Legislative Assembly for the
Australian Capital Territory
Standing Committee on the Integrity Commission and Statutory Office Holders

Submission Cover Sheet

Inquiry into the operation of the 2024 ACT Election and Electoral Act 1992

Submission number: 030

Submitter: ANU Law Reform and Social Justice Research Hub's

Date authorised for publication: 14 October 2025

Standing Committee on the Integrity Commission and Statutory Office Holders

27/07/25

Dear Officer,

RE: Inquiry into the Operation of the 2024 ACT Election

The Australian National University Law Reform and Social Justice Research Hub ('ANU LRSJ Research Hub') welcomes the opportunity to provide this submission to the Standing Committee on the Integrity Commission and Statutory Office Holders, responding to the terms of reference of the inquiry, with a particular focus on **4(a) and 4(c)**.

The ANU LRSJ Research Hub falls within the ANU Law School's Law Reform and Social Justice program, which supports the integration of law reform and principles of social justice into teaching, research and study across the School. Members of the group are students of the ANU Law School, who are engaged with a range of projects with the aim of exploring the law's complex role in society, and the part that lawyers play in using and improving law to promote both social justice and social stability.

Summary of Recommendations:

> **Recommendation 1:** Amend the definition of 'electoral matter' in section 4 of the *Electoral Act 1992,* replacing the subjective test of "likely to affect voting" with a more objective and broader "reasonably capable of influencing voting", while expressly excluding material produced or authorised by the Assembly in the ordinary course of its proceedings.
>
> **Recommendation 2:** Amend section 293A of the *Electoral Act 1992* to clarify the definition of 'private capacity', closing loopholes that may enable coordinated inauthentic behaviour or astroturfing campaigns.
>
> **Recommendation 3**: Consider introducing harsher and tiered penalties for breaches of political advertising provisions, particularly for the creation and dissemination of materially misleading or deceptive electoral material, ensuring penalties act as a genuine deterrent.
>
> **Recommendation 4:** Amend the *Electoral Act 1992* to explicitly regulate AI-generated content by requiring prominent disclosure on any electoral matter that is created or significantly altered using generative AI, and prohibiting the use of deceptive deepfakes of candidates or other persons in electoral matter.
>
> **Recommendation 5:** Empower the ACT Electoral Commission with a specialised, tech-focused integrity unit to rapidly monitor, investigate, and advise on misinformation, AI misuse, and other technologically-enabled threats to electoral integrity.

If you require further information, please don't hesitate to contact us at

On behalf of the ANU LRSJ Research Hub,

Authors: Ethan Zhu
Editors: Jae Brieffies

Introduction

This submission addresses the urgent need to modernise the ACT's electoral framework to confront emerging threats to democratic integrity, particularly those posed by digital platforms and generative Artificial Intelligence (AI). While the *Electoral Act 1992* (the Act) contains some of Australia's most robust provisions on political communication, its definitions and enforcement mechanisms were designed for a pre-digital, and certainly pre-AI, era.[1]

This submission is divided into three parts. The first section examines foundational definitions within the Act, specifically 'electoral matter' and the 'private capacity' exemption. It argues that their current ambiguity is no longer tenable in an era of coordinated digital campaigns and sophisticated astroturfing, and proposes clearer, more objective legislative standards. The second section provides a detailed analysis of the Act's penalty and enforcement regime. It contends that the existing penalties for misleading political advertising are manifestly insufficient to act as a genuine deterrent against well-resourced and malicious actors. It recommends the introduction of a harsher, tiered penalty system to ensure consequences are both proportionate and effective. The third and final section confronts the novel and significant threat posed by generative AI and synthetic media (deepfakes). It highlights how this technology can circumvent existing 'truth in advertising' provisions and erode public trust on an unprecedented scale.

Collectively, our recommendations propose a suite of legislative and administrative reforms designed to establish a clear, enforceable, and technologically informed framework. This framework aims to protect both the implied freedom of political communication and the fundamental integrity of the ACT's electoral process from modern threats.

[1] Electoral Act 1992 (ACT) (*'Electoral Act'*).

1. Defining and Regulating Electoral Matter in the Digital Age

Much of the ACT's electoral regulation, including authorisation requirements, spending caps, and advertising laws, relies on the definition of 'electoral matter'. The current definition in section 4 of the Act, while comprehensive in its intent, contains a degree of vagueness that undermines its suitability in the digital age.[2] This ambiguity risks chilling legitimate speech whilst failing to target genuine electoral campaigning effectively.

