THE FEDERAL PRIVACY COMMISSIONER: PURSUING A SYSTEMIC APPROACH

JUDGE KEVIN O'CONNOR AM*

I INTRODUCTION

Respect for the privacy of the individual is a core value of a democratic society. The right to privacy is the bedrock for the enjoyment of many other human rights, including the right of free speech, the right of free association, the right to vote, the right to found a family and the right to a religion of one's choice. But the individual's right to privacy is often seen as sitting uneasily with the community's collective needs, in particular, with the need to protect its members from harm. Furthermore, privacy is often seen as not capable of sufficiently precise definition to be enforceable as a legal right. These themes have been at the heart of the Australian courts' reluctance to develop a common law tort of breach of privacy. They also play an important role in the general debate in Australia on the value of a charter of human rights, which would include a right to privacy. Thus privacy remains a right unprotected either by tort or as a constitutional human right in Australia.

Australians recognise the importance of privacy to the enjoyment of life. But Australian attempts to uphold privacy through law have tended to be somewhat ad hoc in nature. The focus of the various parliaments – primarily the Commonwealth Parliament – was initially on eavesdropping devices, and has only extended to the protection of personal privacy in relation to the handling of personal information by government agencies, credit providers and (most recently) the private sector more generally. It was in the context of safeguarding personal information that the office of Federal Privacy Commissioner was created in 1989. The creation of the Office of the Federal Privacy Commissioner in Australia is typical of a modern trend, both here and overseas, of creating independent offices (and officers) to oversee and ensure adherence by government agencies and private businesses to fair standards for handling personal information.

The mix of roles that the Federal Privacy Commissioner is called upon to play is unusual if not unique. The Commissioner has the power to issue binding

* President, Administrative Decisions Tribunal of New South Wales; Chairperson, Fair Trading Tribunal of New South Wales; first Federal Privacy Commissioner, 1989-96.

statutory instruments, to issue binding and non-binding guidelines, to make policy submissions to government and parliamentary inquiries, to engage in community education and public comment (necessarily often done through the mass media), and to receive complaints, investigate them and then make final determinations. Thus the Privacy Commissioner's responsibilities fall across all parts of the 'legislative', 'executive' and 'judicial' spectrum (using those terms broadly, rather than in the more technical sense found in the *Australian Constitution*).

Between 1989 and 1996, I was the Federal Privacy Commissioner with that spread of responsibilities. Now, however, I am a State Judge and Tribunal President with a role strictly confined to the 'judicial' end of the spectrum. It is unacceptable for judges to have either legislative or executive responsibilities. The authoritativeness of judicial rulings depends in large part on judges being seen not to be involved in activities that fall within the hurly-burly of public debate or in roles that give rise to conflicts: for example, one cannot be both investigator and judge.

But I would argue nonetheless (perhaps some would say from a position of obvious conflict!), that the office of Federal Privacy Commissioner has functioned well despite – and possibly because of – the mix of functions to which I have referred.

II HANDLING COMPLAINTS AND FORMAL DETERMINATIONS

In the more than 30 overseas jurisdictions where privacy commissioners are found, most of them are substantially involved with 'access-and-amendment' complaints relating to personal records. In Australia, complaints of that kind (relating to personal records held by the government) fall within the framework of the Freedom of Information laws. During my years as Privacy Commissioner, this meant that the only involvement the Commissioner's Office had with access-and-amendment complaints concerned one category of private sector records: consumer credit records, generated and used in the context of obtaining credit history reports.

Because the vast majority of access-and-amendment complaints were siphoned off in this way, the Office of the Federal Privacy Commissioner had a relatively small complaints load (compared with its overseas counterparts). These complaints were principally concerned with improper disclosure, inadequate security and (sometimes) lack of adequate explanation as to proposed uses of information. As a result, the Office had the capacity to focus much of its effort on the systemic practices of agencies (discussed below).

When a complaint was considered by the Office's investigation staff to be well founded, the Commissioner would be advised. As Commissioner, I would appraise the brief from the investigation staff and authorise them to advise the agency concerned of the adverse initial finding and to enter into discussions as to

the resolution of the complaint without formal determination. The complainant would be kept informed of all these steps.

In the time I was Commissioner, only two matters in eight years were subject to formal determination.[1] I have not followed closely how my successors as Privacy Commissioner have used the power to make formal determinations, but I understand that the Office remains 'determinations-averse'. Of course, the existence of the power of determination remains vital to achieving good settlement outcomes. And the content of the power (ie, the range of remedies available) informs and structures the parameters of settlement discussions.

I recognise that a consequence of this 'determinations-averse' approach is the unavailability of traditional case-rulings to guide lawyers, officials and others interested in the operation of the *Privacy Act 1988* (Cth) ('*Privacy Act*') as to how the Act might be applied in specific circumstances. The Commissioner's Office did begin providing case examples in annual reports, and this practice has continued. One solution to providing greater public information may be the publication of an anonymous complaint log, with reasonable detail given in respect of complaints giving rise to settlements.

