Australian Privacy Foundation

post: GPO Box 1196
Sydney NSW 2001
phone: +61 2 9231 4949
facsimile: +61 2 9262 3553
email: mail@privacy.org.au
web: www.privacy.org.au

Senate Legal and Constitutional Committee

Inquiry into Privacy Act 1988

Submission

The Australian Privacy Foundation

March 2005

Senate Legal and Constitutional Committee
Inquiry into Privacy Act 1988
Submission by the Australian Privacy Foundation

The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which 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 Foundation uses the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed. For information about the Foundation and the Charter, see www.privacy.org.au

Contents

Overview

We welcome this Inquiry, particularly since its terms of reference[1] are much broader than the limited review of the private sector provisions currently being undertaken by the Privacy Commissioner at the government's request. While that review will hopefully lead to recommendations for improvements in the private sector regime, it cannot be expected to address many other crucial questions about the adequacy of current privacy protection, including in relation to government intrusion. Similarly, the government's claims[2] that issues such as the protection of employee records and children's privacy are already being addressed should not be accepted by the Committee as a reason for not looking at those issues as part of its broader Inquiry

We note that this submission repeats points made in our submission to the Privacy Commissioner's review and to other relevant reviews and inquiries. We make no apoology for this as the terms of reference overlap with the Committee's. We request the Committee to consider all of our concerns and suggestions whether or not the Commissioner, or other reviews, are currently addressing them as well.

Effectiveness and appropriateness of the Privacy Act 1988

General

The need for strong and effective privacy legislation is greater than ever, and the survey research commissioned by the Privacy Commissioner in 2004 shows that the public understand and want this protection, but are not confident they are getting it. Unfortunately the current Privacy Act is neither strong nor effective.

The threats to personal privacy and autonomy, from business and government, are constantly increasing. There is a seemingly insatiable appetite for more and more information collection – involving routine surveillance and monitoring without consent – despite strong evidence that large organisations are unable to responsibly handle the information they already hold[3], and that attempts to compare data collected for different purposes are fraught with difficulties and often create more problems than they solve.

At the same time, fears of crime and terrorism are being cynically exploited by both bureaucratic and commercial interests to falsely suggest that privacy protection stands in the way of security and good government. We draw the Committee's attention to the report in the Sydney Morning Herald of 22 February under the title "Ruddock wants 'fix' for privacy laws" for examples of the half truths and propaganda that are being used to undermine the already weak privacy protection regime.

It is simply not the case, for example, that Centrelink, or any other agency, is seriously inhibited by privacy laws from detecting fraud or delivering benefits. The legislative regime already provides over-generous exemptions that allow agencies to exchange data without consent. It is also untrue that

[1] Attached at Annex A
[2] The review of the employee record exemption and of childrens' privacy are being carried out by inter-departmental committees which cannot be considered independent of government interests, and in any case little progress has been made, or at least made public, on either of these reviews.
[3] We would be pleased to provide on request numerous examples, drawn both from experiences of breaches of Australia's privacy laws, and from overseas.

private sector service providers contracted to provide government services cannot check details of claimants with government agencies. Their contracts can and do require them to do this and the Privacy Act accommodates this. Similarly, claims that privacy laws inhibit health research are false, put about by a well-organised and powerful lobby that simply finds it inconvenient to use the existing processes for approving research uses of personal information.

Consent based regime

At the outset, we feel the need to emphasise that the foundation of any privacy protection regime should be the maximum possible control by individuals over the use of information about them. Discussions about privacy principles too often stray from this underlying objective. We note in this respect that whenever privacy issues become highly visible, they often quickly distil into a clear balance between an individual's right to control/consent and another public interest. This quite rightly raises the bar on the case for the other public interest, and often leads to better privacy outcomes than would be achieved from a more technical discussion. A good example is the Spam Act 2003, where arguments about commercial free speech were never going to win against the shared sense of frustration of all computer users – leading to a consent based or 'opt-in' regime for Spam. This can be contrasted with the difficulty we and other consumer groups have had in arguing for opt-in in the context of other direct marketing, health research, etc. It is always a useful rule of thumb to bring privacy debates back to the central question – "why can't this be done with consent?".

Consistency between Commonwealth and State privacy laws

There is a major and growing problem of inconsistency between federal and State and Territory privacy laws. This stems largely from the failure of the Commonwealth to ensure that the federal law provided adequate protection across the board. Had it done so, a major objective of the 2000 amendments – to provide a consistent national framework, might have been realized. But it is hardly surprising that, faced with major gaps and weaknesses, the States and Territories have felt it necessary to provide their citizens with additional protection both in general privacy laws and in specific areas of health privacy and surveillance.

Where private sector contractors normally subject to the NPPs are engaged by State or Territory government agencies subject to other principles, there is much confusion and at least the potential for contractors to entirely escape the application of any principles. The NSW Privacy Commissioner drew attention to examples of inconsistent definitions leading to gaps in coverage in his submission to the 2004 NSW Attorney-General's Department review of PPIPA[4].

The only complete solution to these problems is the harmonisation of the different statutory regimes, which we favour provided it levels up to a highest common standard. In the meantime, revision of the provisions dealing with contractors is required, together with clearer guidance. Strengthening of the *Privacy Act 1988* would also reduce the need for Sates and Territories to develop their own schemes.

[4] http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_publications#13 – pages 127-128

Rationalisation of Information Privacy Principles

The distinction between the public and private sectors is increasingly artificial and there is no good reason to maintain two separate sets of principles. Government services are increasingly being delivered by the private sector, whether under contract or by other arrangements. It is confusing to individuals and organisations to have different principles trying to achieve the same underlying objectives. The IPPs and NPPs should be merged and the new principles should apply to everyone handling personal information - government agencies, commercial organisations , associations, charities, elected representatives and political organisations. We would expect the merged principles to be more like the NPPs (e.g. a single use and disclosure principle, (stronger) anonymity and identifier principles) such that the cost to business of transition would be minimal. There may be some training and education costs to Commonwealth agencies of a merger of principles, but there should be relatively little substantive effect on government systems.

We put forward the Australian Privacy Charter as a possible model for a new set of principles. This charter[5] – attached as Annex B - was developed by a coalition of interested parties under the chairmanship of Justice Michael Kirby between 1992 and 1994 and represents an updating and strengthening of the current international instruments used as benchmarks, such as the OECD Principles of 1980. Some information privacy elements of the Charter have already been incorporated into Australian privacy laws – such as the right to anonymity – now NPP8(Cth) and IPP8 (Vic). Leading privacy experts in the Asia Pacific Region are currently working on a new version – the Asia-Pacific Privacy Charter[6], partly in response to the APEC Privacy Framework initiative discussed below.

The responsibilities of contractors relative to principals, and the contracted service provider provision in s.6, are far from clear. There is a major problem of overlapping jurisdictions where private sector contractors normally subject to the NPPs are engaged by government agencies subject to other principles – either the IPPs for Commonwealth agencies or the principles applying to state or territory agencies. Rationalising the NPPs and IPPs would at least eliminate this problem for many private sector contractors.

Privacy broader than just personal information

The Australian and draft Asia Pacific Privacy Charters emphasise the reality that privacy has many dimensions – e.g. privacy of the person and communications privacy as well as information privacy which is largely what the Privacy Act deals with. We urge the Committee to consider what additional protection needs to be put in place to deal with contemporary threats, going beyond information privacy principles to limit the development of a surveillance society and protect individuals from assaults on their physical integrity such as mandatory drug and DNA testing and increasingly prevalent and intrusive searches, and from other intrusions (such as by telemarketing or media harassment). These forms of privacy invasion may not involve the creation of a record of personal information, and yet are just as important in terms of a more general "right to be let alone".

