THE IMPACT OF PRIVACY LEGISLATION ON THE WORKPLACE: THE NEW ZEALAND EXPERIENCE

Paul Roth

Faculty of Law
University of Otago

Abstract

This paper describes how New Zealand's Privacy Act applies in practice to the workplace, and what its effect has been in relation to the protection of workers' privacy interests. While there are a few areas where the legislation is effective, it has been largely a disappointment for workers, who are increasingly subject to privacy-intrusive practices in the workplace.

Individuals' interests have always tended to be overridden in institutional and contractual settings where individuals lack bargaining power. The main argument of this paper is that New Zealand's Privacy Act, now in force for over eleven years, has hardly affected the balance of power in relation to workplace privacy matters. The irony is that those who are best placed to take advantage of the legislation in the employment setting are unsuccessful job applicants and dismissed employees; ie those who are not actually in a subsisting employment relationship. Despite the existence of privacy legislation, it is employment law that remains of paramount importance for the protection of workers' privacy interests.

The New Zealand experience suggests that effective workplace privacy protection can only be attained through specific sectoral regulation that overrides managerial prerogative and the ability of workers to contract out or their rights.

Introduction

Privacy interests raise important and often difficult issues in the workplace. As might be expected in an institutional setting, the individual as job applicant or employee tends to be in a position of relative weakness in relation to an employer who wants to acquire or use information. While individuals may in law consent to intrusions into their personal sphere, it is usually because refusal is not an option. In these times when the success of a growing service industry sector and the exaltation of professionalism rests on a foundation of public image,[1] and technological developments have opened up new possibilities in the way we work and the ways in which workers can be monitored both on and off the job, the importance of regulating employer control over the conduct and private lives of workers has never been greater.

Privacy legislation covering both the public and private sectors has now been in force in New Zealand for just over a decade. The aim of this paper is to describe how New Zealand's Privacy Act 1993 applies in practice to the workplace, and what its strengths and weaknesses have been in respect to protecting the privacy interests of workers. While there are a few areas where the legislation is effective, it has been largely a disappointment for workers, who are increasingly subjected to privacy-intrusive practices in the workplace as in other spheres of their daily lives.

Individuals' interests have always tended to be overridden in institutional and contractual settings where the parties are not positioned on a level playing field. The main argument in this paper is that New Zealand's Privacy Act has hardly affected the balance of power in relation to workplace privacy matters. The irony is that those who are best placed to take advantage of the legislation in the employment setting are unsuccessful job applicants and dismissed employees -- that is, people who are not actually in a subsisting employment relationship at all. Moreover, despite the existence of privacy legislation, it is employment law that remains of paramount importance for the protection of workers' privacy interests. The New Zealand experience suggests that effective workplace privacy protection can be attained only through specific sectoral legislation that overrides managerial prerogative and the ability of workers to contract out of their rights.

The Privacy Act 1993

The centerpiece of the Privacy Act is the set of information privacy principles in s 6 that govern the collection, holding and use of personal information. In relation to the employment setting, they may be summarised as follows:

- personal information can only be collected if it is necessary to do so for a function or activity of an agency (principle 1);
- personal information should normally be collected directly from the individual concerned unless otherwise authorised (principle 2);

- where information is collected directly from individuals, they should be made aware that it is being collected and for what purpose, and who will hold or receive it (principle 3);

- personal information should be collected by lawful means and not in an unfair or unreasonably intrusive manner (principle 4);

- personal information should be protected by adequate security measures (principle 5);

- individuals have rights of access to and correction of their personal information (principles 6 and 7);

- agencies should not use personal information unless it has been checked for accuracy and relevance in relation to its intended purpose (principle 8);

- agencies should not retain personal information for longer than they may lawfully use it (principle 9);

- agencies must not use or disclose personal information for any purpose other than that for which it was collected unless authorised (principles 10 and 11);

Some of the principles that might be expected to be important for privacy protection in the workplace allow for derogations, so that, for example, individuals can waive their application (principles 2, 3, 10, and 11). The benefit of protection by the other principles cannot by waived or contracted out of by individuals. Therefore, it is these non-derogable principles that should have the strongest effect in the workplace and other settings where the individual proceeds from a position of relative weakness. The principles, however, are framed somewhat loosely, and are subject to many exceptions.

