Australian Privacy Foundation

Evidence to the Joint Standing Committee on Electoral Matters
Inquiry into the Electoral and Referendum Amendment (Maintaining Address) Bill 2011

Supplementary Submission

15 February 2012

Speaker Background

I am an eBusiness consultant of long standing, and a Visiting Professor in Computer Science at the ANU and in Law at UNSW. I am also a Member of Civil Liberties Australia. I am appearing before the Committee in my role as Chair of the Australian Privacy Foundation.

1. Introduction

The APF is an entirely voluntary organisation that advocates for the public interest in privacy. The Board and its Committees comprise volunteers with a range of professional backgrounds and expertise. They prepare proactive policy statements and reactive submissions that are carefully balanced and evidence-based, within the constraints applying in the particular circumstances, and the limited time of Board and Committee members.

The APF has submitted on electoral matters on multiple previous occasions, variously to this Committee, to another Committee of the Commonwealth Parliament, to the Victorian Electoral Commissioner and to the AEC.

The APF provided a submission to the Committee in relation to this Inquiry on 3 February. It was of necessity brief. It was prepared by several other members of the Board, but submitted over my signature. I had not previously been directly involved in the matter, but spent 7 hours yesterday preparing for this appearance.

We thank you for your repeated invitation to provide evidence, and note the importance of our evidence to you, as indicated by the Media Release of 13 February.

2. Preamble

The APF's Submission made clear that "the changes need to be assessed in the wider context". My first purpose is to draw attention to key aspects of that context, and to their consequences. I will then address the specifics of the Bill that is the subject of the Inquiry, within that context. Finally, I will draw attention to some procedural aspects of the matter.

(1) Mandatory Voting

Universal suffrage was fought for over an extended period. But, in Australia, the right to vote is tarnished by also being an obligation under s.245 of the Commonwealth Electoral Act. Many individuals want to vote for parliamentary representatives at every opportunity, some only on occasions, and others would sooner abstain from all elections. The last group is not only required to submit a voting form, but also subject to obligations in relation to enrolment under s.101, to exposure of personal data, to appropriation of personal data, and to enforcement actions.

Some individuals who would prefer to abstain from voting in elections are apathetic and unengaged politically, but others are active politically. There are many opportunities to participate in policy and in politics, and eDemocracy is creating even more avenues, and forcing further changes in representative democracy. The justification for compulsory enrolment and compulsory voting, as distinct from the right to vote, is increasingly unclear.

The right to vote is further tarnished by partisan behaviour in relation to electoral matters. When in power, parties that expect to get more votes through compulsory enrolment and voting seek to impose more heavily on people uninterested in voting. Parties that expect to be disadvantaged by high enrolment percentages and large voter turnouts, when in power, adapt the law to close the rolls early and adopt other devices to delay or obstruct enrolment.

(2) Address

The enrolment of electors appears to be based on "the address at which the person is living", e.g. s.99(3)(c). In systems that awarded the vote on the basis of real estate ownership, that approach was convenient and effective, because real estate is static and the government agency that manages electoral boundaries can reliably allocate voters to appropriate Rolls and parts thereof.

In systems that award the vote on bases other than ownership of real estate (such as citizenship and the absence of particular constraints, in this case as defined in s.93), address is much more problematic.

The concept "address at which the person is living" embodies a presumption that a person only lives in one place, all the time; or is reliably and legally associated with one place, at the time relevant to the determination of their voting rights in respect of any particular election. For many people, this is difficult, or ambiguous, or even unresolvable.