[5] See http://www.privacy.org.au/About/PrivacyCharter.html
[6] See http://www.bakercyberlawcentre.org/appcc/

Application of the Act to personal information, records and generally available publications

Definition of personal information

The definition of 'personal information' is too limited, and can give an arbitrary result when applied in the context of different technologies. It is not clear if it would cover, for example, video images that have not been 'indexed' by reference to individuals, or email or IP addresses that do not themselves contain any indication of an individual's identity.

The first weakness could be addressed by changing the definition to the formulation used in the European Union Data Protection Directive, i.e. 'information relating to an identified or identifiable natural person … an identifiable person is one who can be identified, directly or indirectly …' (emphasis added).

To address the second weakness, we support an 'ability to contact' test as suggested in the Issues paper – perhaps by adding wording along the lines of '… or information sufficient to allow communication with a person', i.e. whether or not it is sufficient to allow the person to be identified.

Other considerations include whether 'intention to identify' is significant, and whether inability to identify in the hands of a particular user takes information outside the protection of the Act, even though a third party may be able to identify individuals. This is obviously undesirable, and any change to the definition should ensure that personal information that is potentially identifiable by anyone else remains covered by the Act wherever it is held.

An exception would then probably be justified for information where reasonable steps have been taken to de-identify it. This is particularly relevant in the research context, where justifiable exemptions from the requirements of the Act should not be undermined by the remote possibility that someone might be able to 'guess' the identity of a particular individual from information that has been adequately 'de-personalised' to recognised research industry standards.

Records

Unlike the NZ and NSW Acts, personal information is currently only regulated under the Privacy Act 1988 if it is in 'a record'[7] (the collection principles apply also to collection for a generally available publication). This has the effect that information passed orally between individuals, even if obtained and/or used in a work context, is excluded, as is 'real time surveillance', e.g. by security guards. While it would not be appropriate to try to regulate informal personal communications, consideration should be given to closing the gap that would allow agencies and organisations to breach the spirit of the Act by avoiding making a record. Clearly some of the principles would not be applicable to information unless it is in a record, but others can and should be applied. The relationship of the Privacy Act to surveillance laws is relevant here.

Generally available publication

The APF fundamentally disagrees with the exemption of personal data from the provisions of the Act merely because it is 'generally available'. All such collections were created for one or more purposes, and the handling of the data should be subject to protections that reflects that purpose or purposes.

[7] included in the IPPs for the public sector and effected by s.16B for the private sector

We accordingly urge reconsideration of the breadth of exemption for information in 'generally available publications' from all of the NPPs except the collection principles[8]. Firstly there seems no good reason why some of the other principles – such as the data quality and correction principles, should not apply even if the information is published. Secondly, it invites attempts to avoid the application of the principles by publishing information – which could often compound a privacy breach. Thirdly, it is possible that the exemption could be used to argue that information held by an agency or organisation is not subject to the principles merely because the same information has been published by an unrelated third party. This would clearly be contrary to the spirit of the principles and the exemption, but is a danger which should be eliminated.

See also our submission to OFPC's consultation on Publicly Available Information in 2002[9].

Sensitive information

The private sector amendments introduced a defined category of 'sensitive information' which is subject to an additional collection principle (NPP 10). No such distinction is made in the public sector regime.

This category aligns with the types of information that have been recognised as 'sensitive' internationally. Such information has been used, and is still used, to discriminate against and persecute groups of individuals and minority communities. We fully support the policy behind the identification of this information as requiring particular protection against misuse. However, in Australia our anti-discrimination and racial vilification legislation address this issue more effectively and comprehensively than our privacy legislation does.

From a privacy perspective, sensitivity is contextual – the address of someone on a witness protection program is clearly highly sensitive (yet not covered) while a gym club membership, or religious affiliation of the well known local priest are covered and yet arguably trivial. Financial information, which most surveys show to be typically considered highly sensitive by individuals, is not included in the definition.

In our view the issue of sensitivity from a privacy perspective can best be dealt with by judgements on 'reasonable steps' in relation to the application of other principles. This approach would supplement and support anti-discrimination legislation while making the privacy legislation more workable.

Relationship to other laws

We touch in this submission on the relationship of the Privacy Act to other laws, in a number of specific contexts. There are two particular problem areas, health and telecommunications, which deserve separate mention.

Health

The application of privacy principles to health information and the use of other information for health related purposes can be difficult, with a mass of existing regulation, custom and practice, professional standards, and very strongly held views. These have now resulted in a proliferation of health specific privacy rules and laws. The confused situation that many health service providers currently find themselves in – being covered by at least two separate health privacy laws - federal and State or Territory – represents a failure of good government and is definitely not in the interests of consumers.

[8] definition of record in s.6 for the public sector and s.16B for the private sector
[9] See http://www.privacy.org.au/Papers/SubmnOFPCQ&A0212.html

We perceive too many of the inconsistencies in this area being the result of vested interests and bureaucratic rivalries rather than due to any real concern for the privacy interests of individuals.

We therefore support the development of a National Health Privacy Code, provided it achieves a highest common standard of privacy protection. But this initiative, which already appears to have stalled, will be wasted without a strong commitment by all interested parties to adopt the National Code as the basis for their own laws or rules, without further 'tinkering'.

Telecommunications

Telecommunications legislation (particularly the Telecommunications Act 1997 and the Telecommunications (Interception) Act 1989) provide important privacy protections (although the Interception regime has been seriously weakened in recent years). However the operational relationship between the Telecommunications Act (TA) and the Privacy Act (PA) remains confused and uncertain. A range of relevant Australian Communications Industry Forum (ACIF) Codes and the roles of the Australian Communications Authority (ACA) and Telecommunications Industry Ombudsman (TIO) overlapping with the Privacy Commissioner are additional complications. These overlaps have already complicated the resolution of a number of key privacy issues including the use of directory information, and a representative complaint about disclosure of Calling Line Identification (CLI) information by Carriers to Internet Service Providers.

The TA is unusual in that it both sets higher use and disclosure standards (i.e. more limited) than the PA, but also requires co-operation with and specific disclosures to law enforcement and intelligence agencies.

Privacy of communications is one of the most precious of all privacy rights, in that it underpins unconstrained discourse in a free society. Without a reasonable presumption of confidentiality in communications, there is a major risk of a chilling effect on freedom of expression – including political expression - which is an essential quality of our democracy.

We feel strongly that current telecommunications law has developed in an unplanned and inconsistent way so as to both support and undermine communications privacy at the same time. It is also inconsistent in some respects with the law as it applies to postal communications, and to informal face to face communications (governed by surveillance laws). As telecommunications accounts for a rapidly increasing share of all communications, we suggest that a review of the relationship between privacy and communications law is overdue. We suggest that the Committee could recommend this as a separate exercise.

International comparisons

In our view the Privacy Act does not meet current international 'best practice' standards and obligations. Australian business therefore continues to be disadvantaged in international trade involving personal information, currently by the uncertainty and cost involved in assessing the requirements and the position in other countries.

The government failed to meet its objective, with the private sector amendments, of satisfying the European Union about the adequacy of our law, and the further amendments in 2004 only partially dealt with the EU's outstanding concerns. We understand the EU Commission is currently reviewing the adequacy of our law again, and fully expect that they will again find that it has significant weaknesses.

