New Zealand Journal of Employment Relations, 41(2): 36-57

Privacy Law Reform in New Zealand: Will it Touch the Workplace?

PAUL ROTH*

Abstract

This paper explores the implications of the introduction of new information-gathering technologies into the workplace. It concludes that, unfortunately, proposed reforms to the Privacy Act 1993 are unlikely to 'step in' to protect workers' rights to privacy. A comparison between privacy complaints in the workplace in New Zealand and Hong Kong demonstrates a regrettably lax approach on the part of New Zealand's privacy regulatory actors and bodies. The issue of workplace surveillance is only going to become more vexed over time, as new emerging technologies develop.

Key words

Privacy Act 1993, labour law, privacy law, Privacy Commissioner, workplace privacy, personal information.

Introduction

The Privacy Act 1993 is currently in the process of being amended in light of some of the Law Commission's recent review recommendations.[1] The short answer to the question posed in the title of this paper is 'probably not'. This would be disappointing, because privacy interests often raise important and difficult issues in the workplace. In particular, the collection of information about workers in relation to their private lives and their on-the-job conduct will continue to be a flashpoint at the employment law / privacy law interface, and this is only likely to increase as technology develops new ways of collecting and analysing such information.

The issue is whether or not the law is ever going to step in to set some firm limits. While there is legal support for business and managerial prerogative, and excitement over new technological developments that can have workplace applications, the fact that workers might have any privacy rights is generally regarded as a subsidiary matter, if it is regarded at all. And yet New Zealand is legally bound to give substance to the right to privacy, as provided for under art 17 of the International Covenant on

* Professor of Law, University of Otago.

[1] The extensive review, which occurred between 2007 and 2011, generated the following papers: *A Conceptual Approach to Privacy* (NZLC MP19, 2007); *Privacy Concepts and Issues, Review of the Law of Privacy, Stage 1* (NZLC SP19, 2008); *Public Registers: Review of the Law of Privacy stage 2* (NZLC R101, 2008); *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, 2009); *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy, Stage 3* (NZLC R113, 2010); *Review of the Privacy Act 1993* (NZLC IP17, 2010); *Review of the Privacy Act 1993: Review of the Law of Privacy, Stage 4* (NZLC R123, 2011).

Civil and Political Rights 1966 (ICCPR):[2]

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks.

While it is true that inroads can be made into some human rights with the individual's consent, such as the right to privacy, agreeing to be an employee does not mean that individuals have completely surrendered the right. Interference with privacy must not be "arbitrary". This means that there must be some reasonable basis for employer inroads into the right, and that the interference itself must be reasonable.[3]

Moreover, while individuals may in law consent to intrusions into their personal sphere, it is usually because refusal is not a practical option. In addition to being bound by the ICCPR, New Zealand also has a Privacy Act:[4]

> …to promote and protect individual privacy in general accordance with the Recommendation of the Council of the Organisation for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines).

The standards set out in this instrument, however, have been implemented in New Zealand law in a way that is highly flexible, and that tends to be balanced more towards the employer's rather than the employee's benefit. This could be due to the value our society places on material or quantifiable, as opposed to intangible, interests, as well as the political influence of business as opposed to human rights proponents.

Some jurisdictions, such as Hong Kong, have set stricter limits than New Zealand on employer intrusions into employee privacy, though each purports to be acting in accordance with international privacy standards. The Hong Kong position may be a case of human rights protections making up for a lack of employment protections. The efficacy of data protection regulation in protecting workers' privacy interests generally tends to depend on the approach of the data protection authorities and legal institutions that apply and interpret the law. Such limits as have been imposed in New

---

[2] 999 UNTS 171 (opened for signature 16 December 1966, entered into force 23 March 1976); ratified by New Zealand on 28 December 1978.

