

The Implications of the Privacy Act on Employment

Paul Roth*

Introduction

In relation to employment law, the Privacy Act, which came into force on 1 July 1993, can be usefully characterised as both a human rights statute and a freedom of information statute.

Before proceeding to discuss the Privacy Act under these two broad headings, it will be necessary to grasp the basic conceptual jargon of the Act. The currency of the Privacy Act is "personal information," which is defined in s.2 as "information about an identifiable individual." The term "information" itself is not defined, which appears to be deliberate, as to define a word is to limit it.

For the Privacy Act to apply, the personal information in question must be collected, held, or used by an "agency". The term "agency" is used to denote individuals and organisations in both the public and private sectors that are subject to the requirements of the Act. The few exceptions to the definition of "agency" are listed under s.2; they are entities such as the Sovereign, the House of Representatives, and the courts. This means in practice that virtually every individual and organisation in New Zealand today falls under the definition of "agency".

The "Information Privacy Principles" in s.6 are a set of twelve rules, together with limited exceptions to those rules, that are binding on agencies and around which much of the Privacy Act is structured. These deal with matters relating to access to and the collection, security, correction, accuracy, retention, use and disclosure of personal information, and the assigning of unique identifiers (for example, identification numbers). These 12 principles constitute the basic rules with which we are concerned.

The Privacy Act as human rights legislation

As human rights legislation, the Privacy Act is the direct product of relatively recent developments on the international scene. With rapid advances in information technology and the increased role played by government in the lives of its citizens in the latter half of the twentieth century, international attention has been directed to the formulation of standards in accordance with which the law might strike the right balance between the protection of individuals' privacy and the pursuit of legitimate activities by business and government. This has been reflected by Article 12 of the 1948 Universal Declaration of

Human Rights and Article 17 of the 1966 United Nations Covenant on Civil and Political Rights (ratified by New Zealand in 1978). More recently, and specifically in relation to information privacy, in 1980 the Organisation for Economic Co-operation and Development (OECD) recommended a set of Guidelines Concerning the Protection of Privacy and Transborder Flows of Personal Data, to which New Zealand was also a signatory.

The long title of the Privacy Act states that the general purpose of the Act is "to promote and protect individual privacy" in accordance with these OECD Guidelines. The enactment of the Privacy Act now brings New Zealand in line with a number of other developed nations which have adopted similar legislation, including Sweden, the United States, Canada, the United Kingdom, and Australia.

The interest individuals have in controlling information about themselves and in enjoying freedom from unreasonable intrusion into their personal affairs has long been recognised as raising human rights issues. Such issues are especially relevant to institutional settings such as the employment context. The basis for much of the concern about employees' privacy stems from their inherent powerlessness to assert their privacy interests, and from the traditional disinterest and weakness of the law in compensating for this lack of power in the employment relationship. Job applicants and employees are normally the weaker party in the relationship; therefore, they are not in a position to deny requests by an employment agency or employer that amount to unwarranted intrusions into their personal affairs. While the individual may in law consent to the intrusion, it is only because the relationship is one of unequal power.

The Privacy Act, however, imposes limits on the extent to which an individual's privacy can lawfully be invaded. The Act thus purports to redress the power imbalance somewhat by placing restrictions on the collection, handling, and use of information by agencies such as employers and employment agencies.

One common privacy concern involves information requested from job applicants or employees that is unnecessarily intrusive and seemingly irrelevant to the purpose for which it is being sought. Such information would include, for example, criminal convictions far in the past for offences that are in nature unrelated to the employment concerned; personality test true/false responses to questions such as "I dream frequently of things that are best kept to myself" (asked, unknown to the individual concerned, in order to catch out the subject who is "faking-good"); and medical certificates in cases of absence that are required to disclose with unnecessary specificity the nature of the employee's illness.

Under the Privacy Act, however, the employer or employment agency is not allowed to collect personal information unless the collection of the information is *necessary* for a purpose connected with a function or activity of the agency (Principle 1); the individual must be aware of the fact that the information is being collected, and the purpose for which it is being collected (Principle 3); and it must not be collected by means that are unfair or unreasonably intrusive in the circumstances (Principle 4).