The Australian government has played a leading role in the development of the APEC (Asia Pacific Economic Co-operation) Privacy Framework adopted in November 2004. While this Framework could provide a useful stimulus to privacy protection in other countries in our region, it could also potentially be used as an excuse to undermine existing levels of protection in countries such as Australia. Much depends on what is included in the 'missing' section of the Framework on 'cross border elements'. A detailed assessment of the APEC Privacy Framework by one of our Board members, which is endorsed by the Board, is attached as Annex C.

New technology and challenges to privacy

The Committee's terms of reference include as issues for consideration 'Smart Card' technology and the potential for this to be used to establish a national identification regime; biometric imaging data, genetic testing and the potential disclosure and discriminatory use of such information, and microchips which can be implanted in human beings. While all these technologies raise important issues, it is essential that any legislative privacy protection regime is as 'technology neutral' as possible, as we simply cannot predict the next innovations or their implications.

Privacy protection needs to be founded on the underlying principles of justification, proportionality, and limitation of collection and use which have underpinned all international privacy instruments, together with newly developed principles, already partially incorporated into the Privacy Act 1988, such as a right to anonymity and pseudonymity, and express control of unique identifiers.

We welcome calls for a debate about identity management in modern society, and acknowledge many of the public policy issues that proponents of personal identification schemes seek to address, such as identity crime, and verification of entitlements. But we are concerned that too many initiatives in the area of identity management, some involving the use of biometrics and smart cards, are being developed behind closed doors, by vested interests, and without due regard for wider social implications, including for privacy. The previous Privacy Commissioner made identity management a priority but the lack of resources means that even the OFPC cannot be adequately involved in all the current initiatives – another argument for opening them up for wider public input.

There is far too much loose thinking around the subject of identity management. The extent of the alleged problems of identity crime are poorly quantified and often exaggerated.[10] It is also far from clear how some of the proposed identification and identity checking schemes would actually contribute to solutions. In contrast the very real risk is that the inevitable breaches of supposedly higher integrity systems could have even more dire consequences – for organisations and individuals – and this is rarely acknowledged or discussed.

There is a very strong argument to be made that the separation of data in functional silos (health, taxation, transport etc) – far from being a problem – is actually one of our strongest protections against security breaches having traumatic consequences. Proponents of identity schemes, monitoring and data matching seem to proceed on the naïve assumption that their scheme can somehow be made 100% accurate and secure, despite the evidence of history, and the reality of all human systems, that errors and security breaches will inevitably occur. We submit that much of the emerging work on critical infrastructure protection (against terrorist and other threats) would support our arguments against putting all our identity management eggs in too few baskets.

[10] The AUSTRAC Report 'Identity Fraud in Australia' produced a much lower estimate of cost than had previously been in circulation, and yet still inappropriately included costs of security measures which would be in place whatever the level of identity crime.

Major projects: PIAs, Digests and Matching protocols

The Act does not currently provide an adequate mechanism for identifying and addressing the implications of major privacy intrusive initiatives or proposals. We comment in detail below on the weakness of specific NPPs in this respect, but however strong the principles, they would still not adequately provide for public debate about the desirability of, and privacy risks involved in, major projects. We have in mind particularly those projects involving new requirements for evidence of identity; biometrics; tracking technologies and/or bulk data linkage or matching.

The best way of getting all of these issues into the open, and ensuring that public policy decisions in this area are better informed, is to carry out and publish comprehensive privacy impact assessments (PIAs) for all major projects with significant privacy implications, whether in the public or private sectors. The technique of PIA has been developed internationally over the last decade (drawing on but also learning from the experience of environmental impact assessment) and is now a mandatory requirement in several jurisidictions including the USA and Canada. Criteria should be developed, drawing on international experience, for triggering such a requirement under the Privacy Act. PIAs should be conducted by independent assessors but paid for by scheme proponents, with the Privacy Commissioner setting and monitoring appropriate standards.

Agencies or organisations, when conducting PIAs, should be under an obligation to conduct meaningful consultations with representatives of, and advocates for, the public interest. This requires disclosure of sufficient information, provision of adequate notice, provision of a reasonable opportunity to interact with the people performing the PIA and to communicate information and argument, and publication of an outline of the consultation process and outcomes.

PIAs, where required, should also be submitted to the Privacy Commissioner for consideration. The Commissioner's views, while not binding, should be published along with the PIA itself as part of the public consultation and before any final decision is made to proceed with the initiative in question.

We acknowledge that a requirement for PIAs would interrupt the normal decision making process for many organisations, where initiatives would not normally be exposed to public scrutiny until they were well advanced. But this should not be seen as an obstacle to such a requirement. Rather, PIAs should be seen as an instrument of greater accountability for at least one aspect of a 'triple bottom line' concept of corporate and public sector governance.

PIAs are not of themselves an adequate safeguard if considered only prior to implementation. One use of PIA findings would be to provide a benchmark for testing actual privacy impacts after implementation of the project, service, or system. It should then be incumbent upon the implementing organisation to test the anticipated impact against the *actual* resulting impact after a period of time, say one or two years later. Otherwise the PIA will have had only limited utility and could even be actively misleading if changes are made in implementation that were not anticipated in the initial design. This is a relatively new concept and should be further explored in conjunction with the Privacy Commissioner in the role of auditor.

Requirement to follow data-matching guidelines

Data-matching is generally considered to carry with it particular privacy risks, and is already specifically regulated for specific Commonwealth agency matching under the Data-matching program (Assistance and Tax) Act 1990, as well as in New Zealand and Hong Kong). Other agencies have signed up to voluntary data-matching guidelines issued by the Privacy Commissioner. While the focus in Australia and NZ to date has been on government matching programs, the NZ and HK laws both allow for regulation of private sector matching. For reasons already mentioned, we think that it

makes no sense to limit such regulation to the public sector and recommend a specific requirement under the Act to comply with data-matching guidelines, to be generalized from the Privacy Commissioner's existing advice to Commonwealth Agencies. Such guidelines would include a requirement to publish details of a matching program and to provide for a period for public comment.

It might be appropriate to include the notification and consultation requirements of data matching guidelines in a more general requirement for PIAs (see above) but this would still leave a role for specific data-matching guidelines to address the particular risks associated with matching.

Specific technologies

In relation to Smart Cards and Biometrics, we offer these as examples of issues potentially to be addressed by expanded Code of Practice provisions discussed below. Our submission to the Biometrics Insititute on its draft Code of Practice under the Privacy Act is attached as Annex D. The Foundation has also made detailed submissions on specific smart card (and RFID) and biometric applications, which we would be pleased to provide to the Committee if requested.

In relation to genetic privacy, we applaud the comprehensive work of the ALRC in its 2004 Report *Essentially Yours* and broadly support its recommendations. Our submission to the ALRC is attached as Annex E.

Private Sector regime

The weaknesses of the private sector regime were the subject of our comprehensive submission to the Privacy Commissioner's current review and we repeat below the main points.

Balance of interests

The private sector provisions do not in our view strike an appropriate balance with competing interests in that the provisions themselves (and the exemptions) excessively favour public interests (primarily those supporting commercial interests) that intrude on privacy. A free flow of information is only a desirable objective to the extent that it respects individuals' privacy and autonomy, and other public interests should only outweigh privacy where a compelling case can be made out in specific circumstances. The business community overall is not currently sufficiently aware of its obligations, but there is no reason why businesses should not be able to operate efficiently while complying with the current, and desirably with stronger, privacy obligations. Efficiency must always be defined as the most effective use of resources *given* social, ethical and legal constraints, and in this respect compliance with privacy standards is analogous to health and safety, anti-discrimination and key environmental requirements – they all clearly impose costs and constraints, but should be non-negotiable.