[3] The Human Rights Committee, which is the supervisory body for the ICCPR, has explained that "The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances": *General Comment 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation)* HRI/GEN/1/Rev.9 (Vol I) (adopted 8 April 1988) at [4]. See, for example, *Rojas García v Colombia*, Communication No 687/1996, UN Doc CCPR/C/71D/687/1996 (2001); *M G v Germany*, Communication No 1482/2006, UN Doc CCPR/C/93/D/1482/2006 (2008); *Nystrom, Nystrom and Turner v Australia*, Communication No 1557/2007, UN Doc CCPR/C/102/D/1557/2007 (2011); *Naidenova et al. v Bulgaria*, Communication No 2073/2011, UN Doc CCPR/C/106/D/2073/2011 (2012). One commentator notes that "regardless of its lawfulness, arbitrary interference contains elements of injustice, unpredictability and unreasonableness": Manfred Nowak *UN Covenant on Civil and Political Rights: CCPR Commentary* (2nd rev ed, Engel, Kehl am Rhein, 2005) at 383.

[4] Privacy Act 1993, long title.

Zealand mainly seem to have been set by the specialist employment law institutions rather than through privacy law.

There are arguably two factors that account for a lack of active protection for workers in the privacy context. Firstly, there is the nature of the relationship, which is viewed as consensual rather than one where there is a power imbalance between the parties that needs no more in the way of adjustment than guarantees of minimal employment law rights, as opposed to civil rights. Secondly, the Privacy Commissioner has fallen into a legitimising role in relation to new technologies, facilitated by the lack of any real power to exert control over new and intrusive practices. This characteristic is not unique to New Zealand officials, but is common among privacy commissioners elsewhere who have been left to advise from the sidelines. The New Zealand approach will be compared here to that in Hong Kong, where the law is similarly based on the OECD Guidelines, but standards appear to have been upheld more strongly in the face of employer initiatives to employ new technologies to collect worker information.

Overview of the Privacy Act in Relation to Employment

Privacy legislation covering both the public and private sectors has now been in force in New Zealand for just over 23 years. The Privacy Act 1993 is based around 11 information privacy principles that draw on the 1980 OECD Guidelines.[5] The currency of this legislation is "personal information", which is defined as information about an identified or identifiable individual.[6] The concept of "personal information" in New Zealand also covers both opinion and false information about an individual. "Personal information" need not be in recorded form,[7] and the concept extends to what is held in a person's memory. A case that illustrates the utility of extending the concept to unrecorded information in the employment context is that of an unsuccessful job applicant who requested the interview notes of an appointment panel. Although the panel members destroyed their notes after the employment decision was made, on review the individual panel members were asked "each to supply a written statement of reasons why the other candidates had been considered better suited, or the requester considered less suited, for the position."[8]

There have been many New Zealand privacy cases relating to the workplace. An important feature of the legislation is that a breach of a privacy principle on its own does not necessarily lead to liability under the Privacy Act. Except in the case of denied access or correction rights, the breach of a privacy principle must always 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".[9] This functions as an important sifting mechanism in the legislation to filter out complaints of a minor nature.

[5] Section 6.
[6] Section 2.
[7] See, for example, *Re Application by L [information stored in person's memory]* (1997) 3 HRNZ 716.
[8] *Case No 794* (1987) 8 CCNO 66 (Ombudsmen's Cases), a public sector case dealt with under the Official Information Act 1982; after 1993, it would have been dealt with in a similar manner by the Privacy Commissioner under the Privacy Act.
[9] Section 66(1)(b)(iii).

The Privacy Commissioner oversees the application of the Act and plays an important role in investigating and conciliating complaints. The Privacy Commissioner's views, however, are not legally binding.[10] Only the Human Rights Review Tribunal can determine legal issues at first instance,[11] but it cannot do so unless the Privacy Commissioner has first investigated the complaint. If a complaint has not been resolved by the Privacy Commissioner, it can be taken to the Tribunal by the Director of Human Rights Proceedings if he decides to do so, or else personally by the aggrieved individual. There are rights of appeal from the Tribunal to the higher courts of general jurisdiction in the judicial hierarchy.[12]