There is a clear relationship here with the Human Rights Act. The Human Rights Act deals with acting on the basis of particular prohibited grounds of discrimination. This *indirectly* discourages the collection of some classes of personal information (such as that relating

* Faculty of Law, University of Otago

to political or religious affiliations and marital or family status). Moreover, s.15 of the Human Rights Act makes it unlawful "to use or circulate any form of application for employment or to make any inquiry of or about any applicant for employment" that suggests that a decision will be made on the basis of a prohibited ground of discrimination. The Privacy Act overlaps with such provisions since it applies to the collection of *all* information that is either irrelevant to the employment decision to be made or that is unreasonably intrusive.

Another privacy concern arises where an employment agency or prospective employer obtains information from third parties without the knowledge or consent of the prospective employee. This is inevitably the case with "headhunters," who would be working largely behind the scene. However, even in cases where interest has been registered in seeking employment, the agency may contact third parties formally or informally to seek verification of details provided by the applicant, and perhaps additional information. Personal information might also be sought through other channels as well, such as the police, business connections, and friends. In a country the size of New Zealand, the use of informal channels of information is bound to be great. The practice of blacklisting suspected "trouble-making" employees is occasionally cited, but it is difficult to confirm whether, and if so, to what extent this practice exists. According to Privacy Principle 2, however, an agency can only collect personal information "directly from the individual concerned" unless the collection can be brought under the exceptions listed.

At the end of the application and vetting process, the employer or employment agency is bound to have quite a lot of information about both the successful and unsuccessful applicants. There are concerns about preserving the confidentiality and preventing the misuse of such material. The same concerns apply to information held about an employee during and after the employment relationship. Personnel records commonly contain a great deal of information about employees, such as bank account numbers for direct deposit payments, wages and time records, PAYE records, IRD numbers, home addresses, marital status, accident and health information (which may include details about current health status and the presence of disease, disability, or addiction), disciplinary records, performance appraisals, references, and *curricula vitae* (which in turn include details concerning work history, education, and other personal information). There are concerns that personal information may be disclosed without authorisation to third parties, such as other employers, debt collectors, private investigators, credit bureaux, banks, and insurance companies. The Privacy Act requires that personal information be protected against unauthorised access, use, disclosure and other misuse (Principle 5); that personal information should not be kept for longer than necessary (Principle 9); that strict limits be imposed on the use of personal information for purposes other than those for which they were obtained (Principle 10); and that strict limits be imposed on the disclosure of personal information to third parties (Principle 11).

Another privacy concern involves surveillance of employees. Electronic surveillance has become an increasingly accessible option for most employers. It may be used for security reasons, such as the detection of pilfering, or for monitoring job performance. Monitoring telephone use is a particularly common practice, especially by means of logging systems that are able to record the time, duration, destination, and cost of telephone calls. Principle 3 requires an agency to:

... take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of

- (a) The fact that the information is being collected; and
- (b) The purpose for which the information is being collected . . .

One exception to this Principle is where the agency believes, on reasonable grounds, "That compliance would prejudice the purposes of the collection" (para.(4)(d)). Accordingly, surveillance and monitoring without the individual's knowledge appear to be permissible if it is *necessary* for a lawful purpose connected with the agency's function or activity (Principle 1) and if the means, in the circumstances of the case, are not unfair or do not intrude to an unreasonable extent upon the personal affairs of the individual concerned (Principle 4). If the collection or use of personal information is made in breach of this or another of the Information Privacy Principles, and the information is relied upon for a decision to dismiss or discipline an employee, this in itself may constitute procedural unfairness.¹

Like the Human Rights Act, the Privacy Act is very much aimed at behaviour modification. The Information Privacy Principles establish norms of conduct for agencies in relation to their collection, handling, and use of personal information. Compliance with these principles is assisted by the rights granted to individuals to have access to information about themselves and to seek correction of it. The Privacy Act's complaints procedures place emphasis upon conciliation and the reaching of voluntary settlements. In the last resort, unresolved complaints under the Privacy Act, like those under the Human Rights Act, are determined by the Complaints Review Tribunal.

The Privacy Act as freedom of information legislation

It is important to appreciate the relationship between the Privacy Act and New Zealand's two other freedom of information statutes, the Official Information Act 1982 ("the OIA") and the Local Government Official Information and Meetings Act 1987 ("the LGOIMA"). There are significant interconnections among the three statutes in subject matter, jurisprudence, and administration. In short, the three enactments must be viewed as complementary components of the same overall statutory scheme.

