



Australian Government

Office of the Privacy Commissioner

**Australian Government Electoral
Reform Green Paper-
Strengthening Australia's
Democracy**

**Submission to the
Department of the Prime Minister
and Cabinet**

December 2009

KEY RECOMMENDATIONS

The Office acknowledges and supports the consideration which has been given in the Electoral Reform Green Paper- Strengthening Australia's Democracy to the importance of protecting personal information privacy in enrolment processes and building good privacy practice into the electoral architecture. The Office's key recommendations are:

- i) Better privacy practice for an automatic enrolment or electoral roll maintenance scheme would be an 'opt-in' model where individuals consent to the sharing of their information. As part of any automatic scheme individuals should be given appropriate notice as to the handling of their personal information. (paras 8-13)
- ii) Data-matching as part of an automatic scheme should only occur after appropriate regard for privacy issues has been given. In particular, the purpose of the data-matching should be narrowly defined as being to maintain the accuracy of the electoral roll. (paras 8-13)
- iii) If an automatic scheme is implemented consideration should be given to developing personal information sharing protocols as part of a memorandum of understanding with participating state based agencies in those states that do not have specific privacy legislation. (paras 8-13)
- iv) Privacy enhancing technologies should be considered as part of the design of new technological approaches to the management of the electoral roll to meet both e-security and privacy objectives. (paras 14-17)
- v) Robust identity verification and management processes should be built into enrolment processes and the range of documents accepted as evidence of identity expanded to provide flexibility for individuals. (paras 18-21)
- vi) Reducing the number of data repositories containing comparable elector information into a single common roll with robust security protections could be privacy enhancing in that the number of large repositories containing similar amounts of personal information would be reduced. (paras 24-28)
- vii) Given the mandatory nature of enrolment, it is appropriate that access to information on the electoral roll beyond that which is publically available, remain relatively narrow with access limited to where there is a legitimate public interest. (paras 29-31)
- viii) The Australian Electoral Commission should develop privacy guidelines to apply to entities not currently covered by the *Privacy Act 1988 (Cth)*, which handle electors' personal information, including postal vote applications. (paras 33 and 37)
- ix) Privacy Impact Assessments should be conducted to help identify and address potential privacy issues associated with any proposed reforms to the electoral architecture. (paras 38-40)

OFFICE OF THE PRIVACY COMMISSIONER

1. The Office of the Privacy Commissioner (the Office) is an independent statutory body established under the *Privacy Act 1988* (the Privacy Act) whose purpose is to promote and protect privacy in Australia.
2. The Privacy Act contains eleven Information Privacy Principles (IPPs) which apply to Australian and ACT Government agencies. It also includes ten National Privacy Principles (NPPs) which generally apply to all businesses with an annual turnover of more than \$3 million, all private sector health service providers and some other small businesses. They do not apply to certain exempt organisations including political parties.¹
3. The coverage of the Privacy Act is limited to 'personal information'. This is defined in section 6 (1) of the Act as information or an opinion, whether true or not, about an individual whose identity is apparent or can be reasonably ascertained from that information.

BACKGROUND

4. The Office welcomes the opportunity to provide comments on the Electoral Reform Green Paper- Strengthening Australia's Democracy, September 2009 (the Green Paper).
5. The Office is pleased that the Green Paper refers to privacy considerations², which in the Office's view are particularly relevant to any review of electoral architecture and processes. The Office also agrees that it is desirable to have a transparent and open electoral system and recognises that the right to privacy is not absolute and needs to be balanced with other important public interests.³

ENROLMENT AND PARTICIPATION (Chapter 7)

Introduction of automatic or online enrolment and updating

6. The Green Paper notes that enrolment processes and systems can become a barrier to the exercise of the right to vote and considers options to increase participation rates through the introduction of automatic or online enrolment and/or updating.⁴

¹ Information relating to the operation of the Privacy Act can be found on the Office's website at www.privacy.gov.au. Specific information outlining the privacy provisions covering private sector organisations and Australian government agencies can be found at:

www.privacy.gov.au/business/index.html for businesses

www.privacy.gov.au/government/index.html for government

Specific information outlining exemptions to the private sector provisions can be found at: http://www.privacy.gov.au/publications/IS12_01.html