The legislation, however, contains a disjunction in the processing of privacy complaints between the approach to be taken by the Privacy Commissioner and that taken by the Tribunal and appellate courts. This results from the Privacy Commissioner's express duty to balance privacy against other important social interests, such as the right of businesses to operate efficiently,[13] a balancing exercise that does not apply to the Tribunal or appellate courts. The Court of Appeal majority in *Harder v Proceedings Commissioner* once commented that s 14(a), although directed to the Privacy Commissioner, implicitly applies to the Tribunal and appellate courts,[14] however this wider reading of s 14(a) has never been subsequently adopted. We are therefore left with a difference in legal approach between application of the Act by the Privacy Commissioner, and that by the Tribunal and other judicial institutions. The reason for the difference in approach is not evident,[15] but it allows the Commissioner to promote the settlement of complaints in a pragmatic way. However, it also tends to permit the Commissioner to operate in a manner that is less strict on employers, as is evident from a number of investigation case notes. It seemingly permits business efficiency considerations to trump workers' privacy interests under the information privacy principles. Neither the New Zealand Law Commission nor the government has indicated that s 14(a) ought to be changed.

New Zealand employment law, however, has been ready to recognize the privacy principles in the Privacy Act and has used them to inform decisions on whether an employer's action has been fair and reasonable, even though the specialist employment institutions do not have the jurisdiction to interpret these principles or apply them directly; only the Human Rights Review Tribunal has such jurisdiction, with the Privacy Commissioner's views being relevant (though of no legal force) for the purpose of conciliating privacy complaints.[16] The Employment Court has

[10] Section 78. The Privacy Commissioner can only make a final and binding decision about an unreasonable charge imposed for access to personal information held by a private sector agency (personal information held by public sector agencies is available free of charge).

[11] There is currently a proposal to amend the legislation to allow the Privacy Commissioner to determine access complaints: see *Government Response to Law Commission report on Review of the Privacy Act 1993* (27 March 2012) at 5.

[12] These are the High Court, the Court of Appeal and the Supreme Court.

[13] Section 14(a) provides that the Privacy Commissioner must "[h]ave due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way".

[14] [2000] 3 NZLR 80, at [23].

[15] This feature of the legislation is perhaps unintentional in relation to complaints. It has greater relevance to the Privacy Commissioner's public advocacy function in promoting privacy.

[16] The earliest employment law case drawing on the principles of the Privacy Act was *Graham v Christchurch Polytechnic* CEC 48/93, 14 September 1993, which was decided just a few months after the Privacy Act came into force. In *NZ Amalgamated Engineering Printing and Manufacturing Union*

recognized that "[t]he Privacy Act's provisions may be said to represent current community standards and expectations",[17] which are considerations that are relevant in deciding whether or not an employer's actions are justifiable.

Collection of Personal Information

The basic international standards relating to the collection of personal information are that collection should not be unlimited, and that the manner of collection should be fair. This is expressed in the OECD Guidelines collection limitation principle, which provides that:[18]

> There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

This principle is transposed into the Privacy Act by principles 1 to 4.[19]

Firstly, the collection of information must be "necessary" for the purpose for which it is being collected.[20] The term "necessary" has been judicially interpreted as "reasonably necessary",[21] and, as will be seen, the Privacy Commissioner tends to take a wide view of what is necessary to collect, since the legislation under s 14(a) requires the Commissioner to have:

> …due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way.

Secondly, personal information must also be collected by lawful and fair means.[22] It should be noted that this requirement refers to the manner of collection rather than the content of the information concerned.

These two aspects of the collection limitation principle are non-derogable, in the sense that there are no exceptions and there is no provision for the individual concerned to waive the right.

Inc v Air New Zealand Ltd (2004) 7 HRNZ 539 at 218, the Court observed that "the Privacy Act 1993 does not give rights or impose obligations that are enforceable in this or any other Court of law. Questions of statutory privacy are to be dealt with by a discrete and exclusive procedure involving, among others, the Privacy Commissioner and the Human Rights Review Tribunal."

[17] *NZ Amalgamated Engineering Printing and Manufacturing Union Inc*, above n 16, at 221.

[18] Council of the Organisation for Economic Co-operation and Development (OECD) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980, updated in 2013) at [7].

[19] Section 6.

[20] Principle 1.