Information Privacy Principles 6 and 7 give individuals rights of access to and correction of information about themselves. In terms of subject matter, therefore, the Privacy Act has taken over an important aspect of the official information regime through its coverage of all personal information held by public sector agencies relating to natural, as opposed to corporate, persons. The effect of the new legislation has been largely to remove the application of the OIA and LGOIMA to natural persons and transfer their coverage to the Privacy Act, the scope of which extends beyond the public sector to cover private sector agencies as well.

¹ Cf. *Graham v Christchurch Polytechnic*, unreported, CEC 48/93, 14/9/93, Palmer J., p.25.

In its role as a freedom of information statute, therefore, the Privacy Act has particularly significant implications for employment law. This is because it enables private sector employees to enjoy the same rights of access to and correction of personal information held by their employer as were enjoyed previously only by public sector employees under the freedom of information legislation. Moreover, these rights of access and correction extend to personal information held by *all* agencies that are subject to the Act. Thus, both private and public sector employees now also have access to personal information held by such agencies as employment agencies, trade unions, professional and trade associations, and those in a client or contractor relationship with the employer.

These new rights of access mean that employees who have been dismissed, disciplined, or otherwise disadvantaged are *prima facie* entitled to access to all information held about them by their employer or former employer. This would include diary notes, communications with industrial consultants that are not protected by legal professional privilege, internal memoranda, and in fact anything that is about the individual concerned. Access to such information is likely to be helpful in deciding whether or not to pursue a personal grievance. Moreover, if one is pursued, the right to access enables an applicant to gather evidence without the pleadings in the case having to be filed first in order to seek an order for discovery. In addition, an individual should be entitled to obtain a copy or written record of his or her individual employment contract *after* the employment relationship has ended, a right not presently conferred under s.19 of the Employment Contracts Act. Other types of personal information, such as performance appraisals, management comments about individuals, and details of personnel decisions concerning individuals should all normally be accessible under the Act by the employee concerned, whether the motive behind the request is contemplated litigation or mere curiosity.

By virtue of the Privacy Act's savings provision (s.7), an employer would be justified in refusing to generate a statement of reasons for an employee's dismissal if requested to do so outside the 60 day period specified by s.38 of the Employment Contracts Act. However, the savings provision will not affect an employee's entitlement to disclosure of *existing* material held by the employer relating to the reasons for the dismissal, or the generation of a statement by the employer in relation to any matter other than the reasons for the dismissal (such as the reasons behind a final warning).

The Privacy Act gives individuals access to personal information about themselves regardless of whether that information was obtained before or after 1 July 1993 (s.8(2)). As was the position under the OIA and the LGOIMA, personal information held by public sector agencies is available free of charge (s.35(1)). Private sector agencies are permitted to require a payment for making information available, partly in order to discourage excessive or vexatious requests. Any such charge, however, must be a reasonable one (s.35(5)). An agency has up to 20 working days for deciding whether or not to grant a request for information (s.40(1)); provision is made for extension of this time limit in certain circumstances (s.41). The information itself must be made available without "undue delay," or else this is deemed to be a refusal to make the information available (s.66(4)). Where information is refused, the agency must give its reasons and inform the requester of the right to seek an investigation and review of the refusal by the Privacy Commissioner (s.44).

As a corollary to the right of access under Principle 6, individuals also have the right to seek correction of their personal information (Principle 7). This right is connected with the duty of agencies to ensure that personal information is accurate (Principle 8). The right to seek correction of information that may be misleading or inaccurate is a valuable one, for inaccurate information may be relied upon, for example, in order to prepare a reference, obtain a loan, or for purposes relating to superannuation or health insurance. Moreover, an employee's records may include a supervisor's comments in relation to competency, conduct, or matters such as suspected substance abuse, which in fairness (and therefore in accordance with good industrial practice) ought to be brought to the employee's notice before being acted upon, so that the employee can have an opportunity to put his or her side of the story.

Because the Privacy Act deals with the same conceptual currency as the OIA and the LGOIMA, its jurisprudence will inevitably draw to a great extent on the existing jurisprudence of those earlier freedom of information statutes. Many of the relevant provisions of the Privacy Act are cast in identical terms, and it is to be expected that the very great guidance given over the years by the Ombudsmen in the interpretation of terms and the application of concepts in those earlier enactments will be followed by the Privacy Commissioner. Such, at any rate, is arguably the implied intention of Parliament in modeling many of the Privacy Act's provisions on those of the earlier freedom of information statutes.

