



Our reference: 89-73-10
Your reference: gals5069

Committee Secretary
Joint Standing Committee on Electoral Matters
Department of House of Representatives
Parliament House
CANBERRA ACT 2600
AUSTRALIA

Dear Secretary

Inquiry into the Conduct of the 2001 Federal Election - Review of sections 89-92 of the Electoral Act 1918 (Access and use of the electoral roll)

Please find attached a supplementary submission to this Review, made in addition to the submission already provided by my Office and dated 22 July 2002. This supplementary submission discusses areas of concerns beyond those already raised with the Committee.

If you wish to discuss any details of either submission or require further information from this Office in relation to the Review, please contact Ms Barbra Luby on (02) 9284 9874.

Yours Sincerely

Malcolm Crompton
Federal Privacy Commissioner

1 October 2002

Joint Standing Committee on Electoral Matters	
Submission No.	164
Date Received	3/10/02
Secretary	

**JOINT STANDING COMMITTEE ON ELECTORAL MATTERS
INQUIRY INTO THE CONDUCT OF THE 2001 FEDERAL ELECTION**

**SUPPLEMENTARY SUBMISSION FROM THE FEDERAL PRIVACY
COMMISSIONER**

**Concerning ss.89-92 of the *Electoral Roll 1918*
(Access and use of the Electoral Roll)**

October 2002

Summary of Recommendations

Recommendation 1

That the Committee reaffirm that the Electoral Roll's primary purpose is to promote free and fair elections by providing an accurate and reliable record of qualified voters, and that any use or disclosure of the personal information contained in the roll should be for this primary purpose.

Recommendation 2

That further expansion to the range of secondary purposes for which the Electoral Roll can be used be subject to strict scrutiny, public discussion and specific endorsement by Parliament.

Recommendation 3

Where additional secondary purposes are permitted, efforts should be undertaken, including possibly by clear notice placed on the AECs website and at electoral offices, to ensure that individuals are made aware of how their personal information may be used and to whom it may be disclosed.

Recommendation 4

That firm grounds for any expanded data-matching or powers of demand be established prior to such provisions being considered.

Recommendation 5

Should further data-matching be deemed necessary, consideration be given to identifying a small number of optimal data sources, rather than legislate to provide demand powers over any public sector agency.

Recommendation 6

That strict oversight be applied to any current and future data-matching activities, including resources to enable the Office of the Federal Privacy Commissioner to discharge any increase in responsibilities thoroughly.

Recommendation 7

That Parliament consider providing the same end-use restrictions on personal information contained in the Electoral Roll, whether it is provided electronically or in printed form.

Recommendation 8

Use or disclosure of data derived from the electoral roll by political parties for commercial purposes should be prohibited and that greater clarity be afforded to the permitted

purposes prescribed by the Electoral Act. Proposals by the AEC to this current Inquiry to limit the types of personal information available to political parties are supported.

Recommendation 9

That the proposal to make the Electoral Roll available in a restricted form via the internet be considered further.

Recommendation 10

That the Electoral Act be amended such that the Electoral Roll is not available for sale.

Recommendation 11

That the AEC be asked to develop options for allowing limited extension of the silent elector provisions in the context of agreed end-use restrictions.

Introduction

1. The integrity of the Electoral Roll is integral to the democratic process in Australia. It is difficult to challenge the view that the Electoral Roll should accurately reflect the true status of those who are entitled to participate in the democratic process. Further, the principle that the Electoral Roll is available for examination by citizens is a longstanding one, and one that promotes a sense of openness and transparency in the democratic process.
2. Similarly, our democratic process is built upon the premise that it is compulsory to enrol to vote upon reaching 18 years of age. At this point, the individual submits to the Australian Electoral Commission (AEC) personal information for inclusion in the Electoral Roll. What happens to this personal information after this point though, will often remain a mystery to most Australians. Most citizens remain unsure as to how their personal information contained in the Electoral Roll is used, for what purposes and by whom. Such a situation serves neither to advance the privacy rights of Australians, nor reassure electors that their personal information is treated appropriately, thus potentially undermining confidence in the process of electoral registration.
3. The Information Privacy Principles (IPPs) contained in section 14 of the *Privacy Act 1988* (Privacy Act) require Commonwealth agencies to use and disclose personal information only for the purpose for which it was collected unless certain exceptions apply. Individuals are also entitled to know when and why their personal information is used and to whom it is disclosed, as well as having the right to access and, where necessary, correct personal information about them contained in agency records.