Scope of the Act and Exemptions

Employee Records exemption

The employee record exemption should be removed. The handling of personal information in the employment context is one of the areas in which protection is most needed, and the vacuum created by this exemption is already being partially filled by State government initiatives on workplace

privacy, further complicating the regulatory environment, which is in no-one's interests. The government's 'excuse' that the employee record exemption is already under separate review might carry more weight if that other review were not being conducted effectively in secret, with no submissions having been published and no progress reported for almost twelve months.

Political acts and practices exemption

The exemption for political acts and practices is unconscionable and hypocritical. The government cannot morally and ethically justify exempting politicians and political parties from the privacy protection rules which have been applied to the rest of the community. We urge members of the Committee to set aside any self interest in leaving themselves outside the Privacy Act regime, and to take the only principled approach of recommending the removal of this exemption. There may be a need for modified rules to recognise the public interest in the democratic process, but the starting point should be a level playing field with equivalent standards.

Personal use exemption

The exemption for private/personal use (s.16E) needs to be revisited in light of growing incidence of abuses including inappropriate use of mobile phone cameras and misguided and extremely prejudicial 'vigilante' websites. Disclosure to a single person may be private/personal but publication via the web or other media is not. Adjustment of this exemption may not be sufficient on its own to address abuse of mobile phone cameras, which may also require separate remedies for unacceptable intrusion.

Media exemption

The journalism exemption in s.7B(4), and the associated definition of 'media organisation' are far too wide and effectively allow any organisation to claim exemption from the Act for information which is 'published'. This weakness is compounded by the failure to define 'journalism'. The only constraint on organisations claiming this exemption is the condition of committing to published media standards, but as there are no criteria for these standards, or provision for review of them, the condition is effectively worthless.

The Foundation recognises, as do the public, that media organisations can and do, all too frequently, seriously intrude into individuals' privacy without adequate justification. The low level of enquiries and complaints in this area cannot be taken as implying satisfaction – it is probably explained by a widespread and correct view that media are effectively above the law in relation to privacy – unless individuals have the resources to pursue defamation or other common law actions (and even then with very limited chances of success).

Current industry self regulation – including the Press Council and broadcast media codes of practice, only pay lip service to privacy and are widely regarded as ineffectual. However, the Foundation has always accepted that application of privacy principles to the media raises some special issues and that there needs to be a balance to reflect the public interest role of some media organizations.

The solution is not the current 'blanket' exemption. In the medium term we favour a separate independent review and inquiry into the media and privacy. In the short term the journalism exemption should be amended to focus more narrowly on the bona fide public interest media role of news and current affairs.

The media exemption should also only apply on condition that (a) the privacy standard is a bona fide attempt to protect privacy from media intrusions (assessed as such by an independent arbiter – perhaps the Privacy Commissioner); (b) is enforced in some effective way; and (c) is generally observed by the media organisation concerned.

Small business exemption

The small business exemption is in our view too broad, but also too complex, such that many small businesses, and individuals dealing with them, are uncertain as to whether or not the businesses are subject to the law.

The concept of an exemption based on business size (whether measured by turnover or employee numbers) is essentially flawed. Some of the most privacy intrusive activities are carried out by very small companies and even sole traders – examples include private detectives, debt collectors, internet service providers and dating agencies. Also, there is no easy way for consumers to know the turnover of a business and therefore whether or not it is likely to be subject to the law.

The condition on the small business exemption that it is lost by organizations that 'trade' in personal information, is, we suggest, not effective in practice. The meaning of the condition[11] is very uncertain[12] and is almost certainly being ignored by most organizations who will have made a simple judgement about the Act's relevance based primarily on the clear turnover threshold.

We recognise that the vast majority of small businesses either handle no personal information at all, or do so without any significant risk or threat to the privacy of the individuals concerned. However, privacy risks are always contextual – any organisation which holds information as basic as name and address could potentially use or disclose it in circumstances which could cause damage to the individual concerned.

The core requirements of the NPPs – being open about use of personal information, handling it in accordance with reasonable expectations, and keeping it secure, should apply to all organisations. It would however be reasonable to exempt many smaller businesses from any formal requirements to take particular actions, in advance of enquiries.

Where an organisation only collects and handles personal information for a purpose which is or should be obvious to the individuals concerned (a more constrained version of NPP2), it should not have to give any specific notices under NPP 1.3 or 1.5 But all organisations should be required to answer enquiries (NPP 5), and to give access and make corrections on request (NPP 6), subject to suitable exemptions from these principles. They should also all be held accountable after the event for justifying their collection and use (NPP 1.1 & 1.2) and for any data quality or security breaches (NPPs 3 & 4).

An alternative way of formulating the threshold for relief from some obligations would be if the organisation is using the information only for the purpose of completing a transaction that has been initiated by the consumer. In contrast, if the organisation intends to use the information from a transaction to build an ongoing relationship with the customer, or if the organisation collects personal information from other sources to initiate a relationship with an individual, the full requirements would be imposed.

If there is to be a residual size threshold, we submit that $3 million pa turnover is far too high – businesses with this turnover are hardly 'small' in most peoples' eyes. We strongly suggest that any residual exemption threshold be more consistent with that used in analogous jurisdictions – for example the NSW Anti-Discrimination Act 1977 uses a threshold of 5 employees. While no more

[11] Privacy Act 1988 s.6D(4)(c) and (d), together with s.6D(7) & (8).

[12] On one view, any merchant who accepts credit card payments is 'disclosing personal information (to the credit card company) for a benefit service or advantage', and consent for the disclosure is not typically obtained from customers. This would completely undermine the value of the exemption. But if not this meaning, then what? The Commissioner's Information Sheet No 12 does not give any useful guidance on this point.

related to privacy risk than turnover, a number of employees threshold would at least be familiar to many businesses and somewhat more transparent to consumers.

Application to deceased

We note that the NSW legislation (PPIPA and HRIPA) expressly extend protection to information about deceased individuals until 30 years after their death, with a 'person aggrieved' having the right to bring complaints. Given the potential for distress to relatives from disclosures about individuals, we suggest that consideration be given to similar coverage of the Privacy Act 1988.

Related Bodies Corporate

We believe the provisions in s.13B, apart from being overly complex and difficult to understand, are too generous in allowing exchanges of information between related companies which effectively avoid some of the NPP obligations. Individuals typically have no knowledge of corporate structures and relationships. If businesses choose for their own reasons to structure their affairs through separate incorporations, we do not see why this should give them any exemption from the normal application of the NPPs. Related bodies corporate should be treated as any other third parties – s.13B should therefore be repealed.

Issues concerning the NPPs

We submit that the following changes should be made to the NPPs and should also be carried over into any rationalisation of the IPPs and NPPs.

Collection – NPP1

NPP 1 should expressly include a prohibition on collecting information known to be unlawfully disclosed. This would avoid the situation that has been encountered in a two recent representative complaints where it is suggested by OFPC that an organisation A does not breach NPP 1.1 or 1.2 if it collects information from organisation B, even where it knows that B is not lawfully entitled to disclose it13. This cannot be an outcome consistent with the scheme of the NPPs.

Similarly, it should be an express requirement that the purpose of collection is lawful – NPP 1 currently only requires that the *means* of collection be lawful (1.2). This change would bring the principle into line with the equivalent principles in the IPPs (IPP 1(1)(a))[14] This concept is also standard in copyright law where a test of 'lawfully obtained copy' is included for allowing fair dealing exemptions.

We would like to see clarification that NPP 1.1 'necessary for one or more of its functions or activities' in NPP 1.1 requires an *objective* test of functions or activities, i.e. the organisation collecting cannot be the sole judge of whether information is necessary. If this is not the interpretation, the principle should be amended to make it clear that compliance can legitimately be challenged by third parties, particularly by the subject of the information being collected.

