Australian Privacy Foundation

p o s t: GPO Box 1196
Sydney NSW 2001

e m a i l: enquiries@privacy.org.au

w e b : www.privacy.org.au

6 June 2005

Commentary on *Getting in on the Act*: The Review of the Private Sector Provisions of the *Privacy Act 1988*

Introduction

This document is a review of the Office of the Federal Privacy Commissioner's report, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* ("the review report").

This document does not seek to re-iterate the Australian Privacy Foundation's views on the adequacy or operation of the Privacy Act 1988. Our views are set out comprehensively in two recent submissions:

- *Review of the Private Sector Provisions of the Privacy Act 1988* (December 2004), and
- *Senate Committee re Review of the Privacy Act* (March 2005)

Both submissions are available from the Australian Privacy Foundation website, at: http://www.privacy.org.au/Papers/index.html

This document is instead intended as a brief commentary on the OFPC's review report, focusing on:

- the scope and tenor of the review
- the structure of the review
- conclusions drawn, and
- some of the recommendations arising

The scope and tenor of the review

The review focused just on the operation of the newer 'private sector provisions' in the Act. These unnecessarily restrictive terms of reference for the review, which were determined by the Attorney General, have resulted in a review report which attempts to draw conclusions in somewhat of a vacuum.

This is by no means the fault of the Privacy Commissioner. Indeed one of the Commissioner's key recommendations is for a wider review of the entire Act, and this recommendation is supported by the Australian Privacy Foundation.

The Australian Privacy Foundation also hopes that the wider review being currently conducted by the Senate Legal and Constitutional Committee will provide more of an analysis as to whether or not Australians' privacy is being adequately protected by the Privacy Act.

Nonetheless on a number of complex issues that were directly within scope, the review report appears to duck the hard work of formulating a position, preferring instead to suggest that topics such as access to private sector records for medical research be further considered in a wider review.

Even taking into account the narrow terms of reference for the review, the Australian Privacy Foundation is disappointed to find that the review report fails to assess whether or not privacy protection has improved in a meaningful way since the introduction of the private sector provisions. The focus instead appears to mostly be on how well business has coped with the change. In general therefore, the tone of the analysis and the recommendations appear to give more weight to the concerns of business than either the individual or the public interest.

The Privacy Act was designed to protect the rights of individuals - while keeping the impact on business to a minimum. Therefore any evaluation of the Act and the privacy principles should logically preference the protection of the rights of the individual, and thus first and foremost assess whether the protection of privacy is being achieved. Unfortunately, several areas of this report do not take that position.

Indeed in several instances, key issues in the report appear to have been analysed solely through the lens of 'impact on business'.

For example, the issue of the continued lack of EU acceptance of the Privacy Act is treated as an issue for business, such as by examining the impact on trade. The impact on consumers of international data exchange is virtually ignored, despite the significant risks for consumers posed by data export, data havens, and globalisation of business interests.

Another example is provided by the analysis on gaps and overlaps within the Act itself and with other jurisdictions, particularly with respect to health and the privatisation of formerly public service activities. We are pleased to see attention paid to these on-going problems, and support the majority of recommendations to address these problems. However again the report's evaluation of the problem is very much cast in the light of the 'cost to business', without considering the impact on individuals seeking to exercise their rights, or the impact of accountability gaps on the public interest.

A further example is provided in the description of the problems caused by the length of time taken to address complaints in the Office. The analysis again appears to preference business interests, by highlighting the cost of 'investment' in compliance, which is seen to necessitate the speedy resolution of complaints made "against them", before any mention is made about complainants also obviously preferring speedy investigation and resolution.

We are concerned that the tone is almost antagonistic towards complainants, as if those who bring privacy complaints are creating a nuisance for business. We believe that the consideration of the impact on business in a complaint situation should not

be preferenced over that of the consumer. Generally speaking, the complainant has much less power than the respondent, and is more deeply and immediately affected by the issue at hand. Far more so for complainants than for businesses, justice delayed is justice denied. This is perhaps nowhere more apparent than in the areas of residential tenancy databases and credit reports, where inaccurate or irrelevant information can block a person's access to housing and household necessities. If our reading of the tone of the report is correct, it would suggest a much greater problem in terms of the attitude of the Office to the relationship between consumers and business.

The structure of the review

The Australian Privacy Foundation commends the OFPC on the comprehensive nature of the report. It is well structured by exposing and summarising submissions as they relate to thematic issues, and provides the options identified and recommendations proffered as a result of the analysis of the OFPC.