Primary Purpose of the Electoral Roll

4. The primary purpose for collecting personal information for inclusion in the Electoral Roll is to produce and maintain an accurate record of those who are entitled to participate in the electoral process, thus minimising electoral fraud and promoting the valid and lawful participation of all eligible citizens in the democratic process. Clearly, such objectives are of merit and serve the public interest.
5. Public inspection of the roll enables individuals to check the accuracy of their own enrolment details, to check the correctness of the enrolment of others and, in doing so, to prevent electoral fraud. Making the Electoral Roll available for such inspection is directly related to the primary purpose of maintaining the Electoral Roll.
6. There is, however, a balance required between making the Electoral Roll available for inspection and promoting the individual's right to privacy. This balance would seem to be promoted where protections exist that are effective in ensuring that personal information is used and disclosed only for the primary purpose of the Electoral Roll. However, there is increasing evidence that the protections afforded by both the Privacy and Electoral Acts are failing to provide this adequate protection.
7. The Committee acknowledged that concerns have emerged regarding the public availability of the Electoral Roll in its report of May 2001 *User Friendly, not Abuse Friendly: Report of the Inquiry into the Integrity of the Electoral Roll* ('the *User Friendly Report*'). These concerns were also mirrored by the

AEC,¹ which confirmed that it was aware that the Electoral Roll is being used for a range of purposes inconsistent with the intention of the Electoral Act.

8. This Office shares these concerns. In various previous submissions and public comment, this Office has strongly argued that protections may be necessary to ensure that the Electoral Roll is not used inappropriately for purposes unrelated to the promotion of the electoral process.² Australians should have confidence when enrolling to participate in their democratic system that the personal information they provide will only be used for that purpose, unless extenuating circumstances apply.
9. The Committee's opinion of May 2001 that "...action on this issue should not be delayed much longer"³ was welcome by this Office when the report was published, and the AEC's recent work in progressing a review of the relevant sections of the Electoral Act (ss.89-92) is also acknowledged.⁴

Recommendation 1

That the Committee reaffirm that the Electoral Roll's primary purpose is to promote free and fair elections by providing an accurate and reliable record of qualified voters, and that any use or disclosure of the personal information contained in the roll should be for this primary purpose.

Secondary Purposes

10. The Privacy Act generally prohibits personal information being used or disclosed for any purpose other than that for which it was collected except in very limited circumstances. One exception to this general prohibition is where a use or disclosure is required or authorised by law.⁵ Over the past ten to fifteen years, successive Parliaments have expanded the secondary purposes for which the roll can be used under the Electoral Act. Schedule 2 of the *Electoral and Referendum Regulations 1940* lists 21 agencies that are currently permitted access to the Electoral Roll, while Schedule 3 lists the permitted purposes for which any personal information collected from the Electoral Roll may be used.
11. The Australian National Audit Office in its recent report of April 2002, explained that:

Most electors would be unaware of that personal information they have provided in order to enrol, and data about them extrapolated from AEC systems, is being provided to external users for a range of secondary purposes.⁶
12. This state of affairs sits somewhat uncomfortably with principles of good privacy. As stated above at paragraph 3, an underlying objective of the Privacy Act is to provide individuals with a right to know what happens to their personal information. Where the range of permitted secondary purposes is allowed to expand, it becomes increasingly difficult for individuals to track the range of organisations who are able to collect and use information that the individual had understood was

¹ *User Friendly Report* at p.2.135 (<http://www.aph.gov.au/house/committee/em/ElecRoll/Report.htm>)

² See, for example, the Privacy Commissioner's Submission to the Joint Standing Committee in Electoral Matter's *Inquiry into the Integrity of the Electoral Roll* in 2000.