We also suggest the inclusion of a clear 'proportionality' requirement, i.e. the type and amount of personal information collected should be no more than is required for the collector's primary purpose. It should certainly not be possible for collection to be justified on the basis of a secondary use, or a subsequent use by a third party, unless that use is required or expressly authorised by law (see

[13] See Complaint Determination No 4 2004 (TICA) and the current complaint about disclosure of CLI information by telcos to ISPs.
[14] and in the NZ Act (IPP 1(a)), the NSW PPIPA(IPP 1(1)(a) and the HK Act (DPP 1(1)(a).

comments below about NPP 2). The 'unreasonable intrusion' element of NPP 1.2 could contribute to this objective, but currently only applies to the means/method of collection, and so cannot be considered a complete proportionality requirement.

Consideration should also be given to including a provision found in the Canadian federal private sector privacy law (PIPEDA) – that collection be allowed 'only for purposes that a reasonable person would consider are appropriate in the circumstances' (s.5(3)). This would help to ensure that organisations are clear from the outset about not only the function or activity the information supports, but the primary purpose for which it will be used.

The collection principle, and the way it interacts with NPP 2, should also be strengthened to prevent unreasonable 'denial of service' to individuals who choose to withhold information requested for non-essential purposes or consent for non-essential secondary uses or disclosures.

Examples of the situations which call for the changes we suggest above are:

- Excessive requirements for evidence of identity

- Attempts to legitimise secondary purposes not essential for the primary transaction, either by simply notifying individuals (relying on 'creating awareness) or by seeking consent either as a condition of the primary transaction (see comments on the bundled consent issue under NPP 2 below) or on an opt-out basis.

Notice requirements

The notice requirements of NPP 1.3/1.5 form an important foundation for the operation of the other principles. While many organisations now give a form of notice when collecting personal information, there are many examples where these notices clearly do not include all of the required information, and not all of these provide links to information elsewhere.

In many collection situations, some of the information specified in NPP 1.3 is self-evident or clearly available elsewhere (e.g. the identity of the organization) and does not need to be given separately. For that reason we have no difficulty with the 'reasonable steps qualification' in this principle. However, we suggest that there is widespread non-compliance, which will not realistically be exposed by complaints, other than incidentally pursuant to other issues. Further guidance – in the form of acceptable and inadequate example notices - would be helpful. More importantly, this is a clear example of where a pro-active auditing is required – only if the OFPC identifies and publicises non-compliant notices can general business practice be expected to improve.

We recognise the difficulty of balancing the amount of information and its intelligibility and clarity. There is no doubt that many of the notices and statements issued around the commencement of the private sector provisions were unhelpful and confusing and probably did more harm than good in terms of public awareness and understanding. Many individuals were and continue to be understandably irritated by the length of some statements and their interruption of transactions – particularly telephone transactions. We suggest that there is considerable scope for layering of privacy notices and statements – with short concise statements of the main points and links to sources of further information. However any discretion in meeting the requirements of NPPs 1.3, 1.5 and 5 could easily be abused. For this reason we would like to see the Commissioner become much more proactive in issuing template notices for different sectors. These should be developed in consultation with industry bodies and relevant NGOs.

The application of NPP 1.4 in practice remains unclear – we are not aware of any evidence that organizations have changed their collection practices in favour of 'direct' collection, and there are

numerous examples of accepted industry practice where third party collection is the norm. It is also unclear as to how this principle affects verification or checking of details provided by an individual. We do not necessarily suggest any change to this principle, but its application could be better explained than in the OFPC Guidelines of September 2001.

We are very concerned about the practice of organizations unilaterally altering their privacy policies and expecting individuals to become aware of changes without express notice. We take this issue up under NPP2 below, but there may need to be a corresponding change to NPP 1.3 and 1.5 to make it clear that telling individuals in terms and conditions that privacy parameters may change from time to time does not constitute reasonable steps to notify any relevant matters under NPPs 1.3 or 1.5.

Anonymity – NPP 8

The anonymity principle has so far failed to live up to its potential as a significant protection device. This is partly because of inadequate promotion and enforcement by OFPC. More than any other principle, NPP8 needs to be implemented at the design stage of new initiatives – three current examples are the use of electronic road tolls, smart public transport fare cards, and the introduction of RFID (smart tags) into the supply chain. In all these cases, applications are in danger of being able to claim 'impracticability' as an excuse for not offering anonymous use options, only because OFPC and other regulators have failed to intervene at the design stage, and because Privacy Impact Assessment is not required.

The principle itself could also be improved by mandating 'pseudonymous' options as a next best practice where anonymity is either impracticable or unlawful. There are many scenarios where pseudonymity is a practicable alternative. It could be implemented by the addition to NPP 8 of words along the lines of:

> 'or not identifying themselves until it becomes necessary for the protection of the interests of the organisation that they do so'.

To support more assertive enforcement of the principle, we also suggest the addition of a second obligation:

> 8.2 'Organisations must design information systems to facilitate the practicable observance of NPP 8.1." to ensure anonymity / pseudonymity should be 'designed in'.

Collection – Sensitive Information – NPP 10

See suggestion above under 'Definitions' for deletion of this concept and principle

Use and disclosure – NPP 2

The Act should clearly define use to include 'mere' access, to avoid the unfortunate interpretation in court judgements that mere access or browsing does not amount to use[15]. The definition of use in s.6 should also be amended to delete 'use…does not include mere disclosure', on the basis that no-one has understood what this means since it was enacted in 1988 (in the context of separate use and disclosure principles in the IPPs).

[15] See *R v Brown* [1996] 1 AC 543 and *MT v Director General, NSW Department of Education & Training* [2004] NSWADT 194

The way NPP2 works in practice is closely entwined with NPP1 – the purposes for which organisations can use or disclose personal information are influenced by how they have defined their purposes and communicate these to individuals.

It would be helpful if the Act clarified whether an organization can have more than one primary purpose.

Because no consent is required for an organisation's primary purpose(s), there is an incentive for organizations to define their primary purpose or purposes very broadly, which is unhelpful in relation to protection under some of the other principles. To counter this incentive, we propose a limitation on 2.1(a) – organisations should only be able to take advantage of the 'related purpose within reasonable expectation' exception if their primary purpose has been sufficiently specific. If an organisation chooses not to be specific, or to define multiple primary purposes, then they should not also have the flexibility offered by 2.1(a).

As already mentioned under Collection, we are very concerned about privacy policies which are subject to change without notice. This is an unfair contract terms issue, which we have commented on recently in a submission to the Australian Communications Industry Forum (ACIF) on its draft Consumer Contracts Code[16].

We suggest that there should be a statutory requirement for privacy policies and notices under NPP 1.3 or 1.5 to be dated, and that amendments to those policies should not be allowed to apply to personal information collected before the date of the change, unless individuals concerned have been given express notice and an opportunity to either opt-out of the changed terms, or to terminate their relationship without detriment.

The Act should expressly state that recipients of personal information from third parties are limited to uses no broader than the purposes for which the third party could legitimately disclose the information. IPP 11.3 makes this explicit for Commonwealth agencies and the same limitation should apply to the private sector.

Use and disclosure exceptions

Consent, bundling and opt-in/opt-out

The provision for secondary uses with consent (either express or implied) (NPP 2.1(b) is superficially unarguable, but in practice is regularly abused.