For example, the various acceptable grounds that justify an agency in refusing disclosure of personal information to the individual concerned are all drawn from the OIA and the LGOIMA. There is therefore a ready-made jurisprudence dealing with this very important aspect of the Privacy Act. Chief among these good reasons for refusing access to personal information is subs.29(1)(b), which applies if:

- The disclosure of the information or of information identifying the person who supplied it, being evaluative material, would breach an express or implied promise --
- (i) Which was made to the person who supplied the information; and
 - (ii) Which was to the effect that the information or the identity of the person who supplied it or both would be held in confidence.

On its face, this provision might be thought to protect material such as performance appraisals, interview notes and reports, and references from disclosure to the individuals to whom they relate. However, s.29(1) is framed as making provision for a series of *permissive* reasons for refusing disclosure ("An agency *may* refuse to disclose any information requested pursuant to principle 6 if --"). Accordingly, the Ombudsmen have long held that this discretion should be exercised in a fair and reasonable way.² Moreover, if the supplier of the evaluative material is another employee or a contractor engaged by the employer, it is unlikely that there would be an implied promise of confidentiality, and if there is an express promise of confidentiality, it may not be reasonable to invoke it as a good reason for withholding the information, since in both cases the information is supplied not *in reliance on* any promise of confidentiality (whether implied or express), but

² Cf. Case No. 129 (1985) 6 CCNO 98, at 100 (G.R. Laking); (1993) 10 *Compendium of Case Notes of the Ombudsmen*, vol.2, p.110.

in the performance of one's duties; as the Ombudsman has put it, "the promise must be operative in inducing the supply of information".³ Such would clearly be the case, however, where there is the gratuitous supply of a job reference, since the promise of confidentiality can easily be implied. Moreover, without such an understanding, the supply of such information would be prejudiced, making reliance on subs.29(1)(b) in this instance reasonable.

The two other freedom of information statutes impinge on the Privacy Act in other significant ways as well:

1. Access to personal information comprised in evaluative material may be less problematic if it is held by a public sector agency, because under s.23 of the OIA and s.22 of the LGOIMA individuals are entitled as of right to be informed about the essential contents of such material if it has been relied upon in making a decision about the individual concerned. The Ombudsman has commented in this regard that:

Once relied on, the evaluative material would have become part of the decision-maker's "findings on material issues of fact" and "reasons for the decision and recommendation."⁴
2. Information Privacy Principle 6 deals only with access to personal information that is held "in such a way that it can readily be retrieved." Where such information is not readily retrievable and held by a public sector agency, it will be official information that may be sought under Parts II of the OIA and the LGOIMA.
3. In respect to personal information held by public sector agencies, the OIA and the LGOIMA will extend the otherwise strict limits imposed by Information Privacy Principle 11 governing the disclosure of personal information to third parties. This is because the disclosure of such information will also be governed by subs.9(1) and 9(2)(a) of the OIA (cf. subs.7(1) and 7(2)(a) of the LGOIMA). This means that the limits on disclosure of such information will be more flexible than those applying to information held by private sector agencies. Whereas information held by the latter "shall not be disclosed" to third parties unless it falls under one of the permitted categories listed in Principle 11, personal information held by public sector agencies is subject to a two stage test under which countervailing public interests favouring disclosure (such as individual justice) must be considered.
4. There are a number of areas where the Ombudsmen and the Privacy Commissioner will have overlapping jurisdictions and duties of consultation with each other (see ss.72, 117, and s.29B of the OIA and s.29A of the LGOIMA).

³ Case No 157, (1986) 7 CCNO 141, at p.146 (L. J. Castle); cf. *Re Low and Department of Defence* (1983-84) 6 ALD 280; (1984) 2 AAR 142 (Cth AAT); *Smith Kline & French Laboratories (Aust) Ltd v Department of Community Services and Health* (1991) 28 FCR 291, at pp.302f. (F.C.).

⁴ 10 CCNO vol. 2, p. 111; cf. Case No. A 255 (N. Tollemache) and Case No. W2834 (J. Robertson).

To sum up, the Privacy Act is highly relevant to the employment context. In particular, it is likely to prove a useful tool for employees and their advocates who know how to make use of it, and a source of potential pitfalls for those employers who are unaware of its provisions.