² See Green Paper paragraphs 7.3, 7.104 – 7.110

³ See section 29 (a) of the Privacy Act

⁴ See Green Paper paragraph 7.22

7. The Office recognises the benefits of automatic or online enrolment and/or updating in making it easier for people to enrol and update their details. The Australian Electoral Commission (the AEC) has noted a trend of increasing resistance to paper-based enrolment methods, and also a growing expectation, especially among young people, that government agencies should take the initiative to provide targeted services to individuals.⁵ It is further noted that many electors believe that automatic enrolment and updates to their personal details already occurs.

Automatic enrolment and updating

8. The Office understands that section 92(1) of the Electoral Act currently permits the AEC to collect, from other federal, state and local government agencies, “all such information as the Electoral Commission requires in connection with the preparation, maintenance or revision of Rolls”. This information is used for the purpose of verifying data on the roll and cannot be used to automatically update electors’ details or enrol individuals.
9. If an automatic enrolment or update scheme is implemented, appropriate notice would need to be provided to individuals about the way in which their personal information will be handled.
10. Agencies participating in the collection of personal information for the automatic scheme would be required by the Privacy Act, or relevant state privacy legislation, to notify individuals that their personal information will be disclosed to the AEC for the purposes of maintaining the electoral roll at the time the information is collected. The Office believes that the AEC should also consider developing personal information sharing protocols as part of a memorandum of understanding with participating state based agencies in those states that do not have specific privacy legislation.⁶
11. Further the Office suggests it would be useful for the AEC to provide a general notification on the handling of personal information for electoral roll purposes. This could be effectively achieved through a layered privacy policy, an example of which is available on the Office’s website.⁷ The notice should clearly explain what personal information will be collected, whether providing certain information is voluntary, how any information will be used and for what purpose, and any security safeguards protecting the handling of such information.
12. The Office supports the option in the Green Paper of an ‘opt-in’ model, whereby clients of participating agencies consent to the sharing of personal information with the AEC as part of an automatic enrolment or update scheme.⁸ The Office generally supports initiatives that allow

⁵ See Green Paper paragraph 7.29

⁶ That is, Western Australia and South Australia, although South Australia has an administrative policy on personal information handling applying to its public sector.

⁷ <http://www.privacy.gov.au/materials/types/policies/view/6810> The Office notes that the AEC already provides a privacy notice on its website, but that this only relates to personal information collected through the website and other privacy issues related to using the website.

⁸ See Green Paper, paragraph 7.45

individuals to have as much control as practicable over the collection, use and disclosure of their personal information and therefore supports the opt-in model as being the better privacy practice.

13. Any data-matching as part of automatic enrolments or updates of the electoral roll should only occur after appropriate regard for privacy issues has been given. In particular, the purpose of the data-matching should be narrowly defined as being to maintain the accuracy of the electoral roll. Further, formal protocols should be implemented to ensure that redundant or unmatched personal information is not retained. The voluntary data matching guidelines⁹ issued by the Privacy Commissioner may assist in ensuring that the development of a data-matching program as part of an automatic system is conducted in accordance with sound privacy practices.

Online enrolment and updating

14. Individuals have an interest in controlling the dissemination of information about themselves and may legitimately only provide information that is required or relevant for the purposes of a particular agency. Online enrolment and updating maintains the positive onus on individuals to provide their details and enables a measure of control to be exercised by the individual.

15. The Office notes comments in the Green Paper concerning the development of an appropriately secure website and data handling techniques as a necessary element of an online enrolment or update scheme.¹⁰ Privacy enhancing technologies (PETs) could be utilised to meet e-security and privacy objectives and should be considered in realising the potential of new technologies and innovative approaches to management of the electoral roll.