In particular, the following problems arise:

- Frequent Movers. In excess of 20% of the voting-age population change address during any given calendar year, some more than once. Many are in transition for a period of time, rather than being able to nominate an appropriate date, consistent with whatever law, policy and practice might apply. Only a small percentage is likely to consider advising the Electoral Office to be any kind of priority.
- Multiple Addresses. Many people have multiple tenable addresses. Some own or rent two or more properties and alternate between them. One set of considerations determines their residence for tax purposes, and other sets of considerations determine their 'address' for the purposes of interactions with various organisations. Politicians are only one of the special cases. Other people live most of their time somewhere other than where they call home. Beyond the traditional categories of shearers and fruit-pickers, there are people who 'follow the sun', tradesmen who spend five nights per week where the work is to be had – often one or more electorates away, seamen and road-workers who spend long periods away, and mining and drilling-rig workers who have long rotations in remote locations.
- No Tenable Address. Homeless vagrants are one category. Another is people who have the attitude 'home is where I hangs me hat', in American parlance 'drifters'. A sub-set of retirees are 'grey nomads' for much, and in some cases all, of the year, and cannot (and do not want to) predict where they will be at any given time. Bumper-stickers declaring variants of 'this is home' and 'my other home isn't' are increasingly evident on the roads.

In an attempt to cope with such realities, the notion of Itinerant Electors is created by s.96. This in no way relieves the individual of any responsibilities (and arguably adds to them), and forces the individual to remain linked to the electorates containing their last address, and only in extremis with the electorates with which the person "has the closest connection" (s.96(2A)).

One of the biggest problems that has to be confronted, and is directly relevant to the present Bill, is that the relevant address under electoral law is subject to definitions and interpretations quite different from those that apply to addresses used by other government agencies.

On its web-site at http://www.aec.gov.au/faqs/enrolment.htm#address, the AEC defines Real Place of Living as "including" "[a place where a person has] a fixed intention of returning for the purpose of continuing to live at this place". This is a bureaucratic invention and imposition that matches poorly to the realities of many people's worlds.

(3) The Untrustworthiness of the Electoral System

In order to administer a voting system, some personal data needs to be handled by the AEC. Under s.83, this comprises "surname, Christian or given names and place of living of each elector", but also "such further particulars as are prescribed". A search of the Regulations has not yet turned up the full list of data items that are captured, and under what circumstances.

It is a fundamental tenet of information privacy that data collected for one purpose should not be used for other purposes, nor disclosed to other parties.

Electoral Roll data, however, is authorised by the Parliament to be used, and to be disclosed, to large numbers of organisations, for purposes far beyond the administration of elections. The APF notes in particular the length of s.90B. Beyond this, the lists are expanded to a remarkable extent under delegated legislation, in Regulations 5A through 9 and Schedule 1. This results in a lengthy list of data disclosures, as recorded in Appendices to the AEC's Annual Reports, e.g. App. F in 2008-09, at http://www.aec.gov.au/About_AEC/Publications/Annual_Reports/2009/append_f.htm.
See also http://www.aec.gov.au/about_aec/roll.htm.

We again draw to attention the Victorian Electoral Commission (VEC)'s 2006 booklet comparing the collection use and disclosure practices of the VEC and the AEC, which clearly demonstrates how much wider the breaches are by the Commonwealth than by the Victorian Commission.
http://www.vec.vic.gov.au/files/ElectoralEnrolmentInformationCollectionandDisclosurePractices.pdf

Most members of the public are astonished when they discover the manner in which the Parliament has, in some cases intentionally and in others while sleep-walking, gifted the data that citizens supplied for the purposes of electoral administration, to other organisations entirely.

A search of the Regulations has not yet turned up the full list of data items that are released, and under what circumstances. It appears that it includes gender and some indicator of age. It may be a sub-set of the data provided on the enrolment form (which includes some particularly sensitive data, including contact-points and identity document numbers), but it may be a super-set, with additional data derived from other sources.

The protections afforded by provisions such as s.91A are incapable of shutting the door after the horse has bolted. The manner of administration of the electoral roll results in many uses that the public regards as being abuses, by corporations, by government agencies, and by political parties.

People's cooperation with government agencies depends on trust. And when they perceive that trust to be breached, they tend to be disturbed by the situation. A small proportion of people – but a substantial number – have good reason to be concerned. Others might be seen to be less rationally anxious about it. Some become unwilling and obstructionist. Most obstruct quietly, particularly if they have something that they want to hide, and especially if that something is themselves. Visible conscientious objectors are always just the tip of the iceberg of discontent.