An important feature of the legislation is that a breach of a principle on its own does not generally lead to liability. Except in the case of denied access or correction rights, the breach of a privacy principle must be accompanied by some loss or harm, and in the case of emotional harm, there must be "significant humiliation, significant loss of dignity, or significant injury to feelings" (s 66(1)(b)(iii)). This functions as the main sifting mechanism of the legislation, to filter out complaints of a minor nature.

The Privacy Commissioner oversees compliance with the Act and plays an important role in investigating and conciliating complaints. The Privacy Commissioner's views, however, are not legally binding.[2] Only the Human Rights Review Tribunal can determine legal issues at first instance, but it cannot do so unless the Privacy Commissioner has first dealt with the complaint. If a complaint has not been resolved by the Privacy Commissioner, it can be taken to the Human Rights Review Tribunal by the Director of Human Rights Proceedings if it is appropriate to do so, or else by the aggrieved individual.

Collection of personal information

Pre-employment inquiries

Without some legal protection, job applicants are ordinarily not in a position to refuse to disclose information requested by an employer or employment agency. Most jurisdictions now provide remedies for discriminatory hiring practices in their human rights legislation, and New Zealand is no different in that respect.[3]

The Privacy Act provides limited protection in relation to pre-employment inquiries. Principle 1 ("Purpose of collection of personal information") is non-derogable and requires that a collection of personal information must be for a lawful purpose connected with a function or activity of the agency, and that the collection is necessary for that purpose. Since collecting information for the purposes of discrimination is unlawful, principle 1 supplements existing human rights protections in that regard.

For example, in the employment law case of *Attwood v Imperial Industries*,[4] the Employment Relations Authority found that an employer's pre-employment form was drawn too widely and therefore was likely to have breached principle 1. The employee had been dismissed because she allegedly misrepresented her medical condition on the form when she applied for a sales position. The Authority, however, determined that the applicant's failure to refer to two pre-existing medical conditions on the form did not amount to misrepresentation because the employer was not entitled to collect this information in the first place because of principle 1 of the Privacy Act. The scope of the information that was sought went beyond what was relevant to the employer's compliance with its health and safety obligations or the employee's ability to do the job. The Authority's determination was upheld on appeal to the Employment Court.[5]

Employers have a great thirst for information that is not necessarily caught by discrimination law. Whether or not the collection of particular information is "necessary" in terms of principle 1 in the employment context has in practice involved an assessment of its reasonableness, and due allowance has been made here, as elsewhere in employment matters, for the exercise of managerial prerogative. The views of the Privacy Commissioner on a number of complaints indicate that non-derogable or not, the "necessary to collect" test in principle 1 involves a low threshold that is not difficult for an employer to satisfy.

In *Case No 2418*,[6] the Privacy Commissioner found that personality testing of job applicants was permissible under the Privacy Act. The complainant had applied for a sales position and was asked to complete a form containing 200 questions. She claimed that the questions were too personal considering the nature of the position sought. The Privacy Commissioner found that in terms of principle 1, the collection of information about a prospective employee's personality and attitudes was a lawful purpose connected with the employer's function.

He noted that other agencies used such tests, and that "the use of such extensive questions could probably be justified only in the context of obtaining the information as part of a comprehensive personality test to assess aptitude for a particular position." On the facts of the case, the Privacy Commissioner was unable to find that the test was unnecessary or that the information collected was excessive.

The Privacy Commissioner did not address the intrusiveness of the test or its relevance to the particular position sought by the applicant. The employer, however, ought to have borne the burden of proving that the test was indeed "necessary". This case illustrates that the Privacy Act tends to be ineffective in substantively limiting the amount and extent of information collected.

The Privacy Act is more strict, however, in relation to job references. This is because of the procedural obligations it imposes on both the collection and provision of this kind of personal information. Since the prospective employee who requests the reference is collecting personal information, the principles relating to collection apply. In particular, the prospective employer must ensure that the collection of information from the referee has been authorised by the subject of the reference (principle 2). Conversely, the person who supplies the reference must also have the subject's authorisation to disclose personal information (principle 11).