As Privacy Commissioner, my reticent approach to the use of the power of formal determination had a number of bases. I felt that it was far better to give the agency concerned (be it a government agency, credit reporting agency or credit provider) an opportunity to settle, once an investigation had concluded by reaching a negative or somewhat negative provisional finding. Much depended on the quality of the investigation, the perception that it was properly and impartially conducted, and the persuasiveness of the final report of the investigation. It was then necessary to propose a resolution which was not unrealistic in the eyes of the agency, as well as being acceptable to the complainant.

The 'carrot' from the agency's perspective was (and still is) that resolution at this point avoids the possibility of expensive, formal proceedings before the Commissioner, and minimises the risk of any adverse publicity flowing from the matter – a significant consideration for organisations operating in a competitive marketplace, and a not inconsequential consideration for government agencies operating in a political and mass media environment where 'privacy intrusion by government' is always a topical issue.

From the point of view of the individual complainant, I do not recall any concerns being expressed by individuals in cases where a provisional finding

---

1 Both of which were issued in 1993. The first concerned a complaint against a Minister, from a prominent Opposition Member of Parliament ('MP'), in respect of alleged disclosure – in contravention of the *Privacy Act* – of information about the Opposition MP connected with an application they had made to the Minister's Department in respect of a travel expense claim. The information contained in the claim had found its way into a press report. While the ultimate publication pointed towards a contravention of the Information Privacy Principles (as set out in the *Privacy Act*), I found that there was insufficient evidence for me to identify the source of the disclosure. In the second case, the agency involved conceded that there had been a wrongful disclosure of information relating to discharge from employment, but stated that it was unable to settle the matter for the proposed amount, which it saw as reasonable, because of restrictions on its Finance delegation. However, this problem could be overcome if there was a formal determination, so a reasoned public determination was issued.

showed that the complaint was sustained but which was then followed by a settlement. My recollection is that all were happy with the settlements achieved, usually involving such steps on the agency's behalf as an apology and an agreement to change administrative practice. Sometimes financial compensation was also paid (although that was relatively unusual), which was intended to compensate for any actual losses flowing from the agency's breach, as well as including a component to compensate for emotional distress.

III A SYSTEMIC APPROACH

While I was Commissioner (and from what I can discern this practice has continued), the Office of the Privacy Commissioner was focused on and expended a lot of effort on providing systemic advice to agencies and maintaining a continuous, routine audit program. For example, the Office organised all the ad hoc advice given to credit agencies into a detailed series of Advice Notes on how to comply with the privacy and credit reporting rules in typical business circumstances.[2] Similarly, after lengthy consultation, the Office published 'Plain English' guides to compliance with the Information Privacy Principles, drawing on both the Office's and various agencies' experience of problem situations. These publications provided guidelines on good practice which would avoid privacy infringements and reflect the values of the *Privacy Act*. The Office also published binding rules that had the status of subordinate legislation in areas such as use of tax file number information, data-matching and separation of Medicare and Pharmaceutical Benefits data.

It will be evident from these comments that, as Commissioner, I strongly favoured an approach that was proactive and systemic in its orientation, rather than one that was reactive and case-specific. I was influenced in this approach by several factors. Agencies were more likely to resist embracing privacy values if they were unduly castigated over relatively narrow complaints, provided of course that the failure did not suggest any pattern of non-compliance. Privacy laws are not easily assimilated into agency cultures, especially agencies with significant revenue or criminal law enforcement functions. Operational secrecy is often critical to the performance of their functions, and for that reason these agencies will sometimes claim to understand and respect 'privacy' values. But operational secrecy is a different concern from that reflected in modern information privacy laws, with their highly detailed inter- and intra-agency information flow restrictions, and their conferral of positive rights on individuals to know how information will be used and to seek access and amendment rights in relation to that information.[3] Because of their complexity, it is far better in my

2 The rules commenced operation in 1992.

3 For example, the Department of Social Security (now Centrelink in this regard) has to ensure that payments are made to the right people based on correct information and in the correct amount. It relies on information given directly by the applicant and may move to cut off payment if other sources of information question the assumptions upon which the agency is making payments. But the desire to act

view to tackle these issues through systemic interventions than to hope that guidance will be found in one-off rulings.

Another factor leading to reluctance on my part to engage too much in formal determinations flowed from the 'fuzzy law' nature of the Information Privacy Principles in the *Privacy Act*. A core statement of general principles is characteristic of all modern information privacy regimes, here and overseas. Their structure and much of their text can be traced to three principal sources: the 1980 Organisation for Economic Co-operation and Development *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*; the 1981 European *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data*[4] (now subsumed by the 1995 European Union Directive on the protection of personal data and on the free movement of such data);[5] and the United States ('US') federal information laws – the *Freedom of Information Act*[6] and the *Privacy Act of 1974*.[7]

These statements of principle, to which legal consequences are attached, often use language of great generality, for example: collection must not only be 'lawful' but 'fair'; use of personal information by an organisation must be 'relevant' to the 'purpose' of collection. There is wide scope for argument as to how standards expressed in such terms apply in practice. Of course, this phenomenon is not unique to this area of the law.[8]

Regrettably, regulators in Australia do not have the benefit of the American doctrine of 'regulatory deference'.[9] Under this doctrine, US courts will not lightly intercede in relation to the interpretations and standards that issue from a regulatory body (regarding the law it is called on to enforce) in situations where there is ambiguity or a range of reasonable interpretations available.