³ *User Friendly Report* at p.2.143 (<http://www.aph.gov.au/house/committee/em/ElecRoll/Report.htm>)

⁴ *AEC Review of ss.89-92 of the Electoral Act* (As provided in Attachment D of the AEC's submission to this Inquiry). (<http://www.aec.gov.au/content/why/committee/subs/sub147/sub147d.htm>)

⁵ IPP 10.1(c) permits other *uses*, while 11.1(d) permits other *disclosures*, where either is required or authorised by law.

⁶ ANAO Audit Report 42 2001-2002 *Integrity of the Electoral Roll*, at p.543.

provided to the AEC for the purpose of maintain an Electoral Roll and facilitating that individual's participation in the electoral system. Research shows that people regard unrelated use of their personal information as an invasion of privacy.⁷ In regard to the Electoral Roll, 70% of people are opposed to it being used for marketing purposes.⁸

13. A review of Schedule 3 (the permitted purposes of collection) is due to take place towards the end of 2003. This Office looks forward to this review and suggests that it include appropriate public consultation.

Recommendation 2

That further expansion to the range of secondary purposes for which the Electoral Roll can be used be subject to strict scrutiny, public discussion and specific endorsement by Parliament.

Recommendation 3

Where additional secondary purposes are permitted, efforts should be undertaken, including possibly by clear notice placed on the AECs website and at electoral offices, to ensure that individuals are made aware of how their personal information may be used and to whom it may be disclosed.

The Need for Specific Use and Disclosure Limitations in the Electoral Act

14. Outcomes from any review of access to the Electoral Roll will also be important because of the way that the Privacy Act interacts with other federal and state legislation in providing the privacy framework for Australians. This interaction is spelt out at this point in more detail.
15. The Privacy Act applies the Information Privacy Principles (IPPs) to the AEC in its management of the Electoral Roll and, for those private sector organisations subject to its jurisdiction, the National Privacy Principles (NPPs) apply to collection and use of personal information from the roll.
16. These principles are the basic minimum standards for the handling of personal information. The principles generally require individuals to be told at the point of collection about how personal information will be used and then set use and disclosure limitations based in part on what the individuals have been told.
17. The principles include provisions that allow them to be flexible and responsive to other laws. They permit additional uses and disclosures of personal information where these are authorised by law. They also allow for and respond to higher or more specific privacy protections in other laws.
18. For example, if another law prevented collection of personal information, it would also be 'unlawful' collection in terms of IPP 1.2 and NPP 1.2.
19. In the absence of restrictions on collection from sources such as the Electoral Roll the IPPs and the NPPs would permit the collection to proceed as lawful although they may then impose other requirements, for example those mentioned above.

⁷ Research conducted by Roy Morgan Research (<http://privacy.gov.au/publications/rcommunity.html#4.29>)

⁸ Research conducted by Roy Morgan Research (<http://privacy.gov.au/publications/rcommunity.html#4.30>)

20. As noted earlier, many Australians have expressed strong views about the re-use of personal information from the Electoral Roll for a range of commercial purposes. On the other hand, many organisations regard this information as publicly available and have built their businesses around its use. These organisations argue that there would be major economic impact in restricting access to the roll. I strongly support the proposed review of access to the Electoral Roll as the mechanism to have a full public debate that can then inform Parliaments consideration of the issues.

The Privacy Act Applies to Collection of Personal Information from all Sources

21. It is fair to note at this point that there is some uncertainty in the community about the way that the Privacy Act applies to generally available publications, that is information including some public registers that are 'out there' for free use. This is relevant to this submission because it appears that some organisations regard the Electoral Roll as a generally available publication from which personal information can be collected without meeting any privacy obligations.

22. The Privacy Act applies to personal information, which it defines as

'... information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.'

23. The definition makes no distinction between public and non-public information. It does not exclude information in public registers such as personal information in the Electoral Roll, land title registers or telephone books.

24. The Privacy Act also states that it applies to the collection of information by an organisation if it collects information for inclusion in a record or a generally available publication (section 16B(1)).