Covert recording

In New Zealand, there are few legal controls on surreptitious video or audio recording in the workplace -- or elsewhere for that matter. There is a prohibition against the carrying out of surveillance by private investigators without the subject's written consent,[7] and a prohibition against the surreptitious use of video cameras that also have audio recording capabilities.[8] Although the Privacy Commissioner has long assumed that surreptitious recording is covered under the Privacy Act,[9] this view is arguably mistaken.

The Privacy Act does not limit the use of surveillance cameras or surreptitious audio recording because information obtained thereby is not actually "collected" in terms of the Act. The term "collect" in the Privacy Act is defined in s 2 as excluding the "receipt of unsolicited information". Information obtained through surveillance or other forms of surreptitious recording is not solicited from the subject. Video cameras, for example, are focused on particular physical areas and capture on film whatever takes place within that space. Since what is captured is unsolicited, it is not "collected" in terms of the Privacy Act. Therefore, the various requirements and limitations relating to the collection of information that serve to promote individual autonomy cannot apply to surveillance techniques.

Indeed, the Court of Appeal took this approach to the concept of "collecting" in *Harder v Proceedings Commissioner*,[10] which dealt with surreptitious audio recording. In that case, a woman rang her former partner's lawyer to discuss the settlement of a dispute. The lawyer recorded what the woman told him. The Tribunal that heard the woman's complaint at first instance found that the lawyer was collecting information in terms of the Privacy Act from the moment he switched on the tape recorder. The Court of Appeal disagreed, finding that the information volunteered by the woman was not "collected" in terms of the Act. From the lawyer's point of view, the information disclosed by the woman was unsolicited, and so in terms of Privacy Act, the lawyer was merely in "receipt of unsolicited information". The Court of Appeal majority remarked that "The unsolicited nature of the information was not affected by the fact that it was recorded or the way it was recorded.

The omission of specific coverage for surveillance activities is consistent with the limited scope originally contemplated for the legislation, as indicated by the debates in the House of Representatives. The chairman of the subcommittee considering the original Bill remarked to the House that the legislation was not intended to cover the entire area, and stated that "snooping or prying into people's private affairs, whether by electronic eavesdropping or by entry on to private property by telephoto lenses or other technological devices probably at some time would need further consideration by the House."[11]

Although the Privacy Act principles that relate to the collection of personal information do not apply to surreptitious recording, the principles relating to the holding, use, and disclosure of personal information thereby obtained (principles 5 – 11) will still apply. However, it is the actual collection of such information -- the fact that it is done and the manner in which it is done -- that raises the greatest privacy objections.

Even if surreptitious surveillance were covered under the Privacy Act, the legislation would be of little avail in the workplace, to judge by the one reported case on workplace surveillance where the Privacy Commissioner found it to be a permissible practice.[12] The case dealt with an employee's complaint about the surveillance of a work changing room in order to detect theft. The Privacy Commissioner found that the employer was not obliged to take reasonable steps to ensure, in accordance with principle 3, that the employee was aware that the surveillance was being undertaken. This was on the basis of a number of exceptions to that principle that illustrate its ineffectiveness for imposing any kind of control over surveillance activities. The Privacy Commissioner found that:

- "it was not reasonably practicable to draw the fact of filming to the complainant's attention as the video surveillance was intended to film covert and unlawful behaviour" (principle 3(4)(e));

    (1) "it would have prejudiced the purpose of collection if the complainant had been told that he was being filmed prior to the surveillance taking place" (principle 3(4)(d));

- "non-compliance with Principle 3 was necessary to gain sufficient evidence of theft to enable prosecution of an offender before a Court" (principle 3(4)(c)(iv)).

Moreover, the Privacy Commissioner found that the way the information was collected did not breach principle 4 ("Manner of collection of personal information") because:

- "the use of the video camera to collect information was lawful;

- the agency had taken steps to minimise the extent of surveillance;

- the locker room was not a private space intended for the removal of clothing;

- in the videotape viewed the complainant had only been recorded removing his outer clothing therefore this limited amount of filming without the use of sound was not an 'unreasonable' intrusion upon the complainant's personal affairs; and

- given the need to identify the source of the stolen property and that the video camera was used solely for this purpose the covert surveillance was not unfair."