1.1 The Ambiguity of 'Likely to Affect Voting'

Section 4(1) of the Act defines electoral matter as anything "intended or likely to affect voting at an election".[3] While the "intent" test is straightforward, the "likely to affect" limb is broad and open to subjective interpretation. It requires speculation on the potential psychological impact of a communication on a hypothetical voter. The result is legal uncertainty for organisations, academics, charities, and community groups.

Take the example of a report or statement on housing affordability by a non-partisan organisation during a campaign. Even though this is not intended to influence votes, and well within the rights of individuals and organisations to exercise free political expression, it could certainly be perceived as 'likely' to do so. This ambiguity can be problematic, as it unintentionally sweeps these groups into this regulatory scheme, which imposes a compliance burden with the potential to stifle public discourse precisely where it is most needed.

Therefore, we suggest a more robust legal standard that is both objective and testable.

> **Revised Wording for Subsection (1):**
> *(1) In this Act, electoral matter means any material, in printed or electronic form, that is intended to influence, or is* ***reasonably capable of influencing****, the way electors vote in an election.*

This change would shift the focus from predicting a voter's reaction to assessing the nature, content, and context of the material itself. This provides greater clarity and ensures that regulation is targeted at material that is genuinely electoral, rather than any communication that might tangentially touch on election issues.

1.2 Defining the Exemption for Assembly Publications

Section 4(3) creates a significant exemption for "a publication of the Assembly".[4] However, this term is not defined, creating ambiguity. For instance, It is unclear whether this exemption would cover a newsletter produced by an MLA using parliamentary resources or a report by a government agency that touches on election issues. This loophole could potentially be exploited to disseminate partisan material under the guise of an official publication.

---

[2] *Electoral Act* (n 1) s 4.
[3] Ibid s 4(1).
[4] Ibid s 4(3).

Revised Wording for Subsection (3):
(3) However, material produced or authorised by the Assembly (including its committees) ***in the ordinary course of its proceedings*** *is not electoral matter.*

This amendment provides crucial clarity. "In the ordinary course of its proceedings" is a standard legal phrase that confines the exemption to the legitimate, non-partisan functions of the legislature, such as committee reports, Hansard, and official inquiries. It closes a potential loophole and ensures that the exemption serves its intended purpose of protecting the core work of the Assembly, not partisan campaigning.

Recommendation 1: Amend the definition of 'electoral matter' in section 4 of the *Electoral Act 1992* by adopting the following wording:

(1) In this Act, electoral matter means any material, in printed or electronic form, that is intended to influence, or is reasonably capable of influencing, the way electors vote in an election.

…

(3) However, material produced or authorised by the Assembly (including its committees) in the ordinary course of its proceedings is not electoral matter.

1.3 The 'Private Capacity' Exemption and Coordinated Campaigns

'Astroturfing' involves creating the false appearance that a sponsored message originates from regular citizens or grassroots movements.[5] It is often highly coordinated inauthentic behaviour, which, whilst meeting formal disclosure requirements set out by the law, does not transparently inform the public about the source of influential advertising campaigns.[6] They allow political actors to hide behind shell entities: eroding accountability whilst fabricating independent support for policies.

With the rise of social media campaigning and the proliferation of chatbot technology, astroturfing is likely to become an increasingly prevalent concern.[7] Malicious actors can use

[5] Daniel Angus, Christine Parker, Giselle Newton, Kate Clark and Mark Andrejevic, *'What Political Ads Are Australians Seeing Online? Astroturfing, Fake Grassroots Groups, and Outright Falsehoods'* (The Conversation, 28 April 2025) https://theconversation.com/what-political-ads-are-australians-seeing-online-astroturfing-fake-grassroots-groups-and-outright-falsehoods-255225.
[6] Ibid.
[7] Ibid.

bots or paid networks to flood social media with messages that appear to be from citizens acting in a 'private capacity'. Generative AI exacerbates this threat by allowing the creation of thousands of unique yet coordinated posts, all appearing to be authentic personal views.[8] The current Act provides no clear way to distinguish this from genuine citizen engagement.