25. These provisions make it clear that the Privacy Act applies to the collection of personal information by an organisation regardless of whether it is collecting it from public or non-public sources. This means that an organisation will have to consider how the collection principles such as NPP 1, NPP 10 and the collection aspect of NPP 3 apply when it collects personal information from public sources, including public registers. It will also need to consider the requirements in NPP 5.2 to tell people, if they ask, about the sort of personal information it holds and how to collect it.

26. In addition, the remaining NPPs will apply to the personal information once the organisation has collected it and holds it in a record even if it collected the information from a public source (section 16B(2)).

Privacy Commissioner's Proposed Information Sheet

27. The NPPs are designed to apply in a very broad range of circumstances. The intention of the Privacy Act is that the NPPs should be applied in context. They do not provide detailed prescriptive rules unique to individual circumstances. The law is still new in the private sector context and there is not large body of experience to draw on in working out how the NPPs apply. The Office's approach at this stage is to focus on the provision of information through case notes about resolution of complaints, guidelines, information sheets and FAQs.

Consultation Paper for Information Sheet: Privacy and Collection of Publicly Available Personal Information

28. Against this background, the Office decided to prepare an information sheet on publicly available personal information because it was receiving a number of inquiries on the topic. Key inquiries include:

- Does the Privacy Act apply to personal information collected from public sources?
- Does an organisation have to notify individuals when it collects information about them from the Electoral Roll or other public register or from a telephone directory?

29. The work on the information sheet to date has involved the following:

- Consultations with key stakeholders including the business, consumer and privacy groups, based on a draft information sheet made available in November 2001;
- Further redrafting following submissions and further consultations based on a re-drafted information sheet March 2002;
- Yet more drafting, and a decision to undertake wider consultation, based on reference group submissions responding to the March draft;
- A consultation paper released in June 2002, to members of the Office list serve, to key stakeholders and via the Office's website with two months for comments;
- Over 70 submissions have received and are currently being considered.

Issues that the Office has been considering, and on which it sought feedback in its consultation paper, include:

- the requirements in NPP 1.2 for collection to be by fair and lawful means – for example, would it be collection by fair means for an organisation to collect personal information for purposes that are inconsistent with the purpose for which a public register is established. In some cases the limitations will be explicit, for example, the Electoral Act governs access to the Electoral Roll in various formats, while the Corporation Act 2001 sets out limits on the use of personal information on share registers and other registers established under that Act. In other cases there will no explicit limitations.
- the requirement in NPP 1.5 to provide notice of certain matters when collecting from someone else (other than the individual concerned). The questions here include what factor to consider in deciding whether notice is reasonable in the circumstances and when the obligation starts to apply in relation to generally available publications such as a newspaper or the white pages. For example, the requirements would not apply to a telephone book on a desk but there may be some circumstances where there are requirements.

Next Steps in the Office's Work on Collection from Publicly Available Personal Information

30. The Office is currently considering the submissions received. It recognises the concern that the paper has generated particularly in the direct marketing and fund raising sectors and will be consulting particularly with this sector and with consumers before issuing further advice.

Data Matching Purposes

31. Data-matching can be a powerful administrative and law enforcement tool. It allows information from a variety of sources to be brought together, compiled and applied to a range of public policy purposes at vastly lower cost than manual methods.
32. Importantly though, data-matching has the potential to pose risks to the privacy of those whose data is be matched. The Privacy Commissioner's guidelines for *The use of data matching in Commonwealth administration* explain these risks:
 - It may involve the use of data for purposes other than those for which it has been supplied or obtained and those purposes may be outside the reasonable expectations of the people the information is about. A basic privacy principle is that personal information should be used only for the purpose for which it was obtained. Departures from this principle need to be justified on strong public interest grounds.
 - Data-matching can involve the automatic examination of the personal information of many thousands of people in relation to whom no action is warranted. This may be done without the knowledge of the people whose information is being scrutinised.
 - Data-matching relies on agencies gaining access to large amounts of information, some of which may be personal information, from other sources. Agencies may be inclined to keep unmatched information for possible future use even though it has no immediate application.
 - It is far from perfectly reliable. A data-matching program may fail to distinguish between individuals with similar personal details; input data may be faulty; errors may be made in programming; or difficulties may be caused if similar fields in different databases are not precisely comparable.
33. Protection against these risks is, in part, provided by the *Data-matching Program (Assistance and Tax) Act 1990*. While this Act applies to the use and disclosure of tax file numbers, guidelines have been drawn up for all agencies to refer to when pursuing data-matching activities.⁹
34. In the context of the Electoral Roll, it may be appropriate that any data-matching only be pursued where 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 may be required to ensure that redundant or unmatched personal information is not retained.
35. Section 92(1) of the Electoral Act permits the AEC to collect, from other agencies, "all such information as the Electoral Commission requires in connexion with the preparation, maintenance or revision of Rolls". The scope of what is meant by "other agencies" is, by this Office's understanding, interpreted quite narrowly.
36. This Office understands that the AEC routinely draws on its authority under s.92(1) to collect and match personal information with Australia Post, Centrelink, the Department of Immigration and Multicultural and Indigenous Affairs and various, although limited, State government agencies.¹⁰