In contrast to the lack of provision in the Privacy Act for any meaningful controls over surveillance activities, employment law provides for standards of due process that regulate how the employer ought to conduct itself once adverse information obtained though surveillance is proposed to be used.[13]

Employee bag and vehicle checks

The Privacy Commissioner's handling of a union complaint concerning bag and vehicle checks illustrates that the privacy principles have a minimal, but still some effect, on such practices.[14] The union complained that the checks were inconsistent with the relevant employment contract, which provided that company personnel "shall not search cars, lockers, bags or any other items belonging to an employee without his/her consent and in his/her presence." The inspection policy provided that all individuals entering or leaving the site were invited to allow a security guard to inspect bags and vehicles. The security guard was only permitted to view the contents, not rifle through belongings. Where there was good reason to suspect that a person had company property, the vehicle or bag would be searched. The search would only take place if the individual consented, in accordance with the employment contract.

The company explained that its policy complied with health and safety legislation, and that there was a need to maintain security. These concerns were based on a bomb threat that involved an evacuation of the workplace and the consequent loss in production. The employer was advised by the police to improve its security measures. There were also concerns about drug and alcohol use where heavy machinery was being operated; weapons being brought into the workplace; and thefts of company property over a number of years.

The Privacy Commissioner's investigation indicated that there were no longer any serious threats to the safety of those at the workplace. Accordingly, the company decided that inspections of people entering the site would no longer take place. The Privacy Commissioner found, however, that the inspection of workers leaving the site was necessary in terms of principle 1 to ensure the security of company and staff property. Nevertheless, the Privacy Commissioner formed the view that the searching of handbags raised concerns about the manner in which information was being collected (principle 4). If the company was particularly concerned about the theft of large and expensive items, such as laptops, it was not acceptable that handbags should be searched if such items could not fit in them. Otherwise, the Privacy Commissioner found the practice acceptable, as the company had notified the policy to staff and explained why it was implementing it, as well as the consequences of non-compliance. The company regarded the search process as voluntary, with individuals having the option of leaving bags and cars outside the site if they did not want to be searched.

Monitoring of e-mail and internet use

There are several New Zealand employment law cases dealing with employees who have been dismissed for inappropriate use of internet facilities. The Privacy Act, however, has not played any significant role in these cases.

In the earliest case,[15] an employee was dismissed for allegedly harassing a female fellow staff member. The employer relied, in part, upon the employee's e-mail correspondence with the woman as evidence for his misconduct. The dismissed employee sought an interim injunction to continue work pending the outcome of the case. He contended that the dismissal was improper and contravened the Privacy Act. The Court held that there was "an arguable case for procedural unfairness in this particular context."[16] Subsequent cases, however, have turned not on the Privacy Act at all, but on such factors as employer training and policies regarding internet use,[17] the nature of the use (messages containing sexual innuendoes and surfing the net for pornography being particularly frowned upon),[18] length of service,[19] and rights of free expression during industrial negotiations.[20]

There are no obvious privacy rights per se in respect of employees' e-mail or other internet use, but the justifiability in terms of employment law of any disciplinary action turns on whether the employee had a reasonable expectation of privacy, and the extent to which the employer has set clear bounds. The emphasis is on fairness and due process, rather than any rights stemming from the Privacy Act.

Adding to the irrelevance of the Privacy Act in this context is the technical issue whether an employer who gathers information about an employee's internet use is

actually "collecting" information in terms of the Privacy Act. This is because the employer already holds this information in its computer system. The information will also likely to be "unsolicited" information (and so it falls outside the Act's definition of "collect"). Therefore, the rules relating to individual notification, and the requirement that the retention, use and disclosure of such information must relate to the original purpose for collecting it, do not apply.

Drug and alcohol testing

As a privacy advocate, the Privacy Commissioner has been at the forefront in opposing random drug testing in the workplace.[21] There have been no reported Privacy Act complaints, however, arising from drug or alcohol testing, and it is doubtful whether the Act could be invoked to limit such testing. So long as the testing is for a lawful purpose connected with a function or activity of the employer and is necessary for that purpose (principle 1), and is carried out fairly and does not intrude unreasonably into the individual's personal affairs (principle 2), then testing could not be impugned under the Privacy Act.