16. As the Office has previously noted¹¹, PETs tend to fall into several categories, for example:

- i) **General information security tools** – these include encryption, logical access controls, use of digital certificates etc.
- ii) **Data separation** – this refers to systems that detach identifying information from other personal information so that the individual's privacy is protected during processing and storage of their personal information. Generally only an authorised person with a digital key is able to re-identify information.¹²
- iii) **Privacy metadata** – this refers to information 'tags' that can be attached to personal information during processing. These tags contain

⁹ <http://www.privacy.gov.au/materials/types/download/8688/6527>

¹⁰ See Green paper, paragraphs 7.56 and 7.60

¹¹ See the Office's submission Towards Government 2.0 Issues Paper, p 8,

<http://www.privacy.gov.au/materials/types/downloads/9388/6926>

¹² See *Privacy Enhancing Technologies: A Whitepaper for Decision Makers* and published by the Dutch Government, see www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf

additional information such as the source of the information, the consent obtained, how it may be used and the policies to which it is subject. Personal information can also be assigned particular conditions or 'obligations' which detail the length of time that information may be retained and whether the person has given consent for the information to be disclosed to any third parties.¹³

- iv) **Privacy management systems** – these allow individuals to find out the privacy practices or processing policies of agencies that handle personal information and see if these match their preferences. The systems can improve the transparency of the information processing for the individual¹⁴.
- v) **Anonymising tools** – these include tools that hide the IP address or email address of the individual.¹⁵

17. The Office notes that a range of personal information is collected by the AEC for electoral purposes and information is not limited to what is publically available on the roll. The use of PETs is important for online transactions to reduce the possibility of hackers and identity thieves inappropriately accessing personal information while it is being transmitted or stored.

Proof of identity requirements

18. The Green Paper considers what changes could be made to 'proof of identity' requirements to improve enrolment processes.¹⁶ The Office recognises evidence of identity as an important part of enrolment processes in preventing fraud and in increasing the integrity and accuracy of the roll. As such, identity documents must meet appropriate integrity requirements and identity verification protocols should be sufficiently robust to minimise identity theft and promote public confidence and trust.

19. The Office supports the expansion of the current tier 1 evidence of identity documents beyond a driver's licence. Allowing the use of other appropriate documents in tier 1 would give more flexibility to individuals in the personal information they need to or can disclose to meet enrolment requirements. Including alternative documents that meet identity integrity requirements, such as Australian passports or Medicare cards, would also enable a broader range of individuals to meet the requirements for enrolment and improve roll integrity.

20. Consideration should also be given to the methods of identity verification used. For example, identity verification may be more privacy invasive where it involves the retention of identity records, rather than simply

¹³ UK Information Commissioner's Office, *Privacy by design*, November 2008, p9, see www.ico.gov.uk/about_us/news_and_views/current_topics/privacy_by_design.aspx.

¹⁴ *Privacy Enhancing Technologies: A Whitepaper for Decision Makers* published by the Dutch Government, see www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf.

¹⁵ UK Information Commissioner's Office, *Privacy by design*, November 2008, p9, see www.ico.gov.uk/about_us/news_and_views/current_topics/privacy_by_design.aspx.

¹⁶ See Green Paper, paragraph 7.67

recording that an individual has met the requisite standard.¹⁷ ‘Once only’ proof of identity, where an individual is required to prove their identity on enrolment only,¹⁸ is also privacy enhancing as the continuing need for collection of identity documentation would be reduced over time.

21. As part of the changes to the identity verification framework, guidelines concerning the security, handling and the destruction of information should be developed. These matters could be examined in a privacy impact assessment of proposals to change the identity verification framework, as noted below.

Special enrolment arrangements for silent electors

22. The Green Paper seeks comment on whether silent elector provisions sufficiently protect those whose safety is under threat. Existing arrangements enable electors to request that their address not be shown on the publicly available roll. Instead only their name and electoral division appear. Silent elector status is not granted automatically and valid concerns for safety must be demonstrated, such as risk of domestic violence. The Office considers the ability for electors to enrol as silent electors to be an important privacy protection where an individual has concerns over their personal safety or that of their family.
23. One option canvassed in the Green Paper is to allow silent electors to suppress their name as well as address on particular roll products. The Office notes that the requirement to publish silent electors’ names and electoral divisions may discourage electors from enrolling where they genuinely hold grave fears for their personal safety. Any broadening of the silent elector provisions needs to be balanced against the principles of transparency and integrity of the roll. The Office would welcome the opportunity to engage in further discussion about future proposals to address this issue.