⁹ Data-matching guidelines are available at:
http://privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.word_file.p6_4_23.15.doc

¹⁰ *User Friendly* Report at p. 249 and 2.50 (available at:
<http://www.aph.gov.au/house/committee/em/ElecRoll/Report.htm>)

This data-matching is required for the purposes of Continuous Roll Update (CRU), whereby data is collected from various Commonwealth and state sources and compared to data held on the Electoral Roll, for the purpose of ensuring that data held on the Roll is consistent with these other sources.

37. In the AEC's submission to the *User Friendly Inquiry*,¹¹ the AEC envisaged an extension of its data-matching capacity, through legislative amendment, to include, for example, the ability to match data held by the Australian Taxation Office. The AEC also indicated that in drafting a proposal to extend its data-matching capabilities, it would consult with the Privacy Commissioner.
38. In returning to discussion of its s.92(1) powers in its recent review of ss.89-92, submitted as Attachment D to this current Inquiry, the AEC has indicated that it seeks to increase its powers of demand for personal information from other government agencies, particularly at state and local government level. In particular, AEC Recommendation 9 calls on section 92 to be amended to expand the demand powers of the AEC such as to apply to any level of government (Commonwealth, state, local), while, under Recommendation 10, failure to comply would result in an offence being committed. However, in regard to addressing privacy issues, the AEC comments in its submission to this current Inquiry that it "...may be necessary to undertake consultation with the Privacy Commissioner".¹²
39. These two recommendations seem to significantly increase the AEC's power to collect personal information from any government body in Australia, without the individual being aware that such collection may occur. As such, it is the view of this Office that there is a strong need to ensure privacy protections are in place well before any such additional collection powers are granted. At the very least, care should be exercised such as to ensure that such a proposal is not interpreted throughout the community as a *de facto* national database, whereby a centralised government database collects personal information about individuals, from disparate and non-disclosed sources, as they go about their daily lives. This Office remains keen to be consulted on any proposal to increase or third-party data collection for the Electoral Roll.
40. Further, before granting such comprehensive data collection powers, it may be appropriate for a more thorough examination of why such powers are considered necessary. While the CRU initiative seems merit worthy, the ANAO audit concluded that a suite of 8 types of Commonwealth and State/Territory agencies could be identified as optimal data sources.¹³ Accordingly, it seems possible that broad and general powers of demand, including from any agency or data source, are excessive and unnecessary for the purposes of CRU.
41. It may also be worth considering what precedent such broad legislation may set. In particular, it seems worth asking whether other agencies might feel equally justified in having such extensive powers of demand. Only when such unintended impacts have been assessed, can any increment such as that sought by the AEC be decided sensibly.
42. Where extended data-matching or data collection is carried out for the purposes of maintaining the Electoral Roll, secondary purposes should be limited to the narrowest possible range and only

¹¹ *ibid* at p.254

¹² AEC *Review of ss.89-92 of the Electoral Act* (As provided in Attachment D of the AEC's submission to this Inquiry) at p.61 (available at: <http://www.aec.gov.au/content/why/committee/subs/sub147/sub147d.htm>)

¹³ ANAO Audit Report 42 2001-2002 *Integrity of the Electoral Roll*, at p.2.40. The ANAO, at Table 3 lists these 8 "Desirable CRU data sources" as: Australia Post; Centrelink; Motor Transport; Fact of Death files; Rental Bond Boards; Public Housing Authorities; State Revenue and/or Land Titles Offices; and DIMIA. (available at: <http://www.anao.gov.au/WebSite.nsf/Publications/4A256AE90015F69BCA256B9E007B5F52>)

approved where there is a strong public interest. It should be acknowledged that the accuracy and quality of data held in the Electoral Roll could tempt various third-parties to seek access in a manner incompatible with the primary purpose of the Electoral Roll.