Section 293A of The Act provides a legitimate exemption from authorisation rules for individuals who disseminate electoral matter on social media in a 'private capacity'.[9] It is undeniably essential that individuals can express personal political views without fear of persecution. However, this exemption is vulnerable to potential exploitation.

> **Recommendation 2: Amend section 293A of the *Electoral Act 1992* to clarify the definition of 'private capacity' to ensure it cannot be exploited by coordinated inauthentic behaviour or astroturfing campaigns, particularly those amplified by automated technology.**
>
> **Suggested drafting approach:**
> An individual is not acting in a 'private capacity' if their communication is made as part of a coordinated campaign at the direction or funding of a third party, or if the dissemination of the matter is automated.

These measures would help the Electoral Commission identify and act against campaigns that deceptively masquerade as grassroots movements.

2. Establishing Proportionate Penalties as an Effective Deterrent

Effective regulations require not only comprehensive rules, but also practical consequences to deter offences. The ACT should be commended for implementing 'truth in political advertising' laws, though its efficacy may be undermined by insufficient penalties, particularly in the high-stakes election campaign environment.[10] Minor financial penalties are often inadequate deterrents: they are seen as the 'cost of doing business' for a well-funded campaign.

This submission will now turn to the penalties available under the Act, analysing the principles of effective deterrence. It will propose a new, multi-faceted framework designed to produce

---

[8] Matt Martino, *'Deepfakes and Falsehoods Are Legal in Political Advertising. Not Everyone Is on Board with Fixing It'* (ABC News, 15 October 2024) https://www.abc.net.au/news/2024-10-15/deepfakes-misinformation-ai-gen-in-political-advertising-legal/104470006.

[9] *Electoral Act* (n 1) s 293A

[10] Kieran Pender, *'Are Truth in Political Advertising Laws Constitutional?'* (Australian Public Law, 13 April 2022) https://www.auspublaw.org/blog/2022/04/are-truth-in-political-advertising-laws-constitutional.

proportionate consequences for the dissemination of deliberately deceptive electoral matter and advertising.

2.1 The inadequacy of current penalties

A breach of section 297A (Misleading electoral advertising) is a maximum of 50 penalty units.[11] As of 2025, one penalty unit amounts to $160 for an individual and $810 for a corporation, which includes a political party.[12]

Modern political parties are very well-resourced. In 2023–24, Australia's political parties collectively raised $166 million.[13] For a major political party, a $40,500 fine is a relatively minor financial risk. A campaign manager could rationally conclude that the electoral benefit of a powerful, misleading attack ad in the final week of a campaign outweighs this potential cost.

The current framework does not effectively punish or deter systemic or repeated breaches by the same political actor across a campaign.

One proposal that could be explored is a multi-layered system that includes enhanced financial penalties and a "penalty points" system to target repeat offenders.

Recommendation 3: Introduce harsher and tiered penalties for breaches of political advertising provisions, particularly for the creation and dissemination of materially misleading or deceptive electoral material, ensuring penalties act as a genuine deterrent.

[11] *Electoral Act* (n 1) s 293A (1).
[12] *Legislation Act* 2001 (ACT) s 133.
[13] Kate Griffiths and Jessica Geraghty, 'Political donations data show who's funding whom in Australia – but they are coming out far too late' (The Conversation, 3 February 2025) https://theconversation.com/political-donations-data-show-whos-funding-whom-in-australia-but-they-are-coming-out-far-too-late-248662.

2.2 A Proposed Framework for Harsher and Tiered Penalties

2.2.1 Tiered System

The financial penalties should be significantly increased and tiered based on the severity of the breach:

Tier 1	**Minor Breach:** For administrative errors or communications with minor, unintentional inaccuracies. A modest increase to the existing penalty unit structure would be appropriate.
Tier 2	**Significant Breach:** For the negligent dissemination of materially misleading information. Penalties should be increased to a level that represents a significant financial impost, such as up to 200 penalty units.
Tier 3	**Major Breach:** For the knowing creation and dissemination of materially deceptive or fabricated content, especially deepfakes. Penalties should be severe, such as: ● For corporations/parties: A fine of up to **500 penalty units or a percentage (e.g., 25%) of the party's total capped expenditure limit for the election**, whichever is greater. This ensures the penalty scales with the size and resources of the campaign. ● For individuals: A fine of up to 500 penalty units and/or a term of imprisonment, reflecting the serious threat such conduct poses to democracy.