However some ranking or prioritising of the recommendations would perhaps have lent more force to the report in terms of its utility for policy-makers. Likewise less timidity in the presentation of many of the recommendations could have spurred more action by the Government, such that instead of being encouraged to just "consider" doing something (thus necessitating further consultation and endless reviews), it could have been given the permission as a result of this review to just "do it".

The conclusions drawn

The key conclusion of the report – that the "provisions work well on balance" - is not supported by the statements later in the report's discussion, where there are clearly identified differences of opinion from various parties. If everyone is equally unhappy with the Act one might say there is "balance", but this does not necessarily suggest that the provisions "work well".

Furthermore the conclusion that the NPPs have "delivered to individuals protection of personal and sensitive information" is not supported by the views of consumer and privacy advocates, who were described overall as "less satisfied that the private sector provisions had met their objectives of adequately providing for the privacy rights of individuals".

Indeed the 'business versus consumer' approach is ultimately unhelpful, as it virtually ensures that the Office, and the Act, cannot please everyone. The Office is surely setting itself up for criticism from either 'side', as being either 'pro business' or 'pro consumer'. We suggest a more rounded approach to considering the role of privacy protection in society, and thus a less adversarial framework for evaluating the effectiveness of the legislation.

While there are points in the report at which the public interest is raised, particularly in the section about medical research, too often the analysis is presented in terms of a simple dichotomy of business versus 'consumers' (not citizens). There is very little analysis in terms of the bigger issues of public good and the public interest.

We believe that a more comprehensive evaluation of the effectives of the Privacy Act should include the criteria of public benefit as part of the equation. This might reduce the animosity that comes about when issues are presented in terms of a head to head battle between business and consumer. For example, there should be consideration of the role that privacy protection plays in engendering trust, that staple of social capital upon which rest our modern liberal democratic society and market economy.

Commentary on the recommendations

Recommendations 2-4 are aimed at addressing problems of national consistency, but if applied without the agreement of the States and Territories would lead to a lessening of privacy protection for Australians. We urge a sense of caution before any move is made to allow the Australian Government to 'cover the field' on privacy issues if it is not first willing to address the significant gaps in the coverage of the Privacy Act – most particularly, in the areas of employee privacy, the small business exemption and surveillance, but also exemptions for the media and political parties. If those gaps were first filled, the States and Territories would have less demand to legislate for their own jurisdictions.

Recommendation 8 is aimed at clarifying the complex operational relationship between the Telecommunications Act and the Privacy Act. The Telecommunications Act is unusual in that it both sets higher use and disclosure standards (i.e. more limited) than the Privacy Act, but it 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.

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 support this recommendation, in line with the OFPC's warning that the Privacy Act should not be used to lower the requirements in the Telecommunications Act.

We strongly support recommendation 9, to ensure that telecommunications businesses of all sizes are regulated by the NPPs. Likewise we strongly support recommendation 15, to bring all residential tenancy databases under the regulation of the Act.

Bundled consent was identified as a concern with respect to tenancy databases, as well as other areas such as telecommunications. This is particularly problematic for people seeking shelter as a tenant, or wishing to contract for telecommunications services. The market power of the provider effectively negates the notion that a person is genuinely 'consenting' to how their personal information is to be handled, if to refuse their consent means they cannot obtain housing or a telephone.

While the OFPC report identifies and extensively discussed these problems – and indeed we are pleased to note the OFPC has been vocal about this issue for some years now - we are greatly disappointed that the report makes no recommendations on how to address this problem. Instead, recommendations 19-21 focus on short forms of privacy notices. We feel that this is an inadequate response to an on-going problem of abuse of consent requirements by business.

We support some of the recommendations aimed at more meaningful enforcement, such as recommendations 40 (review rights) and 44 (remedies). However recommendation 46 brings some concerns.

Recommendation 46 suggests the Privacy Commissioner should be allowed to decline complaints "where the harm to individuals is minimal and there is no public interest in pursuing the matter." Although at first glance this appears to be a reasonable position, possibly due to limited resources, we do not agree that the Privacy Commissioner should be able to pick and choose which complaints to investigate.

To allow complaints to be declined on the basis that no actual harm has been suffered firstly does not take into account the inter-relationship between privacy principles. For example people are unlikely to suffer direct 'harm' from the absence of a collection notification, or a failure to ensure the secure storage of their personal information per se – but either of those actions may lead to a misuse or disclosure.

To allow complaints to be declined on the basis that no actual harm has been suffered also rewards dumb luck by organisations, and will encourage an attitude of complacency instead of proactive compliance programs.

Furthermore a practical issue is raised – how would the Office determine what 'harm' the person has suffered, or where the 'public interest' lies, without conducting at least a preliminary investigation? The Office's resources may well be taken up debating the relative 'harm' and the 'public interest' between the two parties, instead of just getting on with resolving the matter.