43. If expanded data-matching activities, or greater demand powers, are granted to the AEC, then this should be accompanied by complementary restrictions on disclosure and end-use. In particular, where the AEC is granted greater collection powers, this should not necessarily be accompanied by reciprocal data exchanges with the source agency; any flows of personal information should remain one-way, from the source agency to the AEC.

Recommendation 4

That firm grounds for any expanded data-matching or powers of demand be established prior to such provisions being considered.

Recommendation 5

Should further data-matching be deemed necessary, consideration be given to identifying a small number of optimal data sources, rather than legislate to provide demand powers over any public sector agency.

Recommendation 6

That strict oversight be applied to any current and future data-matching activities, including resources to enable the Office of the Federal Privacy Commissioner to discharge any increase in responsibilities thoroughly.

Technological Developments

44. Developments in information technology have enhanced the ease with which data may be copied, modified, cross-matched and disseminated. These developments have out paced the important restrictions on unauthorised secondary disclosures contained in the Electoral Act.
45. The widespread availability of scanning equipment and optical character recognition (OCR) software allows hardcopies of the Electoral Rolls to be converted easily to digital form; it is no longer necessary to even have to manually key data into a computer. That the Electoral Roll can only be purchased in printed form, rather than on disk or tape, offers only marginal protection against the personal information being copied, re-sorted and manipulated for purposes not at all related to promoting transparency in the electoral process.
46. This is a significant concern given the lack of legislative controls on the use of printed copies of the Electoral Roll. While ss.91A and 91B restrict the uses of Electoral Roll in its *electronic form*, no such restriction apply to print or hardcopy form. This anomaly significantly undermines the protections afforded to personal information by the Electoral Act.
47. In drafting the Privacy Act, Parliament deliberately chose a *technology-neutral* approach, such that the technology used in the collection, storage, dissemination and so forth, of personal information is, in effect, irrelevant for the purposes of the Privacy Act. Protections afforded by the Privacy Act are intended to be independent of technology. Such an approach recognised the dynamic nature of information and communication technologies and the difficulties that could stem by attempting to continually re-draft and amend legislation so as to account for technological developments. It

appears that these difficulties, while reduced in the case of the Privacy Act, are apparent in regard to the end-use restriction provisions of the Electoral Act.

48. The AEC has submitted to this Inquiry a recommendation that the Electoral Act be amended such that references to forms of medium be omitted from the provisions of that Act.¹⁴ Such an amendment may result in equal protections being afforded to the Electoral Roll regardless of the medium on which it is stored and manipulated.
49. In its recent examination of the integrity of the Electoral Roll, the ANAO recommended that the AEC give priority to its review of sections 89-92 of the Electoral Act such as to take account of the "...risk inherent in current developments in computer technology."¹⁵ While the ANAO did not go as far as to pre-empt the AEC's eventual recommendation on this matter, it is implicit in the ANAO's recommendation that technological developments have rendered the end-use restrictions of the Electoral Act suspect.
50. Given the generally positive experience with technology-neutral legislation within the Office of the Federal Privacy Commissioner, and the manifest problems of the current medium-specific provisions in the Electoral Act, amendments to this latter Act that remove references to forms of media may be effective in overcoming the difficulties associated with attempting to enforce two sets of rules.

Recommendation 7

That Parliament consider providing the same end-use restrictions on personal information contained in the Electoral Roll, whether it is provided electronically or in printed form.