Consent is only meaningful where it is both informed and free, i.e. capable of being withheld. In the many circumstances where individuals are required to agree to specified (or general) uses and disclosures as a condition of a relationship or transaction, consent is not truly free. It is more appropriate in these cases for so called 'consent' clauses to be replaced with a 'notice and acknowledgement' clause.

For both consent and notice/acknowledgement, bundling is a key issue which the OFPC has previously highlighted as seriously undermining the operation of the Act. Individuals are commonly asked or required to sign off on a 'package' of uses and disclosures, at least some of which are non-essential for the transaction being entered into. Lack of awareness and/or understanding, together with an imbalance of power means that few consumers ever challenge such requests, but this should not be taken as indicating acceptance of a fundamentally privacy intrusive practice. The fact that when

[16] See http://www.privacy.org.au/Papers/ACIFreUnfairContracts

challenged many businesses 'back off' and allow consumers to withhold some information or consent confirms the non-essential nature of many secondary uses.

We accept that 'bundling' is reasonable in some circumstances – for example it is reasonable to reserve a right to investigate future claims when selling insurance. Such exceptions should be addressed with notice/acknowledgement of the secondary use as a condition of the initial transaction. However it should not be open to businesses to make consent for non-essential secondary uses a condition of doing business. The default position should be that clear separate consent is obtained for 'discretionary' secondary uses.

The extent to which consent for secondary uses should be by positive means (opt-in) as opposed to accepting 'notice and opt-out' is highly contentious. We strongly favour opt-in as the default position, but we accept that for some relatively innocuous secondary uses, an opt-out facility could be sufficient, provided it is clearly enough promoted.

It may be helpful in re-designing this aspect of the NPPs to make a distinction between essential and non-essential services. Where individuals are entering into transactions for essential services (e.g. housing, utilities, basic finance) it should generally not be open to providers to even offer secondary use options, whereas with purely discretionary goods and services, the tolerance for secondary use options, and for opt-out rather than opt-in, could be higher.

Direct marketing

If NPP 2 is interpreted and applied as it should be, we doubt if the provision of a specific direct marketing exception at (NPP 2.1(c)) adds any value. It has caused considerable confusion as, unlike the other exceptions, it imposes additional obligations. But as the Issue Paper makes clear, the requirement to offer an 'opt-out' does not apply to the wide range of direct marketing that is either the primary purpose of collection or relies on NPP 2.1(a) or (b).

In our view, the level of public irritation with direct marketing, and the general lack of awareness and understanding of marketing methods, justify a simple across the board requirement for prior consent (opt-in). This could be based on the Spam Act model which allows for either express on inferred consent, although we suggest that the ACA guidance on inferred consent allows for practices which would be outside the reasonable expectation of most consumers, and this aspect of an opt-in regime should be tighter.

A requirement for prior consent should apply to all direct marketing (including by political parties, charities and government bodies, which have been unjustifiably exempted from the Spam Act) even where it is a primary purpose or a clearly notified secondary purpose.

A very much second best amendment, but still better than the current position, would be to require all organisations to offer an opt-out with each communication, to apply to all direct marketing. This is in any case industry best practice, and it is difficult to see whose interests, other than direct marketing service providers, would be harmed by a general opt-out requirement for direct marketing. Certainly suppliers who advertise by direct marketing would benefit from not paying for messages to be sent to individuals who had clearly expressed a preference not to receive them.

In the absence of our preferred prior consent requirement, and possibly even as a supplement to it, we would also support the creation of easily accessible national 'do not market' registers. Our position on this is spelt out in our submission to the Australian Commmunications Authority Inquiry on

regulating the use of telecommunications customer information[17]. We attach our submission as Annex F.

Required or authorized by law

An exception for uses or disclosures that are expressly required by other statutes is necessary and desirable. We are less convinced of the need for the exception 2.1(g) to include 'or under' and 'authorised'. Together, these words massively expand the scope of the exception – whether an action is 'authorised under' a law is highly subjective and open to debate. This ambiguity is further increased if 'law' is taken to include the common law.

We believe that it should be possible to restrict the exception to 'where expressly or impliedly required by a law'. 'Law' could be further defined as a law of an Australian legislature, to avoid any suggestion that a requirement of a foreign law would suffice unless expressly recognised in Australian law. It may also be appropriate to consider whether 'law' should be restricted to Commonwealth (federal) statutes – there need not be an assumption that any State or Territory laws requiring information should automatically override the protection conferred by a federal statute.

The onus should be on others to demonstrate why other uses or disclosures considered desirable in the public interest would not fit within this tighter exception or one of the other exceptions.

It should also be acknowledged that it is exception 2.1(g) more than any other that undermines the 'honesty' of privacy statements and policies which seek to re-assure individuals about confidentiality. The vast array of powers under which a wide range of public agencies can require disclosure of personal information means that such assurances are very misleading. This is probably unavoidable, but it does at least require diligent enforcement of the NPP 1.3 and 1.5 notice requirements to insist on an 'or as required by or under law' qualification to any confidentiality assurance.

We believe that individuals are entitled to know when information about them has been used or disclosed for unrelated secondary purposes under an exception to NPP 2. NPP 2.2 provides some limited accountability in that individuals would sometimes be able to access the note of a law-enforcement use. We believe the note-making obligation in 2.2 should be extended to any use and disclosure under exceptions 2.1(d)-(i) inclusive. We further suggest that a general requirement be added to NPP2 that any organisation using/disclosing personal information under exceptions 2.1(d) – 2.1(i) inclusive must notify the person concerned of this within a specified period of time (with limited exceptions where this would be against the public interest, potentially damaging to the individual, or where the use or disclosure was self-evident).

Access and correction – NPP 6

This principle should expressly require organisations to give access to as much information as possible even where an exception applies to some information. This is already implicit in the wording of 6.1 but is not widely understood or applied in practice. It would be helpful to include guidance as to methods of complying, such as 'by selective editing'.

The weak obligation in NPP 6.3 to only 'consider' intermediary access should be replaced by a general obligation to provide intermediary access wherever access is denied under an exception.

The provision in NPP 6.4 for charges for access to not be excessive seems reasonable, but has been undermined by the Commissioner's interpretation of what is reasonable. In our view the charges

[17] See http://www.privacy.org.au/Papers/ACACustInfo0405.doc

levied by TICA apparently considered reasonable by the Commissioner in Determination No 1 of 2004 – $5.45 per minute for telephone access - are manifestly excessive. Unless the Commissioner's office adopts a more consumer friendly approach to NPP 6.4 we recommend amendment of the clause either to make access free, or to set a reasonable cap.

NPP 6 should expressly provide for the Privacy Commissioner to inspect a record on a person's behalf, where access is legitimately denied under an exception, and where appropriate to also seek corrections (etcetera) on their behalf. (Note: The expression corrections (etcetera) is used in this section to indicate that the action sought may be deletion or annotation rather than changes)
There should be a requirement to consult with third party individuals whose information would be disclosed in response to an access request – modelled on the 'reverse FOI' provision in the Freedom of Information Act 1982 (s.27A).

There should be a prohibition on an organisation requiring an individual to exercise their access rights with a second organisation and then providing the first organisation with the information. We understand that this is a common method of obtaining criminal history information from police, using FOI access rights. While we are not aware of specific cases of this under the private sector jurisdiction (the OFPC may have dealt with them), it has been a common problem in other jurisdictions and is likely to be happening in Australia in contexts other than criminal history. One problem in identifying this abuse is that the individuals being co-erced are unlikely to be in a position to complain.

The onus of proof in NPP 6.5 on the individual should be lessened. It should not be necessary for an individual to 'establish' that personal information is inaccurate (etcetera) – it should be sufficient for them to have reasonable grounds to believe there is a potential inaccuracy (etcetera); and the organisation should then be under an obligation to review data quality.

