offer much additional protection for microtargeting beyond the more general provisions for consent discussed above.

3.3. Stage three: Tailored messaging

In both countries, the most relevant legislation for stage three are the electoral acts. The most relevant aspects of the countries’ election laws for political microtargeting are the provisions that pertain to political advertising because these provisions are relevant for the tailored messaging phase of a microtargeting campaign. In this section, I identify and compare the most pertinent provisions for political microtargeting.

3.3.1. Electoral matter

Political advertising laws only apply to “electoral matter” in Australia, and to “political advertising” in New Zealand. In Australia, electoral matter is defined in the Electoral Act 1918 (Cth) (s 4AA) as “matter that is communicated, or intended to be communicated, for the dominant purpose of influencing the way electors vote in a federal election.” Matter is deemed electoral if it promotes or opposes “a political entity, to the extent that the matter relates to a federal election” or “a member of the House of Representatives or a Senator, to the extent that the matter relates to a federal election.” Personal opinions are not treated as “electoral matter.” In New Zealand, political advertising is deemed to be “an advertisement in any medium that may reasonably be regarded as encouraging or persuading voters to do either or both of the following: to vote, or not to vote, for a type of candidate or party” and includes candidate and party advertisements, but excludes unpaid people sharing personal opinions (s 3(1)).

Given the breadth of the content covered by the definitions of electoral matter and political advertising in each country, vast amounts of political microtargeting content would likely fall into these categories (given the objectives of influencing voters’ political preferences) and thus would be subject to the relevant provisions in the countries’ electoral acts. Yet, this assumes that microtargeting firms conduct their campaigning fairly openly and communicate advertisement-style messages. There might be circumstances in which microtargeters deploy more covert means of messaging which mask content as personal opinion and embed such “opinions” into chat forums. It is possible to leverage the anonymity of the internet and harness artificial intelligence to spread “opinions” without risk of identification.
3.3.2. Truth

While there are provisions in the Australian Electoral Act that prohibit certain types of “misleading and deceptive” advertising during certain time periods, there is no legal requirement for truth in political advertisements. There is only a restriction on misleading information in relation to casting a vote. This is contained in s 329 (1) of the Electoral Act, and states that “[a] person shall not, during the relevant period in relation to an election under this Act, print, publish or distribute, or cause, permit or authorize to be printed, published or distributed, any matter or thing that is likely to mislead or deceive an elector in relation to the casting of a vote,” and the provision includes internet content (s 329(6)). The situation differs in New Zealand, where the Electoral Act (1993) makes it an offense to publish misleading information to influence voters in the two days before the election, and electoral communications are regulated by the Advertising Standards Authority (ASA). The ASA has the authority to instruct those responsible for a misleading advertisement to remove it. The ASA does not have jurisdiction over posts on “branded” social media pages (“organic posts”) or party, advocacy group, or candidate websites (ASA, 2023).

While federal law in Australia offers limited measures to reduce disinformation pertaining to elections, states such as South Australia and the Australian Capital Territory have legislation that promotes truth in political advertising (Electoral Act 1985 (SA)(s 113)) (Hill et al. 2022). Under the laws, it is an offense to publish political advertisements that are inaccurate or misleading.

Assuming that microtargeters use clear “advertisement” style communications for their messages and that their content therefore comes under the Acts, they still do not face many obstacles in either country regarding the veracity of the content they espouse. In Australia, microtargeters could easily orchestrate campaigns disseminating misleading information, exploiting the current regulatory environment. In New Zealand, the barriers are comparatively lax, further facilitating the unimpeded deployment of tailored messaging. In essence, the process of crafting and delivering tailored messages remains largely unhindered in both countries.

3.3.3. Labeling

In Australia and New Zealand, electoral matter/political advertisements need to be labeled with the promoter’s details. For example, the Australian law makes it mandatory for electoral advertisements to include an “authorization” message that identifies the entity that approved the advertisement, but personal communications are not bound by this provision (s 321D). Authorization requirements also apply to social media (Commonwealth Electoral [Authorisation of Voter Communication] Determination 2021) and need to be affixed to the item in a way that ensures it remains visible when it is shared.