The permissibility of drug and alcohol testing therefore turns on employment law rather than on privacy law. Unless specifically provided for in an employment agreement,[22] an employer would be faced with real difficulties if an employee refused to submit to a test, particularly random testing where there is no reasonable cause for conducting it in the first place. The employer cannot physically compel the worker to undergo testing, and could only take disciplinary action if a refusal to be tested was unreasonable in the circumstances. If the employer decides to dismiss the worker, the issue then becomes whether or not the employer was substantively and procedurally justified in doing so. The Privacy Act does not provide any guidance as to what would be fair and reasonable in such circumstances. Like employment law, it simply requires that any collection of personal information be undertaken in a fair and reasonable manner (principle 4). No new substantive rights can emerge from such circularity.

In an interim injunction case where the employee sought reinstatement pending determination of his unjustifiable dismissal case,[23] the Employment Court did not find anything amiss where drug testing was carried out in a procedurally fair manner and in a safety-sensitive context. The Privacy Act was not invoked.

In the recent case *NZ Amalgamated Engineering Printing and Manufacturing Union Inc v Air New Zealand Ltd*,[24] the Employment Court considered the application of both the Privacy Act as well as the New Zealand Bill of Rights Act 1990 to testing. While the issue turned on the application of employment law principles, the Privacy Act was described as "represent[ing] current community standards and expectations in this area." Accordingly, measuring an employer's conduct against the standards set out in the Privacy Act was said to "assist in determining the reasonableness of the proposed drug and alcohol testing."[25]

Use of biometrics

There is one case where the Privacy Commissioner investigated a union complaint about the introduction of finger-scanning technology for an employer's payroll system.[26] The union claimed that a system of time sheets and clock cards was sufficient, and that the introduction of the new system, associated with criminal activity, was "overkill". The company, however, claimed that a scanner had become necessary in terms of principle 1 because of employee dishonesty in completing time sheets. The Privacy Commissioner found that the collection of information through finger-scanning was "necessary" for the company's purposes in the circumstances.

The union also alleged that the use of finger-scanning technology involved an unlawful, unfair, or unreasonably intrusive means of collecting information (principle 4). In particular, the union pointed to the absence of any express or implied term in the employment contract requiring employees to consent to the physical contact involved in having their fingers measured by sensors. The Privacy Commissioner, however, did not find that the proposal breached principle 4, even though he declined to consider the contractual issue. The Privacy Commissioner held that this issue fell squarely within the jurisdiction of the specialist employment law institutions, and remarked that "It would have been quite improper for me to usurp the role of the Court by dealing with the matter." Given that principle 4 requires that agencies not collect personal information "by unlawful means", the refusal to consider whether or not the collection of information in this case was going to be carried out in breach of the employees' contracts amounted to a concession to the employer, who ought to have borne the burden of proof.

Inquiries into employee misbehaviour

Where an employer collects information in connection with the investigation of employee misconduct, much leeway is permitted as to what is "necessary" to collect in such circumstances in terms of principle 1. Thus, the predecessor body to the Human Rights Review Tribunal did not find any fault in a case where it was claimed that the employer was collecting information that was not necessary for the investigation of a sexual harassment allegation against an employee.[27] The information concerned included information about the drinking habits of the employee's father and the employee's sexual preferences and dating habits. The Tribunal found no breach of principle 1 because the employer's inquiry was informal and preliminary in nature. It was intended merely to determine whether the sexual harassment allegation was vexatious or not. The Tribunal commented that "Informal inquires such as these will often elicit information which is irrelevant to the purpose of the inquiry because information will be volunteered which would otherwise not be sought."[28]

The Tribunal found that the collection of personal information about the employee was necessary for the employer's purpose of investigating the allegation of sexual harassment, which the law required the employer

to address. The Tribunal stated that once it was satisfied that a collection of information was necessary for fulfilling this purpose, it could inquire no further into the matter, determining which bits of information should have been received, and which not.