2.2.2 Penalty Points System

- **Accrual of Points:** When a political actor (a party, candidate, or third-party campaigner) is found to have breached a serious political advertising provision, they would be issued a finding and a set number of penalty points (e.g., 1 point for a minor breach, 5 points for a major breach). These points would be publicly recorded on a register maintained by the ACT Electoral Commission.
- **Escalating Consequences:** The accumulation of points over a set period of time (e.g., a four-year election cycle) would trigger escalating sanctions. Consider the following example:

To address repeat offending and introduce a tangible political cost, we propose the introduction of a demerit-style ‘Electoral Penalty Points System’. This would function similarly to a driver's license demerit scheme.

Threshold 1 (e.g., 3 points)	A formal public warning issued by the Electoral Commissioner and published on the Commission's website.
Threshold 2 (e.g., 6 points)	A suspension or reduction of public election funding for that party or candidate at the current or subsequent election. This creates a powerful financial incentive to comply with the law.
Threshold 3 (e.g., 10+ points)	The most severe sanction. This could trigger an application by the Electoral Commission to the Supreme Court for an order to deregister a political party for a defined period or disqualify a candidate from contesting the next election.

The penalty points system introduces a crucial element of reputational and political risk that is absent from a purely financial penalty regime. It creates a public record of misconduct and imposes consequences that directly affect a political actor's ability to campaign and operate, thereby constituting a far more genuine and effective deterrent.

3. Confronting the Threat of AI-Generated Misinformation and Deepfakes

The rapid development and democratisation of generative artificial intelligence (AI) is a genuine threat to electoral integrity. The technology enables the creation of completely falsified text, image, and video-based content, which is increasingly difficult to discern from reality.

A particular concern is the generation of 'deepfakes', which are artificial yet seemingly real synthetic media.[14] This commonly takes the form of realistic yet fake videos depicting political figures. It is easier and cheaper than ever to generate these videos at scale and speed. This will pose a significant challenge that the *Electoral Act* is poorly equipped to address in its current state.

3.1 The Nature and Scale of the AI Threat

The existential threat posed by AI to democracy cannot be overstated. Voters rely on making decisions by consuming content they can trust to be accurate and reliable. With the potential for anyone to generate fabricated information that is identical to reality, AI blurs the line between truth and lies.

AI has advanced at an exponential rate.[15] Increased usage and available data only strengthen it. Many already consider AI-generated video and graphical content indistinguishable from authentic sources, and this trend is expected to continue improving over the coming years. The Australian Strategic Policy Institute (ASPI) has warned that generative AI can lead to the "erosion of trust in the online information space as audiences become increasingly unsure about which content is AI-generated and therefore which sources can be trusted".[16] They further write that "it will enable the generation of information—including disinformation—at a volume and velocity not seen previously and, perhaps even more troublingly, with a verifiability that may make it hard for audiences to discern the truth of the information they are receiving".[17]

The threat from generative AI also extends beyond just deepfake videos. It includes a spectrum of deceptive techniques that can disrupt electoral integrity:

- **Deepfake Audio:** As demonstrated in the 2023 Slovakian election, where fabricated audio of a party leader seemingly discussing how to rig the vote was released 48 hours before polls opened, this can be a highly effective tool for last-minute deception.[18]

---

[14] Ibid.
[15] Ibid.
[16] Sam Stockwell, 'AI disinformation: lessons from the UK's election' (Australian Strategic Policy Institute, 16 August 2024) https://www.aspistrategist.org.au/ai-disinformation-lessons-from-the-uks-election/.
[17] Tom Rogers, 'Protecting our elections against tech-enabled disinformation' (Australian Strategic Policy Institute, 14 August 2024) https://www.aspistrategist.org.au/protecting-our-elections-against-tech-enabled-disinformation/.
[18] Lluis de Nadal and Peter Jančárik, 'Beyond the deepfake hype: AI, democracy, and "the Slovak case"' (Harvard Kennedy School Misinformation Review, Commentary, 22 August 2024). https://misinforeview.hks.harvard.edu/article/beyond-the-deepfake-hype-ai-democracy-and-the-slovak-case/.