Access and Use by Political Parties

51. This Office has previously expressed concern about the lack of privacy protections afforded to personal information held by political parties.¹⁶ Under section 91 of the Electoral Act, the AEC is required, after each general election, to provide copies of the Electoral Roll, in electronic form if requested by the recipient, to registered political parties, each Senator and each member of the House of Representatives. The permitted purposes for which this information may be used include:
 - any purpose in connection with an election or referendum; and
 - research regarding electoral matters; and
 - the performance of a Senator or member of the House of Representatives of his or her functions in that role¹⁷
52. The purposes are general in nature – in effect therefore, there are no specific restrictions on how political parties may use any personal information once they have collected it from the Electoral

¹⁴ AEC *Review of ss.89-92 of the Electoral Act* (As provided in Attachment D of the AEC's submission to this Inquiry) Recommendation 1, page 5 (available at:

<http://www.aec.gov.au/content/why/committee/subs/sub147/sub147d.htm>)

¹⁵ ANAO Audit Report 42 2001-2002 *Integrity of the Electoral Roll*, at p.5.53.

¹⁶ Submission to the Joint Standing Committee in Electoral Matter's *Inquiry into the Integrity of the Electoral Roll* in 2000; Submission to the House of Representatives Standing Committee on Constitutional and Legal Affairs *Inquiry into the Privacy Amendment (Private Sector) Bill 2000* (available at:

<http://www.privacy.gov.au/publications/hor.pdf>); Submission to the Senate Legal and Constitutional Legislation Committee *Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 200* (available at: <http://www.privacy.gov.au/publications/subbill.pdf>).

¹⁷ s.91A(1A) prescribes permitted purposes for a Senator or member of the House of Representatives, while s.91A(2), in effect, mirrors these permitted purposes for political parties.

Roll. Further, an individual currently has no right to know what personal information may be held on them by political parties, let alone rights to access and correct that information, because no such provisions exist in the Electoral Act and political parties are exempt from the Privacy Act.

53. In order to achieve an appropriate balance between the privacy rights of individuals and the ability of political parties and individuals to contribute to the democratic process, individuals should be conferred the right to access records held by political parties and to obtain correction or deletion of that information. Individuals should also be allowed to know when and to whom political parties have disclosed information to third parties.
54. Further, the end-use restrictions imposed on political parties in regard to personal information sourced from the Electoral Roll are particularly broad and, to some degree, vague. It is conceivable that political parties could, given the general wording provided in the Electoral Act, use this personal information for purposes not intended by Parliament when passing the legislation. An article in the *Adelaide Advertiser* of 26 September 2002, discusses this point very succinctly under the heading **Public's right to privacy, flouted by political parties**.¹⁸ For this Committee's convenience, a copy of this article is supplied at Attachment A.
55. It may be necessary to consider prohibiting use of the Electoral Roll to validate personal information contained in commercial databases, or "cleans" data held commercially, as well as where personal information is merged with other databases.
56. The ANAO's view that, in the context of access and use by political parties "...the absence of end use restrictions on data from the electoral roll could increase the potential for electoral fraud"¹⁹ is also worth noting.

Recommendation 8

Use or disclosure of data derived from the electoral roll by political parties for commercial purposes should be prohibited and that greater clarity be afforded to the permitted purposes prescribed by the Electoral Act. Proposals by the AEC to limit the types of personal information available to political parties are supported.

Internet Access for validation of own and others enrolment

57. The AEC has recommended that the Electoral Roll be made accessible for confirmation of data purposes via the internet. Under this proposal, personal information already known to the enquirer would be confirmed, or otherwise, as being on the Electoral Roll. No personal information would be disclosed.
58. This proposal may have some merit inasmuch as it limits the use and disclosure of personal information for purposes largely within the intent of the primary purpose of the Electoral Roll.
59. We note that in addition to the above proposal, the AEC has also proposed amendment to the Electoral Act that would prohibit the sale of the Electoral Roll. Such an amendment could be pursued regardless of the internet initiative and would seem to offer a strong chance of reducing the current mis-use of the Electoral Roll as it would no longer be possible to collect, re-sort, disseminate and so forth, personal information contained in the Electoral Roll en masse.

¹⁸ Adelaide Advertiser, Thursday 29 September 2002, pg.20.