Disclosure of personal information

Employment law is probably just as effective as the Privacy Act, if not more so, in protecting employees' privacy interests against inappropriate disclosures by employers to third parties. In one employment law case,[29] the employee, a homosexual, had been inadvertently "outed" by his employer. The employee successfully proved a sexual harassment grievance against his employer on the basis that others subsequently harassed him as a result of the disclosure. Moreover, the employee also succeeded in establishing his claim for unjustified dismissal on the basis that he had been constructively dismissed: he resigned because he had been placed in a highly vulnerable position by his employer, who then failed to mitigate the effect of the disclosure. In the result, the employee's compensatory award was exceptionally high by New Zealand standards. In another case,[30] the employee was successful in her grievance for unjustifiable disadvantage because her home telephone number was given out in error to creditors of her employer without her consent.

The one reported complaint under the Privacy Act concerning an employer disclosure of employee information was resolved in the employer's favour.[31] The complainant alleged that management started a rumour in the workplace that she was about to leave her employment. The employer acknowledged that a conversation between a manager and a supervisor was overheard, but it was not certain whether or not this was the origin of the rumour. The Privacy Commissioner, however, found that "the nature of the information that was disclosed during this incident was information other staff members were entitled to know." He went on to comment that "Managers need to inform staff members when an employee is leaving as it may have implications for the workload of other staff."

Access to personal information

Under the Privacy Act, employers have an obligation to grant individuals access, upon request, to their own personal information (principle 6), unless one of the "good reasons for withholding" in the Act applies. This has proved to one of the most valuable aspects of the Privacy Act for workers, particularly those who wish to collect information about themselves from a former employer when contemplating legal action for unjustifiable dismissal. This right is quite useful for assessing whether there is sufficient evidence to proceed against one's employer before actually committing oneself to commencing proceedings. Thus, employees can seek access to the employer's diary notes, internal memoranda, performance appraisals, details of personnel decisions, and the like.

The right of access to personal information is subject to a number of "good reasons" for refusing disclosure.[32] However, only two of these "good reasons" are likely to arise in the ordinary employment context: these are where it is necessary to withhold information to protect another person's privacy, and where references obtained under a promise of confidentiality are involved.

Procured access

The right of access to personal information, however, is not without its downside for employees. Prospective employers often require job applicants to exercise their access rights as a condition of being considered for employment. This is called "forced" or "procured" access. It occurs most commonly when an employer requires prospective employees to provide a printout of convictions, sometimes termed a "Police clearance", from the Ministry of Justice. The Teacher Registration Board and the Land Transport Safety Authority, for example, have statutory obligations to obtain this type of information. Many other employers are legitimately concerned with whether a prospective employee has been convicted of a crime involving dishonesty.

Conclusion

The balance between managerial prerogative and workers' privacy interests in New Zealand is largely determined against a backdrop of the usual dynamic of employer superiority. The employer's requirements tend to function as the "default" position, so that it can normally rely on its right within the employment relationship to make its business run effectively and profitably. This right may allow it to do such things as open employee's mail, monitor e-mail communications, and carry out searches of desks, lockers, and bags. The employer will also have the right, based on the employee's duty of fidelity and obedience, to demand accountability for the employee's actions and activities, both on and off the job, where that affects a legitimate interest of the employer. As has been seen, privacy legislation in New Zealand generally tends to reinforce this position. With a few notable exceptions, such privacy rights as do exist are more likely to be enforced through employment law itself than under the Privacy Act.

Where its activities are likely to breach the information privacy principles, the employer may be able to procure the authorisation or acquiescence of the individuals concerned. In practice, therefore, the information privacy principles do not form a very effective bar to privacy intrusions. Experience with the Privacy Act has shown that job applicants who have failed to obtain employment and employees who have been dismissed tend to be the main beneficiaries of the rights conferred under the legislation. It is for this reason that privacy rights in the workplace need to have express protection and be non-derogable if they are to have much potency in the workplace.[33]

This is not to say that the Privacy Act has had little practical impact on employee's workplace privacy interests over the past decade. It appears to have

functioned largely *ad terrorem*, with employers generally being reticent to take bold initiatives that might fall foul of the Privacy Act. The possibility of incurring expense or loss of goodwill through the breach of untested legislation has acted as a powerful deterrent. In truth, however, the legislation's bark is worse than its bite.