Where personal information is corrected in response to a request under 6.5, there should be an obligation to notify any third parties that are known to have received incorrect (etcetera) information. Such a requirement 'where appropriate/practicable' appears in the NSW, NZ, Canadian federal and HK privacy laws.

Codes of Practice

There has been relatively little take up of the Codes option by the private sector. We do not find this surprising and have always been sceptical of the government's enthusiasm for the Code provisions. A Code cannot, overall, lower the standards of the NPPs and that is a critical feature that must remain. Given this, and the equally important feature that decisions of Code Adjudicators can be appealed to the Privacy Commissioner, there is little advantage to businesses in developing or adopting a Code. The Code development and approval process is, quite rightly, fairly lengthy and onerous, and if a Code includes a complaints handling process this is effectively privatising costs which under the default scheme are borne by the government.

The main reason for having a Code would appear to be industry public relations – demonstrating a commitment to privacy protection above and beyond mere compliance with the Act, and this would seem to be the motive behind those Codes that have been submitted for approval. Codes also allow the principles to be customised in sector-specific language and with sector specific examples, but this would not seem on its own to be a sufficient reason.

We have some concern that a proliferation of Codes would further confuse the public and detract from the already difficult task of building awareness of the Act and the Commissioner. Where a Code

provides for complaint handling there is also the potential for complaints to be delayed by jurisdictional uncertainty – this has been the experience with the General Insurance Privacy Code (currently the only Code with a separate Code Adjudicator).

We can see some merit in Codes which deal with specific issues or technologies, although we suggest that the guidance they contain would be more appropriately delivered in the form of binding guidelines rather than as a replacement set of Principles. It is far from clear how the proposed Biometrics Code will work in practice, given that users of biometrics will remain subject to the default NPPs for those parts of their activities that do not involve biometrics.
If the Code provisions in Part IIIAA are to remain, we make the following suggestions.

- Codes should be disallowable by Parliament – they amount to subordinate legislation, and it is not appropriate for the Privacy Commissioner to be able to vary the law without parliamentary oversight and approval

- The Privacy Commissioner should be able to initiate a Code – as the HK and NZ Commissioners can and have done.

- The Privacy Commissioner should be required to make public the submission by a code proponent dealing with public consultation and how they have addressed input.

- The Courts should be expressly deemed to have notice of codes in the Register kept by the Commissioner (this is necessary in light of the judgement in Kadian v Richards [2004] NSWSC 382)

- The Commissioner should be able to review any decision of a Code adjudicator, not only determinations (s18BI)

Resources and Powers of the Privacy Commissioner

Enforcement of Systemic Compliance

Both by design and by failure to provide the Privacy Commissioner with adequate resources, the regime relies largely on complaints. This is a completely inadequate way of seeking to promote privacy compliance. Many interferences with privacy go unnoticed by the particular individuals involved, and even where they are noticed, they rarely cause such significant harm as to warrant the time and effort of complaining. This does not mean that they are unimportant – the cumulative effect of repeated small scale intrusions is just as corrosive of trust in organisations as a few major privacy breaches. Inadequate resourcing means that, amongst other things:

- There are very low levels of awareness about how and where to complain (see OFPC Research 2004)
- The OFPC has very limited resources to conduct own-motion investigations, or to follow up systemic issues revealed by individual complaints.

Problems that we see constantly repeated over many years are not being adequately addressed. It should not be necessary to keep bringing individual or even representative complaints, which are a very inefficient way of addressing systemic problems. Instead, the FPC should be more pro-active in addressing systemic issues using her own-motion investigation powers. The best examples of this

failure to date are in the area of credit reporting and debt collection, which are addressed in detail in submissions by relevant specialist NGOs.

In our view, there has been a general reluctance by the OFPC to recognise the important potential role of consumer representative groups (NGOs) in making the Act work. Provision for representative complaints is useful, but not an efficient way of dealing with systemic concerns identified by NGOs. The OFPC should give priority to dealing with systemic concerns raised by NGOs (and other third parties including the media) without requiring a specific complaint to be brought, involving major resource effort and delays. Slavishly giving priority to individual complaints helps fewer people in the long term than using enquiries, complaints and third party referral of issues to identify systemic issues which can then be addressed with own-motion investigation powers (and audit powers in those jurisdictions where they are available).

There is currently no incentive for respondents to complaints to correct systemic flaws. In most cases, the worst outcome for a respondent, regardless of how bad the conduct, is that they must amend the records. At least in the credit reporting area, the cost of dealing with a moderate number of complaints is apparently less than the cost of ensuring the data is accurate in the first place.

There is a lack of information provided to complainants (or their advisers) when raising repeated (or systemic) problems. While the specific complainant's problem may be resolved, the adviser is rarely informed whether there has been any response to what might be a broader problem with a particular respondent. We understand that the OFPC sometimes provides advice to major respondents that goes beyond anything made public. Consumer advisers should be aware of what that advice is.

Complaints provisions

Notwithstanding our comments above, complaints remain a very important part of the regime, and we have a number of suggestions for changes to Part V and its operation, based on the experience of consumer groups in assisting individuals, and on our members' observations of the process over 15 years.

Need for streamlined complaints processes

Experience suggests that complex problems or problems involving less co-operative respondents can simply exhaust consumers – and their advisers. In some cases a consumer is required to put the same complaint in writing 3 or 4 times and is passed backwards and forwards between OFPC and one or more respondents. The OFPC should be able to facilitate communications and speed up the processing of complaints.

In this respect, there should be an express power for the OFPC to 'sort out' what principles have been breached and who is the appropriate respondent – the onus should not be on complainant – responsibilities for handling personal information are often very confused. It should not be necessary to make this explicit, and we note that the Commissioner has stated that " … the Privacy Act does not require complainants to specify which NPPs may be relevant to the complaint they are making"[18]. But experience suggests that OFPC is not always as pro-active as it could be in researching a complaint to establish which principles, and respondents, might be involved.

[18] In Complaint Determination 2 of 2004, footnote 2.

Right to a determination

A dissatisfied complainant (or respondent although this is less likely) should be able to insist that a complaint be dealt with by a s52 Determination. This would provide them with detailed information as to the reasoning of the Commissioner in disposing of their complaint, the satisfaction of a public acknowledgement of a breach and a basis on which to consider the options of appeal to the AAT (in relation to any compensation) or judicial review. The way most complaints are currently closed – on the basis that they have been adequately dealt with by the respondent, gives the complainant none of these benefits.

Hearing of issues

Experience – specifically of recent representative complaints - suggests that there is a need to ensure that there is a full and proper hearing of issues prior to a s.52 determination – in accordance with the spirit of s43(5).

Determination to include specification of reasonable acts

The recent experience of representative complaints against TICA revealed the alarming view of the Commissioner that s.52 did not allow him to make specific rulings as to the acts and practices which would satisfy the principles. He took the view that the wording of s.52(1) only allowed him to declare a breach and actions to redress any loss or damage – and that any positive suggestions as to actions which would avoid further breaches could only be 'recommended' under s.27.

We submit that this interpretation significantly undermines the value of the s.52 Determination provision. Respondents are free to ignore recommendations and the only remedy for individuals is to then make a further complaint. This could end up in a continuing charade whereby the respondent is told what he cannot do, but cannot be giving binding directions as to what they must do.

We believe that the then Commissioner's view may have been over-cautious, but if it is supported by legal advice then s.52 needs amending to make it clear that the Commissioner can specify reasonable acts to be performed where an interference with privacy has been established.