I think it is unfortunate that there is no equivalent doctrine in Australia. Because of the 'fuzzy law' character of the Information Privacy Principles there is a high chance of differences in interpretation over their meaning. As Commissioner, it seemed to me that there was always a reasonable prospect of

---

quickly to limit damage to revenue has to be balanced against the right of the citizen to fair decision-making and fair and accurate use of personal information.

4 Opened for signature 28 January 1981, ETS No 108 (entered into force 1 October 1985).

5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

6 5 USCS s 552 (1966).

7 5 USCS s 552a (1974).

8 The application of standards of this kind, which involve categories of indeterminate reference, 'must include a decision as to what justice requires in the context of the instant case': Julius Stone, *The Province and Function of the Law* (1946) 186. However, in the context of privacy law, I tend to the view that the use of broad statements of principle is probably unavoidable, and in fact such general principles have an important educative role to play as they state simply and in clear terms the values that are being protected.

9 See *Chevron USA Inc v Natural Resources Defense Council Inc*, 467 US 837, 843-4 (1984). For a recent summary, see *Southern California Edison Co and Los Angeles Dept of Water and Power v United States*, 226 F3d 1349 (Fed Cir, 2000) pt B. See also Mark Aronson and Bruce Dyer, *Judicial Review of Administrative Action* (2nd ed, 2000) 156-75. The *Chevron* doctrine has recently been described as 'clearly anathema' to the High Court: Mark Aronson, 'The Resurgence of Jurisdictional Facts' (2001) 12 *Public Law Review* 17, 20, referring to *Corporation of City of Enfield v Development Assessment Commission* (2000) 199 CLR 135, 151-4, 158. See also Stone, above n 8, 198, where he comments on what he saw at that time as the 'deep rooted common law tradition of judicial hostility to legislation'.

Federal Court over-rule, with the result that the authority of the Privacy Commissioner and the Commissioner's Office might be diminished in the process – an outcome which is minimised under the US approach.

IV FUTURE DIRECTIONS

Now that the *Privacy Act* has been generally extended to cover the private sector,[10] the Office of the Federal Privacy Commissioner faces the challenge of fostering fair systems of sector specific dispute resolution. Otherwise there is a risk that the Office will be flooded with complaints, especially of the access-and-amendment type. If the Office were merely to become an access-and-amendment disputes resolution centre (a situation I felt I had observed in some overseas privacy commissioners' offices), that would detract considerably from its ability to deal with the important social balances to be struck through systemic methods of the kind I have described.

There are mechanisms in the *Privacy Amendment (Private Sector) Act 2000* (Cth) ('the amending Act') that will hopefully prevent the Privacy Commissioner's Office being diverted in the way I fear. The amending Act envisages the possibility of a system of approved privacy codes for industry sectors, which could include their own sector specific adjudication schemes. The Office of the Privacy Commissioner is, I understand, preparing guidelines and other material to inform practice on the part of record-keepers generally. Hopefully many complaints and other compliance issues will be able to be resolved within the industry sector by reference to that material, without the issue ever having to be determined by an external regulator.

Because of the strict approach to the exercise of judicial power reflected in the *Australian Constitution*, the Privacy Commissioner's determinations are not self-enforcing. If an agency fails to comply, the Commissioner must obtain an enforcement order from the Federal Court or the Federal Magistrates Court. A valuable feature of the amending Act is the provision that the Commissioner or the code adjudicator may tender to the court an evidentiary certificate as to the findings of fact in the case which has prima facie force, allowing it to be adopted by the court[11] and thus enabling the court to avoid protracted proceedings. Where it adopts the certificate, the court's role will simply be to decide whether the facts certified give rise, in law, to a breach. But given that the new private sector information privacy principles (known as the National Privacy Principles) also involve 'fuzzy law', I hope that the courts will adopt an approach that involves reasonable deference to the Commissioner's interpretations when determining the meaning to be accorded to the Principles.

My views as to the balance to be struck between the role of the Privacy Commissioner and external courts or tribunals may be seen as standing oddly with the situation I now find myself in as President of the Tribunal in New South

10 Through the *Privacy Amendment (Private Sector) Act 2000* (Cth).

11 *Privacy Amendment (Private Sector) Act 2000* (Cth) s 55B, which is yet to commence.

Wales that hears applications for review of decisions of the State Privacy Commissioner. So no doubt an occasion will arise when I shall find myself, an ex-Privacy Commissioner, reviewing a Privacy Commissioner's decision, and facing directly the challenge of actually according reasonable deference to the regulator!

Complex balances must be struck when reconciling the community's need to protect individual privacy with its other needs. The Office of the Privacy Commissioner can play an important part in ensuring this balance is achieved. However, Australia should also seek to develop a sophisticated response to the major privacy issues that fall outside the domain of 'personal information handling', such as the issues raised by the new forms of surveillance technology, genetic testing, and universal numbering systems in the telecommunications industry.

Privacy remains a right struggling for coherent recognition in Australia.