Notes

1 See, for example, Ronald McCallum, Employer Controls over Private Life, Sydney, 2002.

2 The Privacy Commissioner can only make binding decisions about an unreasonable charge imposed for access to personal information held by a private sector agency (personal information held by public sector agencies is free of charge): s 78.

3 Part II of the Human Rights Act 1993 deals with acting on the basis of particular prohibited grounds of discrimination. In particular, s 23 of the 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.

4 WA 72/01.

5 *Imperial Enterprises Limited v Attwood* (2003) 7 NZELC 97,009, para 59.

6 August, 1999.

7 Section 52, Private Investigators and Security Guards Act 1974. Private investigators apparently do not breach this provision if they merely instruct employers how to use surveillance equipment, rather than operating the equipment themselves: see Privacy Committee of New South Wales, Invisible Eyes: Report on Video Surveillance in the Workplace, Report No 67 (Sydney, September 1995), para 5.5.

8 Section 216B ("Prohibition on use of listening devices"), Crimes Act 1961.

9 See, for example, "Extract from a letter by the Privacy Commissioner concerning video surveillance ", in Office of the Privacy Commissioner, A Compilation of Materials on the Privacy Act 1993 and the Office of the Privacy Commissioner Februrary 1994-December 1994, (Office of the Privacy Commissioner, vol 2), 252-253; and Case Nos 0632 (August 1994) and 16479 (June 2001) of the Privacy Commissioner's case notes.

10 [2000] 3 NZLR 80; (2000) 6 HRNZ 173.

11 71 New Zealand Parliamentary Debates, 18 March 1993, p 14132.

12 Case No 0632 of the Privacy Commissioner's case notes (August 1994).

13 See *B W Bellis Ltd v Canterbury Hotel, etc, Employees' IUW* [1985] ACJ 956, *Pillay v Rentokil Ltd* [1992] 1 ERNZ 337.

14 Case No 38463 of the Privacy Commissioner's case notes (June 2002).

15 *Graham v Christchurch Polytechnic*, CEC 48/93, Palmer J (Employment Court).

16 Ibid, p 24. The case was eventually settled out of court.

17 *Clarke v Attorney-General* [1997] ERNZ 600 (Employment Court).

18 Ibid, and Allerton and *Offord v Methanex* (NZ) Ltd, WC 23/00, Colgan J (Employment Court).

19 Ibid.

20 *Howe v The Internet Group Ltd* (IHUG), [1999] 1 ERNZ 879 (Employment Court).

21 Bruce Slane, "The Privacy Implications", in Drug Testing. The Sporting Experience: the Employment Possibility, Legal Research Foundation, Auckland, April 1995, pp 89 – 92, and "Critical Privacy Issues for Employers and Employees," Address to IIR's 10th Annual Industrial Relations Conference, 19 March 1996.

22 There has been only one case concerning the legality of testing as required under a contract, but that was on the issue whether a collective agreement providing for unrestricted random testing was "harsh and oppressive" under s 57 of the now-repealed Employment Contracts Act 1991: *Harrison v Tuckers Wool Processors Ltd* [1998] 3 ERNZ 418l [1999] 1 ERNZ 894. That is no longer the legal test under current employment legislation.

23 *Philson v Air NZ Ltd*, AEC 35/96, Colgan J.

24 AC 22/04, 13 April 2004, Full Court.

25 Ibid, para 221.

26 Case Note 33623, February 2003.

27 *Clydesdale v Christchurch Polytechnic*, Decision No 8/2001 (Complaints Review Tribunal).

28 Ibid, para 13.

29 *L v M Ltd* [1994] 1 ERNZ 123 (Employment Court).

30 *Dunlop v Waikato Students Union Incorporated*, AA 72/03 (Employment Relations Authority).

31 Case No 2594, November 1994.

32 These are set out in ss 27, 28, and 29 of Part 4 of the Privacy Act.

33 See, for example, the suggested standards in the Protection of workers' personal data. An ILO code of practice (Geneva, 1997). The code was intended to provide guidance in the development of legislation, regulations, collective agreements, work rules, policies and practical measures in the workplace.