- **Shallowfakes:** Simpler, manipulated media, such as selectively edited videos, mis-captioned images, or slowed-down footage, can be just as damaging and are often harder for platforms to detect.
- **AI-Generated Text:** Sophisticated language models can be used to generate thousands of unique, context-aware comments and posts for "astroturfing" campaigns, creating the false impression of a widespread grassroots movement and overwhelming genuine online discourse.

This technology creates a pernicious secondary effect known as the ‘liar's dividend’.[19] As noted by legal scholars Robert Chesney and Danielle Citron, as the public becomes more aware of deepfakes, it becomes easier for malicious actors to dismiss genuine, incriminating evidence as a fabrication.[20] This erodes the very ideal of shared truth upon which democratic accountability depends.

3.2 Current ‘Truth in Advertising’ Laws Are Unprepared

We acknowledge that the ACT’s ‘truth in political advertising’ laws are innovative.[21] The rule prohibits electoral matter that contains a "statement purporting to be a statement of fact that is inaccurate and misleading".[22]

The issue is that deepfakes are not necessarily a ‘statement of fact’. They are fabricated realities, often portrayed as political satire and commentary. This argument can be used maliciously to circumvent the law. This legal ambiguity renders the provision ineffective against the most potent form of AI-driven misinformation. Therefore, the law must evolve to recognise and prohibit this specific form of conduct. To address this, the law must explicitly recognise this new form of deception.

---

[19] Danielle K Citron and Robert Chesney, ‘Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security’ (2019) 107(6) *California Law Review* 1753.
[20] Ibid.
[21] *Electoral Act* (n 1) s 297.
[22] Ibid.

Recommendation 4: Amend the *Electoral Act 1992* to explicitly regulate AI-generated content by:

(a) Mandating Disclosure: Require a prominent disclosure on any electoral matter that is created or significantly altered using generative AI

This approach aligns with global best practice. The European Union's *Digital Services Act* is moving towards clear labelling of deepfakes,[23] and several US states have introduced similar legislative requirements for political advertising.[24] Disclosure establishes a transparency baseline, informing voters that the content they are viewing is synthetic and empowering them to apply a higher degree of critical scrutiny. This shifts the regulatory focus from *authorisation* alone to include *authenticity*.

(b) Prohibiting Deceptive Use: Ban the use of deceptive deepfakes of candidates or other persons in electoral matter by expanding the definition of misleading conduct in section 297A

A specific subsection should be added to clarify that conduct is misleading if it involves creating or sharing synthetic media that deceptively impersonates an individual or depicts them saying or doing something they did not say or do, without their consent and with the intent to mislead voters. This must be carefully drafted to distinguish deceptive impersonations from clear and obvious satire.

3.3 The Need for Specialist and Rapid Enforcement

Recommendation 5: Empower the ACT Electoral Commission with a specialised, tech-focused integrity unit to rapidly monitor, investigate, and advise on misinformation, AI misuse, and other technologically-enabled threats to electoral integrity.

[23] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC [2022] OJ L 277/1 (‘*Digital Services Act*’).
[24] REAL Political Advertisements Act, HR 3044, 118th Cong, 1st sess, 2023.

To navigate the increasingly complex use of AI in election campaigns, a dedicated unit, perhaps modelled on the specialist branches within bodies like the ACCC or the eSafety Commissioner, would be particularly beneficial. It would have several key roles:

- **Technical Capacity:** Providing technical expertise to identify and analyse synthetic media used in elections.
- **Rapid Response:** Establishing an efficient, expedited, and transparent process for resolving complaints about potential deepfakes and AI-generated political misinformation.
- **Platform Liaison:** Serve as the primary point of contact for digital platforms (such as Meta, Google, and TikTok), facilitating the swift escalation of reports of illegal content for review and removal.
- **Enforcement Advice:** Provide the Electoral Commission with technical advice needed to issue a rapid correction or takedown for material found to be in breach of the Act.
- **Public Education:** Proactively increase digital media literacy among the ACT electorate, educating voters on how to spot and report synthetic media

Conclusion

The ACT has a proud history of leading Australia in electoral innovation and integrity. To uphold this reputation, it must now proactively reform its laws to meet the challenges of the digital age. The recommendations outlined above clarify crucial definitions, explicitly prepare regulations for the rise of AI use in campaigns, and empower the Electoral Commission with the necessary tools to act to combat misinformation. This will enable the ACT to safeguard the fairness and integrity of our democracy for many years to come.