We therefore do not support recommendation 46. However if recommendation 46 is to be followed, purely on the basis of a measure to allow the Office to focus its resources on complaints that suggest systemic problems, we argue that there must be a corresponding allowance for direct civil action by individuals against organisations that breach the Act.

Codes of practice was a consistent theme, raised with regard to tenancy databases and other areas. Recommendation 47 states that the Office's guidelines on the development of Codes should be simplified. Our position is that Codes add little value, diminish clarity in the law, and disperse accountability. Codes are no better than legislation that is not enforced.

Recommendation 51 nominates changes to the small business exemption, to align with the ABS definition of small business (based on less than 20 employees) rather than turnover. We agree that the current threshold is both too high and lacks clarity for a consumer. However we believe that privacy risks are contextual, rather than created or heightened simply by the size of the business. 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, dating agencies and tenancy databases. (We are pleased to note that recommendations 9, 15 and 52 should actually address some of these problems.)

Nonetheless, while no more related to privacy risk than turnover, we support the OFPC's recommendation 51, since a number of employees threshold would at least be familiar to many businesses and somewhat more transparent to consumers. However we argue that the threshold should be lower, at the level of around 5 employees, consistent with anti-discrimination legislation.

We support recommendation 53 with respect to the "with consent" provisions within the small business exemption, so that if a small business collects or discloses personal information for a benefit, service or advantage, they 'lose' their small business exemption.

We are concerned by recommendation 68, which suggests amendments to allow disclosures during 'national emergencies'. The Act already allows disclosures necessary to prevent or lessen serious and imminent threats to any person, and agencies such as DFAT and the Australian Federal Police already have exemptions to enable co-ordinated approaches to finding missing persons. Individuals concerned about their family's access to information in case of accident or emergency can already establish mechanisms to deal with such situations, such as a power of attorney. There could be greater education around these mechanisms.

We are therefore not convinced that diminishing privacy protection in times of emergency is warranted, given the corresponding risks of harm to individuals – of identity theft and fraud, and of personal security risks from those people who wish another individual physical harm. In particular, any disclosures should be made to the law enforcement authorities charged with finding a missing person, rather than to family members direct. This would provide greater reassurance for the private sector organisation (such as a bank or airline) than asking them to assess, in the heat of the moment, whether or not a 'family member' is genuine, and whether or not the subject person is even affected by the emergency.

We suggest further options be considered, such as an opt-in register for intending travellers, on which they could nominate a 'next of kin' authorised to receive information in the event they are declared missing during some accident or emergency. Furthermore, better education about the existing exemptions, and greater clarity around the powers of law enforcement authorities to seek information quickly from private sector organisations, should ameliorate the 'BOTPA' phenomenon. ('BOTPA', coined by the former Privacy Commissioner of New Zealand Bruce Slane, refers to a situation in which an organisation refuses to disclose information "because of the Privacy Act", even in circumstances where the Act does not create a barrier to disclosure.)

We support recommendation 70, which is to participate in international discussions about cross-jurisdictional implications of new technologies such as Voice over Internet Protocol. This interest would elevate the dialogue with the EU and APEC regions, and could also open discussions with the United States, which has had its own problems with international data handling.

Conclusion

In many ways, what this report does not say is more telling that what it does say.

Key issues in current privacy debates, such as employee privacy, and the role of mass surveillance and dataveillance, are ignored – a consequence of the restrictive terms of reference for the review. The overly timid language of the recommendations, and the focus on evaluating the Act in terms of its impact on business, instead of its impact on individuals (consumers, employees, other stakeholders) or the 'public interest', also suggest a review that was ideologically hamstrung from the start.

Indeed there is little discussion, and no empirical measurement, to suggest that privacy protection for individuals has actually improved since December 2001.

And finally, there are few recommendations that could bring about genuine and systemic improvements, such as private sector auditing powers for the OFPC or a requirement for independent and published Privacy Impact Assessments of significant projects.

While the comprehensive review of many detailed aspects of the Act's operations are welcome, we are disappointed that this report does not set a unifying or robust 'big picture' agenda for the future direction of privacy protection. The result is that the review report fails to see the forest for the trees.

About the Australian Privacy Foundation

The Australian Privacy Foundation is the leading 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.

Since 1987 the Australian Privacy Foundation has led the defence of the rights of individuals to control their personal information and to be free of excessive intrusions. For further information about us see www.privacy.org.au

Contact Details for the APF and its Board Members are at:
http://www.privacy.org.au/About/Contacts.html