The decline in the ratio of enrolments to the eligible population, noted in the AEC's Submission (at 2.2 on pp.4-5), is surprising only in its small size. It takes time for the public to realise that their Parliament has authorised massive incursions into their personal data, so the levels of distrust and obstruction do not rise immediately. The public's willingness to be on the Rolls will inevitably drop further.

The AEC has notably failed to draw this to the Committee's attention and to investigate how exercising proper controls over use and disclosure would improve enrolment. Yet worse, the AEC has signalled to the Committee its desire to move from an 'encouragement' stance (2.31 on p.13) to one of 'enforcement' (2.32-35 on p.14). Moreover, it even indicates an interest in overriding the reluctance of the courts to record a conviction or impose the maximum penalty (2.32).

The AEC's evidence in support of its desired switch to an enforcement stance is poorly researched. It establishes from a Victorian sample that compulsion works and the people submit (2.34), but it fails to consider the effect of moving from a small sample to broader implementation. This includes inevitable and substantial media coverage. It also includes the alienation of many people who are currently unwilling but compliant, and even of many people who have been willing, but who resent excessive granting of powers to government agencies and excessive use of such powers.

(4) Silent Electors

As previously mentioned, there are many categories of 'persons at risk', who have cause to be concerned about the exposure of personal data on the Electoral Rolls, especially in view of the widespread abuse of the data. The APF commonly uses a short, indicative list of such categories, comprising:

- people hiding, or on the run, from other people who threaten them with violence, or who they perceive to threaten them. These categories include:
  - people concealing themselves from previous criminal associates;
  - people concealing themselves from previous partners or friends;
  - victims of domestic violence;
  - protected witnesses; and
  - people under fatwa;
- celebrities, notorieties and VIPs, who are subject to the unwanted attention of excessively zealous fans and of kidnappers, extortionists and stalkers. These categories include:
  - politicians;
  - entertainers and sportspeople; and
  - people 'in the public eye', such as lottery-winners; and
- people in security-sensitive roles such as national security operatives, undercover police, prison warders, and staff in psychiatric institutions.

There are also many circumstances in which people imagine themselves or other householders to be among such categories, and hence anxieties may exist without clear evidence of a threat to safety.

The Electoral Roll's widespread availability and use creates at least one additional category – people in households that contain no enrolled (and hence adult) male.

Such people naturally seek to remove or obscure their personal data, and especially data that provides clues about their current whereabouts. A 'silent elector' arrangement exists, but it is far from clear that the whole of a person's entry is reliably suppressed from the vast numbers of copies of the Rolls, nor suppressed from disclosure for purposes other than electoral administration.

The form is a "request for address not to be shown on Roll" (s.104). (We note that, in a further breach of reasonable public expectations, neither the web-page nor the application form appear to provide any reference to the legal authority under which the process is conducted: http://www.aec.gov.au/Enrolling_to_vote/special_category/Silent_Electors.htm).

The "request for address not to be shown on Roll":

- demands the disclosure of the reasons why the suppression of "residential address" from "the publicly available rolls" is sought, which inevitably exposes sensitive personal data
- limits the acceptable reasons to solely "because it places the personal safety of [the elector] or members of [their immediate] family at risk"
- is not a right that individuals can exercise, but is "granted" by the Electoral Commissioner

It is inevitable that some individuals will be unable to gain the "grant", in some cases because the individual is unable, or unwilling, to disclose sufficient (inherently sensitive) information, or because the evidence is insufficient to convince the Commissioner to exercise the discretion.

Further, there are many other circumstances in which individuals are unable to apply, because the reasons are so limited. Anxiety arises from many sources, and many are not threats to personal safety that are express, or that the Commissioner can necessarily be convinced are real.