Labeling and authorization requirements may pose a minor obstacle for microtargeting, as they signal to voters that the information is indeed advertising. This transparency could potentially undermine covert attempts at influence. In certain scenarios, this could prove effective in thwarting influence—for instance, if the source is recognized as originating from a disliked political party or organization. However, the crux of the issue lies in enforcement. The vastness of social media means that it is practically impossible for anyone to monitor all the advertisements spread across numerous platforms. Even though some platforms maintain registers of ads (for instance), there exist many platforms lacking the same level of cooperative or regulated practices. While this could present a challenge when aiming to reach a broad audience, it might not significantly impact political microtargeting efforts.

Political advertising laws could, theoretically, improve transparency and accountability, but success remains largely in the hands of social media companies. It relies on three assumptions: (1) that platforms rigorously police content, and (2) that platforms will remove non-compliant content; and (3) that content is attributable to a source, so that if it is not labeled the punitive consequences can be enforced. But, the reality of the internet is that attribution is not always possible due to technologies that shield identities and locations. And, for microtargeters, the potential for attribution is likely to be actively evaded. This means that there are minimal consequences for unlabeled and unauthorized advertisements. Damage to the democratic process may already have occurred irrespective of whether a platform eventually removes the content (Ray, 2021). Attribution difficulties render other potentially relevant provisions, such as restrictions on foreign entities partaking in political advertising, toothless when it comes to microtargeting because enforcement is impossible.
4. Conclusion

Political microtargeting presents a set of complex challenges for lawmakers, yet despite the absence of legislation specific to microtargeting, Australia and New Zealand have a variety of provisions that may nevertheless mitigate microtargeting in some circumstances. Evidently, lawmakers have made significant progress toward modernizing their laws for the digital era, with some provisions explicitly applicable to online environments wherein microtargeting operations are carried out.

Privacy legislation in both countries provides restrictions to the collection and use of personal information, which potentially reduces the amount and type of data available for microtargeting operations. Australia’s push for de-identification of personal information is, theoretically, one of the strongest defenses against microtargeting, since it has the potential to restrict the amount of identifiable data in circulation for microtargeters to access. Yet, New Zealand’s aims of “information minimization” might lead to an even more effective obstacle for microtargeting by reducing the amount of information shared more broadly. However, in Australia, the fact that political parties are exempt from the Privacy Act means that the mitigation prospects of the Act are likely to be minimal in practice, since political parties—one of the main types of actors engaging in microtargeting—remain free to collect and use data unencumbered by the legislation.

Meanwhile, political advertising laws cater toward curtailing the tailored messaging component of microtargeting campaigns by mandating advertisement labeling, authorization, and placing some limits on sharing deceptive content. However, these provisions tend to be narrowly construed which limits their applicability to microtargeting scenarios. Widening the time-frame and contexts of application of these laws might provide a solution; however, tensions between regulating political speech and protecting free speech clearly present a concern. Removing the exemption for political parties from the Australian law would likely improve incidental protections against microtargeting, and calls to remove the exemption already have considerable traction (Attorney-General’s Department, 2023).

Both the privacy legislation and political advertising laws are unlikely to capture the most insidious forms of microtargeting whereby operations are covert, untraceable, and unattributable. The laws rely on punitive enforcement mechanisms which can only function if the actors who are responsible for the illicit conduct are identifiable and fall within the legislation’s jurisdiction. With the rise of alt-tech platforms like Gab and Telegram, which operate even further from the regulatory space than mainstream platforms such as Facebook and Twitter, platform compliance and cooperation are not guaranteed or enforceable.

Moving forward with this research, it is imperative to evaluate these laws in light of case law to gain a more fine-grained understanding of how these provisions discussed have been applied in practice. Furthermore, given the deficiencies of the piecemeal approach, it is necessary to investigate the constitutional permissibility of legislation to regulate microtargeting holistically with a view to establish law that is tailored to protect democracy.

Through identifying legislation relevant to microtargeting and evaluating its role in potentially mitigating microtargeting, this paper has offered a comparative foundation for ongoing research on the preparedness of the law to contain the microtargeting problem in liberal democracies. Although existing piecemeal provisions are not entirely toothless when it comes to mitigating microtargeting, they are not well-equipped for limiting the most insidious microtargeting operations in the evolving digital arena.

Acknowledgments

This paper was funded by the Australian National University.

Data availability statement

Research data are not shared.
References


Privacy Act 2020.