Harmonisation of enrolment requirements and processes

24. Under joint roll arrangements, the Commonwealth is able to share personal information for the purposes of updating the electoral roll with the State and Territory electoral commissions. Variations in the qualifications and processes for enrolment across jurisdictions have led to divergence between the rolls and complexity for electors who may not understand the differences in requirements.¹⁹
25. The ways in which personal information is shared between jurisdictions to update the electoral roll, should be considered in light of recommendation 16-3 in the Australian Law Reform Commission’s recommendations to amend the Privacy Act in its Report 108 *‘For Your Information: Australian*

¹⁷ See, eg, Office of the Privacy Commissioner of Canada, *Collection of Driver’s Licence Numbers Under Private Sector Privacy Legislation: A Guide for Retailers* (December 2008), at www.privcom.gc.ca/information/pub/guide_edl_e.asp.

¹⁸ See Green Paper, paragraph 7.72

¹⁹ See Green Paper, paragraphs 7.98 – 7.99

Privacy Law and Practice (the ALRC Report). Recommendation 16-3 generally provides that the Commonwealth, state and territory electoral commissions and privacy commissioners should develop protocols to address the collection, use, storage and destruction of personal information shared for the purposes of the continuous update of the electoral roll.²⁰

26. The Australian Government has accepted recommendation 16-3 in its first stage response to the ALRC Report. The Government has stated in the response that it supports the development of more consistent privacy protections in relation to the sharing of personal information for the continuous update of the electoral roll. The Government has also indicated that it supports data-matching occurring with strong privacy protections in place.²¹
27. Generally, the Office would support schemes to harmonise elector enrolment that are transparent and have appropriate privacy protections. Enrolment requirements should provide consistent robust privacy protections and require that the same level of confidence in identity evidence is met across jurisdictions. Common standards are important if more information is to be shared between the commonwealth and states as well as between electoral commissions and commonwealth and state agencies.
28. The Office notes comments in the Green Paper concerning the development of a single, common electoral roll for enrolment processes.²² A common electoral roll would increase clarity for electors as to how their personal information is being used and shared between agencies by removing the uncertainty generated by jurisdictions with different requirements and processes. Further, reducing the number of data repositories containing comparable elector information into a single common roll with robust security protections could be privacy enhancing in that the number of large repositories containing similar amounts of personal information would be reduced.

Access to electoral roll information

29. The Green Paper seeks comment on whether further limitations should be placed on access to information on the electoral roll.²³ The Office supports the Green Paper's focus on the importance of privacy protections as part of considerations of access to information on the electoral roll beyond that which is publicly available.²⁴

²⁰ See ALRC Report paragraph 16.154 and Recommendation 16-3 (<http://www.austlii.edu.au/au/other/alrc/publications/reports/108/>)

²¹ See Australian Government First Stage Response, page 35 (<http://www.dpmc.gov.au/privacy/alrc.cfm>)

²² See Green Paper, paragraph 7.103

²³ See Green Paper, page 111

²⁴ See Green Paper, paragraphs 7.105 – 7.106. Subsection 90B(7) of the Electoral Act limits access to information on the electoral roll beyond an elector's name and address.

30. Information on the electoral roll is collected to produce and maintain an accurate record of those who are entitled to participate in the electoral process. The community has a strong expectation that this information will only be used for electoral purposes. A gradual expansion of uses risks undermining the community's trust in the handling of personal information and may jeopardise participation in electoral processes.
31. The Office has previously noted that a range of agencies can obtain access to additional information on the electoral roll which is not publicly available and use it for regulatory, law enforcement and public revenue purposes.²⁵ Given the mandatory nature of enrolment, it is appropriate that access to this additional information on the electoral roll remain relatively narrow.