In short, the current arrangements leave many people at risk, and abuse many people's data in ways that are unacceptable to them. The AEC has breached, and breaches on an ongoing basis, the trust of these people. The APF has warned throughout the last quarter-century that such authoritarian attitudes breed a climate of distrust, and encourage the citizenry to lie to government agencies in order to provide themselves with protections that the government refuses to give them.

To achieve trust in the AEC, the logic of the scheme needs to be reversed, such that no detail is required from the applicant, and the onus is on the Electoral Commissioner to provide reasons why the address should not be suppressed, and access limited to electoral administration.

(5) 'Continuous Roll Update' (CRU)

In addition to being a source of data for vast numbers of other government agencies, the AEC is authorised to expropriate data from other agencies and to re-purpose it firstly for electoral administration, and secondly for a range of purposes, some of them internal, but others involving disclosure to yet more organisations.

A search has not yet run to ground the authorities for the Continuous Roll Update (CRU) program, and this section has relied on the brief (and probably greatly curtailed) description in the AEC's Submission (2.8-11 on pp.6-7).

AEC acquires "large and regular volumes" of personal data from at least one Commonwealth agency:

- Centrelink

and from at least one set of State and Territory government agencies:

- motor registries, via NEVDIS

and from at least one government business enterprise:

- Australia Post

It is unclear whether this list is complete, or the organisations listed above are examples.

It is unclear whether private sector sources are also used, such as Veda Advantage and Acxiom.

The data is matched, but it is not clear what data-items are used in the matching processes, nor what account is taken of differences in data definitions. For an introduction to computer or data matching, see:

Clarke R. (1994) 'Dataveillance by Governments: The Technique of Computer Matching' Information Technology & People 7,2 (December 1994) 46-85, at http://www.rogerclarke.com/DV/MatchIntro.html

This process is not the subject of consent, but is authorised by law. It represents expropriation and re-purposing of personal data, and results in further reduction in the respect in which the AEC is held, and in the willingness of the public to comply with electoral law, and to provide accurate and complete responses on forms filled in for government agencies.

3. The Present Bill

The new proposal embodied in this Bill takes the already problematic CRU process a very large step further, into territory where the Australian government has never previously ventured.

The results of data matching are to be used not merely as a basis for contacting electors with a view to achieving updates of the Roll, but to making changes unilaterally, by fiat. This inverts the process from its present consent-based approach (or in American parlance 'opt-in'), to imposed (or 'opt-out'). This can be seen as authoritarian, exerting power over the populace, or as paternalistic, transferring power over people's lives to an organisation asserted to be more capable of looking after them than they are themselves.

The primary justification advanced for this extraordinary change in the balance of power between the individual and the state is that "Providing the AEC with authority to directly update an elector's address will mirror other roll maintenance processes where the AEC can directly act in such a manner: for example, initiating objection action, and removing people from the roll on the basis of data from Births, Deaths and Marriages registries advising death" (1.4 on pp. 2-3). The examples are not in the least bit commensurate with the new proposal, because the objection process is quite limited, and in the case of death the elector is no longer able to perform the action themselves. The word "mirror" is entirely inappropriate.

Two further grounds are presented:

- it's just a further application of the existing objection process (2.13-2.17 on pp.8-9)

  This is spurious, because the receipt of a 'return to sender' or 'left address' message is positive evidence that the old address is no longer relevant; whereas an inference drawn from an error-prone matching process, coupled with the non-receipt of a response to a letter, represents negative evidence. It is far from sufficient to be treated as confirmation of the inference; and the two mechanisms are not in the least comparable.

  Further, the suggestion that "a proportion of these individuals ... were effectively disenfranchised by prescriptive legislative requirements that they did not clearly understand" (2.17) would apply to the new provisions, just as it does to the existing ones

- the community expects to interact like this (2.13, 2.18-22 on pp. 8-10)

  This is spurious for a different reason. Many people would welcome a consent-based cross-notification arrangement. These have been proposed or half-heartedly implemented in many contexts from the 'public kiosk' era prior to the advent of the Internet, right through the eCommerce and eGovernment phases. What the AEC is proposing is not consent-based. It is imposed, with an opt-out clause that is highly ineffective

  The attempt is made to claim that governments are much more trusted than business or charities, because only 12-16% of people said that they avoid government agencies that cross-reference or share information (2.20). We note that the AEC repeated this in its verbal evidence.