¹⁹ ANAO Audit Report 42 2001-2002 *Integrity of the Electoral Roll*, at p.5.33.

Recommendation 9

That the proposal to make the Electoral Roll available, in limited circumstances, be considered further.

Recommendation 10

That the Electoral Act be amended such that the Electoral Roll is not available for sale.

Silent Elector Provisions

60. Under s.104 of the Electoral Act, individuals who fear that their personal safety may be at risk, can request for address not to be shown on Electoral Roll for the subdivision for which the enrolment is claimed. In effect, these individual's become "silent electors".
61. In its recently completed audit of the integrity of the Electoral Roll, the ANAO reported that an increasing number of people are requesting, and being granted, silent elector status on the grounds of privacy, rather than a threat to personal safety.²⁰ The ANAO further suggested that "...there would be merit in reviewing and updating the requirements for silent elector status..." and that "[b]roadening the criteria for silent elector status could provide a means to ensure citizens, in order to protect their privacy, have an option other than refusal to enrol and to participate in the democratic process."²¹
62. While the intent of the ANAO's suggestion in this regard are privacy sensitive, for such an initiative to be an effective solution to privacy concerns, the option of silent enrolment would need to be available to the whole community. Were this option taken up by large numbers of individuals, then the principles of transparency and openness in the electoral administration process could be compromised.
63. Accordingly, this Office does not necessarily subscribe to the view that the broadening of silent elector provisions in the Electoral Act would be an appropriate response to privacy concerns. Rather, a limited extension of the silent elector provisions to permit applications on the grounds of privacy, when coupled with complementary end-use restrictions, would seem to offer greater potential to protect the privacy rights of electors.

Recommendation 11

That the AEC be asked to develop options for allowing limited extension of the silent elector provisions in the context of agreed end-use restrictions.

²⁰ *ibid* at p.5.48.

²¹ *ibid* at p.5.49.

ATTACHMENT A

Advertiser (Adelaide) Thursday 26/9/2002
General News Page 20
Circulation: 216,243
Size: 238.17 sq.cms.

Public's right to privacy, flouted by political parties



Dean _____

ONE of the most important tasks of any member of parliament is to represent his or her electors. This means more than sitting in the Parliament and speaking and voting. It means being available to the electors in the district, dealing with their problems and communicating with them.

To carry out these roles with the greatest efficiency and effectiveness, the MP needs a list of who is enrolled in the electorate. The obvious source for this is the electoral roll. All adult Australian citizens are required to enrol, so it should be a complete list for whom the MP is a "servant".

But how much information should be made available about the voters? The decision on this issue, one which raises important issues of privacy, is made by the Parliament. The Electoral Commission or Office simply administers the law.

In South Australia, the electoral roll includes your name and address - crucial for testing your right to receive a ballot paper on election day. No problem with that information going to members - they need it to represent you correctly. But the Electoral Act also specifies that the Electoral

Commissioner "may ... provide ... a prescribed authority" with your sex, place of birth and age band. There is an "escape clause" for the voters. They can ask for a "silent enrolment". That is if they can put a case that, as the Act puts it, if their address was included it "would place at risk the personal safety of the elector". The Commonwealth Act contains a similar provision.

But the Commonwealth Act goes much further. There is a joint electoral roll, used by both federal and state electoral authorities. The federal parliamentarians have set a much greater invasion of privacy. Each registered political party can obtain a copy of the whole Australian electoral roll. And what a source of information they are

allowed to have about you, the voters. Under the Act, the material provided to the parties contains your name, postal address, sex, date of birth, salutation, telephone number, census district, electoral district, local government area and Australia Post delivery point identifier.

What a goldmine for a political party which has the resources to use the latest technology in election campaigning. This "gift" to the parties can be in the form of a tape or disk, which makes computer manipulation into various sectors for targeted political campaigns very easy indeed. As most of the established political parties in Australia have federal registration, they have access to all of that very valuable information about you.

There are real privacy considerations in the way such detailed data are given to the parties, especially when used for the self-interest of the parties. The "silent" enrolment should be automatic for any person who asks for it. Further, the parties should only have access to names and addresses. The rest of the data should be considered as very private.

dean.jaensch@flinders.edu.au