REGISTRATION OF PARTIES, AND CANDIDATE NOMINATIONS (Chapter 8)

Regulation of political parties

32. The Green Paper seeks comment on whether the laws and regulations covering political parties and the way they are administered and organised should be changed.²⁶
33. The Office supports the proposal in the Green Paper about the introduction of requirements that registered political parties comply with privacy guidelines developed by the AEC to govern their handling of personal information (for example, donors' personal information, or personal information obtained from the electoral roll).²⁷ The Office recommended this approach in its submission on the *Electoral Reform Green Paper- Donations, Funding and Expenditure*²⁸. These guidelines could facilitate good privacy handling practices by, amongst other things, requiring political parties to clearly inform individuals of how their personal information will be used and allowing individuals to access and correct any incorrect personal information held about them.
34. The Office considers the ALRC Report to be relevant to discussions about amendments to laws and regulations covering the administration and acts of political parties. The Privacy Act does not currently cover the handling of personal information by registered political parties. In its report, the ALRC recommended removing the exemption for registered political parties from the Privacy Act.²⁹

²⁵ See for example, the Office's submission to the Australian Law Reform Commission's Review of Privacy - Issues Paper 31, February 2007 available at <http://www.privacy.gov.au/materials/types/submissions/view/6757>

²⁶ See Green Paper, page 117

²⁷ See Green Paper, paragraph 8.24

²⁸ See <http://www.privacy.gov.au/materials/types/submissions/view/6690>

²⁹ See paragraphs 41.54- 41.61 and Recommendation 41- 1 of the ALRC Report. (<http://www.austlii.edu.au/au/other/alrc/publications/reports/108/>)

POLLING (Chapter 11)

Postal vote applications issued by political parties

35. The Green Paper notes that privacy concerns have been raised about political parties capturing the personal details of voters who direct their application for a postal vote through a political party. The AEC considers that it is common practice for major political parties to undertake large-scale reproduction and distribution of their own version of the official postal voting applications which are typically attached to campaign material.³⁰ The political party's mailing address is provided to electors for the return of their postal voting application. It has been observed that there is often no information in the political party's postal vote application material that tells the elector that their personal information will be collected and may be used later in the campaign to contact them.³¹
36. The Office suggested that the uses of personal information contained in postal vote applications should be open and transparent to the elector. This includes being told what happens to their voting-related data and who will be receiving it. The Office notes the sensitivity that may attach to personal information about a person's political opinion. This is reflected in the Privacy Act, which defines information about a person's political opinions as 'sensitive information'.³² To ensure community confidence in the handling of this sensitive information, any reforms to the handling of postal vote applications by political parties need to promote and respect the privacy of the individual voter.
37. The guidelines referred to in paragraph 34 above, could also cover the handling of electors' personal information as part of the postal vote application process.

PRIVACY IMPACT ASSESSMENTS

38. Finally, the Office suggests Privacy Impact Assessments (PIA) be conducted in relation to any proposed reforms to help identify and address potential privacy issues associated with changes to the national electoral architecture that impact on the management of personal information.
39. PIAs, updated at key stages of a project, can be an important tool in project risk management. The overarching benefit of a PIA is that the identification and analysis of privacy impacts during a project's design phase can assist in determining the appropriate management of any potentially negative impacts. A project that underestimates privacy impacts can place its overall success at risk by not meeting the expectations of the community as to how personal information may be handled. PIAs are another aid to engendering community trust in new proposals.

³⁰ JSCEM, *Inquiry into the 2007 Federal Election*, paragraph 7.124 Inquiry report available at: <http://www.aph.gov.au/house/committee/em/elect07/report2.htm>

³¹ See Green Paper, paragraph 11.25

³² See section 6(1) of the *Privacy Act 1988 (Cth)*. Under NPP10, sensitive information is given a higher level of privacy protection than other types of personal information

40. The Office has a Privacy Impact Assessment Guide providing an introduction to the PIA process.³³ The Guide describes the purpose and general features of a PIA. The Office considers that it would be good privacy practice to undertake PIAs in relation to reform proposals that impact on the management of personal information.

³³ See <http://www.privacy.gov.au/publications/pia06/index.html>