Right of appeal

Both complainant and respondent should have a right of appeal against any s52 determination, in the form of merits review, preferably initially to a low cost tribunal (the AAT) and then to the courts (initially either Federal Magistrates Court or Federal Court).

Transparency of complaints processes

There is insufficient transparency of the complaints processes, including inadequate details of complaint-resolution policies and procedures; information about these has only emerged piecemeal via the few reported complaints.

We support the suggestion that the OFPC should publish online a comprehensive manual of its complaint resolution policies and procedures, and keep it up-to-date.

Reporting of complaints

There is inadequate reporting of complaints outcomes, despite recent improvements. The absence of a substantial body of reported complaint outcomes makes it very difficult to illustrate the way in which the Act can work for individuals. The media in particular, but also consumer advisers, need 'real life' examples to work with. Concerns about confidentiality and mediation can be dealt with by anonymisation of reports. As a result of the limited publication of cases there is only a limited deterrent effect, and neither organisations nor individuals have any guidance as to the 'tariff' in terms of both the standard required or the appropriate penalties (including appropriate amounts of compensation) for breaches. The lack of publication of the Commissioner's interpretation of the law also limits her/his accountability – without knowing the position that she/he has taken it is impossible to challenge it.

We support the suggestion that the OFPC should develop criteria of seriousness which would guide the decision whether to publish anonymised complaint case studies.

Content of reports

Published complaint case reports should contain sufficient detail to allow readers to understand both the circumstances and the Commissioner's reasoning in forming a view as to whether there has been an interference with privacy. Complainants should be given the option of being named in case studies – some may see this as an additional vindication, and may be content to discuss the case with others, including the media. There are good arguments both for and against naming of respondents, but even if the default position is non-identification, we agree with the suggestion that the Commissioner should have the discretion to name respondents where she considers this to be in the public interest, e.g. to warn other consumers of inappropriate conduct which might be repeated.

Equally, if a complaint has been resolved and changes made, a positive result could present the offending body in a positive public light. Not all findings are detrimental to the involved parties.

The Commissioner should also report, via her annual reports and on the OFPC web site, on relevant cases in the AAT or courts, and, where possible, in other jurisdictions. The AustlLII databases[19], familiar to most lawyers and policymakers, already contain many such cases, and access has been made even easier through the dveloping WorldLII Privacy & FOI Project[20], but this resource can only be as good as the input from Commissioners and others, and in any case direct reporting by Commissioners will reach other markets.

Statistical reporting

It is also important that OFPC reports in detail and consistently on enquiries and complaints, so that interested parties can assess overall performance and trends. Again, there have been improvements in reporting in recent years but more detail should be provided.

[19] See http://www.austlii.edu.au/
[20] See http://www.worldlii.org/int/special/privacy/

Possible requirements for training and for management plans

There is a natural tendency for laws to lose their 'bite' over time, particularly where, as with privacy laws, enforcement action is very limited and the publicised consequences of breaches are only minor. Many private sector organizations put significant resources into setting up compliance systems and staff training around the commencement in 2001-02, but this will inevitably have fallen away subsequently. Staff turnover, and changes to business practices, mean that there is a need for regular new and refresher training and for updating of compliance plans.

In public sector privacy jurisdictions, this issue has been addressed with ongoing requirements, e.g. privacy management plans in the NSW Act (and, for Commonwealth agencies, the digest returns already mentioned above).

Consideration should be given to:

- a requirement for significant personal data users to maintain a publicly available privacy management plan. This would force them to revisit compliance periodically.

- a requirement for at least larger organisations to nominate a designated privacy contact officer for contact by the public and the regulator, and to publicise the contact details (there is now a useful precedent for this in the Spam Act 2003.

- a requirement for larger or significant organisations to have to conduct and report publicly on periodic privacy audits.

Abuse of Privacy Act as an excuse

It is all too common for organizations to cite 'privacy laws' as the reason for not doing something they don't want to do for other reasons, even where there is no factual basis for such a claim. While it is difficult to legislate against misrepresentation of a law's effect, and while some such claims may be based on genuine misunderstanding, there should be some sanction to act as a deterrent against willful misrepresentation of the Privacy Act.

Consideration should be given to empowering the Privacy Commissioner to issue or require 'corrective statements', which would have to be published at the expense of the organization concerned. Repeated misinformation should attract more severe sanctions.

Powers

The range of functions and powers available to the Privacy Commissioner are generally adequate – but are rendered ineffective due to lack of resources (see below). There are some significant changes in powers and functions which we would like to see:

- An extension of the audit function to apply to compliance by private sector organisations with the NPPs
- The ability to initiate a Code of Practice under Part IIIAA to deal with particular issues affecting the private sector, and clarificaton that Codes can set higher standards than the NPPs (see under new Technology above). This suggestion is subject to our general recommendation that the IPPs and NPPs be merged to apply to both private and public sectors.
- A power for the Commissioner to *selectively* require agencies and organisations to publish details of major projects or proposals with significant privacy implications. The Digest provisions applying to Commonwealth agencies (IPP 5.3 and s.27(1)(g)) perform an

important function in at least ensuring that Commonwealth agencies regularly review their holdings of personal information, and the Digest publication by the Commissioner supports the transparency objective also met by IPPs 2 & 5. But the publication has not been well used by third parties. There is currently no equivalent in the private sector regime. We suggest that consideration could be given to a modified disclosure requirement, applying in both the public and private sectors[21]. This would support the requirement for PIAs – see below.

- An express role for the Privacy Commissioner in relation to a new requirement, based on appropriate criteria, for Privacy Impact Assessments (PIAs).
- A power to issue or require corrective statements

For further contact about this submission, please contact

Nigel Waters
Board Member and Policy Co-ordinator, APF
Phone: 02 4981 0828, 0407 230342
Email: nigelwaters@iprimus.com.au

[21] The Hong Kong Personal Data (Privacy) Ordinance contains a discretion for the Privacy Commissioner to require registration by specified classes of data user (Part IV) which could provide a suitable model.

Annex A

The Senate Legal and Constitutional Committee's Terms of Reference for this Inquiry

(a) the overall effectiveness and appropriateness of the *Privacy Act 1988* as a means by which to protect the privacy of Australians, with particular reference to:

(i) international comparisons,

(ii) the capacity of the current legislative regime to respond to new and emerging technologies which have implications for privacy, including:

(A) 'Smart Card' technology and the potential for this to be used to establish a national identification regime,

(B) biometric imaging data,

(C) genetic testing and the potential disclosure and discriminatory use of such information, and

(D) microchips which can be implanted in human beings (for example, as recently authorised by the United States Food and Drug Administration), and

(iii) any legislative changes that may help to provide more comprehensive protection or improve the current regime in any way;

(b) the effectiveness of the *Privacy Amendment (Private Sector) Act 2000* in extending the privacy scheme to the private sector, and any changes which may enhance its effectiveness; and

(c) the resourcing of the Office of the Federal Privacy Commissioner and whether current levels of funding and the powers available to the Federal Privacy Commissioner enable her to properly fulfil her mandate.

Annex B – Australian Privacy Charter from http://www.privacy.org.au/About/PrivacyCharter.html

Annex C - APEC Privacy Framework – A new low standard – Greenleaf ([2005] 11(5) PLPR)

Annex D – APF submission on Biometrics Code, also at
http://www.privacy.org.au/Papers/BiometricsCode0403.doc

Annex E – APF submission to ALRC on genetic information

Annex F – APF Submission to ACA on Directory Information, also at
http://www.privacy.org.au/Papers/ACACustInfo0405.doc