  The claim is completely undermined by the fact that government agencies are legislated monopolies, and in most cases are unavoidable

There are other instances of illogic in the AEC's Submission:

- they impliedly claim that a 0.1% of objections to the NSWEC supports the proposition that the public don't care (2.24 on p.11). Firstly few people ever object, variously because of apathy, lack of skills, lack of confidence, and the designed-in inadequacy of government complaint mechanisms. Secondly, customer relations practice when gauging dissatisfaction levels is to multiply the (hundreds of?) complaints by some factor. Thirdly, there is very little appreciation by the public of the extent of the haemorrhage of data from the electoral rolls, so the level of complaints is less than it would be if the public was well-informed
- they claim that the approach is accepted in Canada, but then admit that the system there is consent-based, not imposed (2.25-26 on pp.11-12)
- they refer positively to use of data for a range of purposes in countries that have a "civil or national register" (2.27 on p.12). The Australian public has emphatically rejected the desires of the Commonwealth Public Service for a national id scheme, on multiple occasions

The justification provided throughout by the AEC is generic, of the kind that indicates that 'it seems like a good idea'.

There is no analysis of sources, no provision of information about experiences to date with matching and with inferencing from the results of matches. Every match with every source of data has its own vagaries, because the purpose of the data guides the design of systems, the definition of data-items, the degree of care taken with quality assurance, and the timeliness of the data. Not one skerrick of evidence is provided that this has even been done, let alone presented to the Committee and the public for review.

The data matching will result, as data matching inherently does, in large numbers of false positives. A few special cases are allowed for – notably Members of Parliament. Of the general public, on the other hand, only the small numbers of people who are able to gain a "grant" from the Electoral Commissioner are to be free of the rigours of the process.

Data matching relies heavily on names, addresses and date of birth. By definition, address is not a suitable basis for matching in this case, because address-differences are being sought. Names are highly variable, contain many ambiguities, and are the subject of 'data scrubbing' (i.e. organisationally-imposed changes). This may assist operations within a single organisation, but adds to the sources of false positives when the data is expropriated for data matching purposes. Date of birth is in many data collections a miscellaneous data-item, not subject to quality assurance, and subject to misrepresentations motivated not only by dishonesty but also by reticence and embarrassment.

Contrary to the AEC's claim (3.8 on p.16), data matching by Commonwealth agencies is not subject to effective controls. The Parliament has failed to pass into law a regulatory framework for data matching. Apart from the narrow scope of the Data-Matching Program (Assistance and Tax) Act, the Privacy Commissioners Guidelines are just that – Guidelines, unenforceable and unenforced. The Guidelines date to the very beginning of the 1990s, and have never been re-constructed to reflect subsequent learning, particularly the considerable accumulated knowledge about Privacy Impact Assessments (PIAs). The Guidelines consequently fail to reflect the key principles of justification, transparency, proportionality, careful design, and amelioration of negative privacy impacts.

Moreover, no control mechanisms have been imposed by the Parliament on the AEC's substantial use of data matching. And nothing exists in this Bill that makes good that massive shortfall, despite the very substantial increase in its intrusiveness as a result of the current proposal.

The AEC implies that the two letters sent to the presumed new address of the elector represent a quality control measure (e.g. 3.6 on p.16). There is a vast array of reasons why a letter from a government agency to a citizen at an address expropriated from a record in another government agency may elicit no response. Many of those reasons would be associated with an erroneous inference by the AEC. And few of the problems will be discovered just because a second letter is sent.

In summary, a great many errors would arise, to the serious detriment of the quality of the Rolls, and to the consternation of some electors.

A further concern expressed in the APF's initial Submission is that "how the Commissioner is to be satisfied, what other sources he is entitled to use, and how to test their reliability ... are too important to leave to Regulations, the Minister's discretion, or the Electoral Commissioner's discretion, or to the general requirement on AEC to comply with the data quality principles IPPs 8&9. An increased power to change without consent deserves an increased onus to ensure reliability, with criteria specified in the legislation".

Further, if the Parliament were to accept the AEC's blandishments and proceed on this course of action, we previously submitted that "any enrolment details changed without consent should be quarantined from the secondary uses which are permitted under the Act ...". We now add that we believe that they should be awarded automatic silent-elector status, in order to cater for the proportion of people who actively did not want that address to become public, and those who provided their data to another agency in confidence, but have had that confidence breached through data matching.

The authority sought by the AEC is spectacularly broad. It is an ambit claim of the highest order.

The agency wants the delegation to do whatever it sees as appropriate, without specific justification and without any need for troublesome approvals, not even the limited oversight that can sometimes be achieved through disallowable instruments.

In these circumstances, for the Committee to recommend passage, and for the Parliament to pass the Bill, would be to authorise serious and unwarranted breaches of privacy and to greatly reduce both the public standing of the AEC and the quality of the Electoral Rolls.

4. Procedural Matters

The enormous deficiencies in the proposal are compounded by (although also in part explained by) the following procedural deficiencies:

1. it is not clear that any Risk Assessment has been performed, as is normal business practice, and is expected by DoF and ANAO. None is apparent even from the perspective of the AEC and the integrity of the Rolls, let alone from the perspective of the people whose data is being expropriated, and control of whose Electoral Roll entries is being seized by the AEC
2. it appears that no Privacy Impact Assessment (PIA) has been performed, as is normal business practice, and as is an expectation of both the Privacy Commissioner and the Government as a whole. We note that the AEC said in evidence that "We have been in consultation with the Privacy Commissioner over this particular bill". The Committee may wish to ask the Privacy Commissioner why he did not raise with the AEC the issues identified in the APF's Submissions, and why he failed to prevail upon the AEC to perform a PIA on a proposal which clearly raises significant privacy issues
3. no consultation appear to have been conducted with NGOs representing the public interest, such as APF and the Councils for Civil Liberties. The AEC appears to assume that, rather than informed discussions in advance, the appropriate form of consultation is duelling Submissions and Evidence before a Joint Committee of the Parliament
4. no consolidated legislation has been provided. Instead of longstanding technologies being applied, in order to provide both Committee-members and the interested public with the ability to understand the new provisions in their context, the AEC appears to prefer everyone to do the hard work of consolidating the legislation themselves

5. Conclusions

The Committee should recommend the government withdraw the Bill and/or that both Houses reject it.

The Committee should require the AEC to make good the procedural deficiencies noted in s.4 above.

The Committee should require the AEC to prepare a comprehensive body of information, make it available during consultations relating to both its Risk Analysis and PIA, and make it available as part of the package brought before the Parliament with any amended Bill.

The APF believes, however, that once the Transparency Principle is respected and it is clear to more people what the threats are to people's capacity to determine their own futures, and what the threats are to trust in the administration of electoral matters, it will be apparent that no Bill should ever be re-submitted containing any such provisions.

The Committee should require the AEC, as part of its deliberations, to consider consent-based arrangements that take advantage of Internet-era capabilities.

The Committee should invert the s.104 arrangements in relation to silent elector, as described above.

Further, the Committee should recognise the inadequacies of the data matching that is already authorised and performed under the CRU, and recommend the enactment by the Parliament of up-to-date regulatory measures over the process.

The Act refers to:
Commonwealth Electoral Act 1918
http://www.austlii.edu.au/au/legis/cth/consol_act/cea1918233/

The Regulations refers to:
Electoral And Referendum Regulations 1940
http://www.austlii.edu.au/au/legis/cth/consol_reg/earr1940327/

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, SubCommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by a Patron (until recently, Sir Zelman Cowen), and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90) http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-) http://www.privacy.org.au/Campaigns/Media/