[21] *Lehmann v Canwest Radioworks Limited* [2006] NZ HRRT 35. In Australia, the phrase "reasonably necessary" is employed in the legislation itself: Privacy Act 1988, APP 3.1 and 3.2. In Hong Kong, however, the term "necessary" in the legislation is more strictly interpreted, as will be seen, inter alia, from the cases dealing with the employment context. Both Australian and Hong Kong privacy law were also based around the OECD Guidelines.

[22] Principle 4.

Thirdly, personal information should be collected with the individual's knowledge or consent, where appropriate.[23] There are a number of exceptions to this aspect of the collection limitation principle.

Collection of Personal Information from Job Applicants

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.[24] New Zealand also has a spent convictions regime.[25]

Whether or not the collection of particular information is "necessary" in the pre-employment context has in practice involved an assessment of its reasonableness, and due allowance has been made here, as elsewhere generally 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.

The Privacy Commissioner has found that personality testing of job applicants is permissible under the Privacy Act. In one case,[26] 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. The Commissioner considered that, in terms of principle 1 ("Purpose of collection of personal information"), 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 Commissioner could not say that the test was unnecessary or that the information collected was excessive. The Commissioner could only find a breach of principle 3 ("Collection of information from subject"), because when the information was being collected, the complainant should have been informed that her information would be passed to another agency for evaluation. The 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 Act tends to be ineffective in substantively limiting the amount and extent of information collected, and that it is more easily invoked where there has been a technical failure to comply with the proper procedure for collecting personal

[23] Principle 3(1).
[24] Part II of the Human Rights Act 1993 deals with acting on the basis of particular prohibited grounds of discrimination. In particular, s 23 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.
[25] Criminal Records (Clean Slate) Act 2004.
[26] Privacy Commissioner *Case Note 2418* [1999] NZPrivCmr 6.

information. In this case, the Act required that the individual concerned be informed of the intended recipients of the information. This is cold comfort, however, where there are loose restrictions on the extent of information that can be collected.

Employment law drew upon the collection principles in the Privacy Act to assist the Employment Relations Authority in a case where it determined whether or not an employer had justifiably dismissed an employee. The reason for the dismissal was the employee's failure to volunteer information in a pre-employment form that the employer was not entitled to collect in the first place.[27] The employee was dismissed because she allegedly misrepresented her medical condition on the form when she applied for a sales position. The form included a question about whether she had medical problems of any kind. In completing the question, she referred only to a condition that affected her hip joint. Once she was employed, her employer thought she was taking an excessive number of sick days. When dismissing her, the employer accused her of having failed to disclose at least two pre-existing medical conditions that had a serious impact on her ability to perform her job. The Employment Relations Authority determined that the applicant's failure to refer to the two pre-existing medical conditions did not amount to misrepresentation because the employer was not entitled to collect this information since it was likely to be in breach of the Privacy Act collection principles. The scope of the information sought went beyond what was relevant to the employer's compliance with its health and safety obligations or the employee's ability to do her job. The Authority's determination was upheld on appeal to the Employment Court, which remarked that the company's question was "inappropriate" and imposed no obligation on the job applicant to disclose all of her medical problems. Therefore, the employee could not be justifiably dismissed because of this failure to disclose the information concerned.[28]

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 on private property without consent of the lawful occupiers,[29] and a prohibition against the surreptitious use of video cameras that also have audio recording capabilities.[30] Although the Privacy Commissioner has long accepted that surreptitious recording is covered under the Privacy Act,[31] this view is questionable[32] and is proposed to be clarified by a change to the law.[33]

---

[27] *Attwood v Imperial Industries* WA 72/01, 25 October 2001. Although this case did not arise in the Privacy Act jurisdiction (which would have been heard in the Human Rights Review Tribunal), the Employment Relations Authority member who delivered this decision was also the Chairperson of the Human Rights Review Tribunal.

[28] *Imperial Enterprises Limited v Attwood* [2002] 2 ERNZ 740 at [59].

[29] Private Security Personnel and Private Investigators (Code of Conduct — Surveillance of Individuals) Regulations 2011, reg 6.

[30] Crimes Act 1961, s 216B ("Prohibition on use of listening devices").

[31] See, for example, "Extract from a letter by the Privacy Commissioner concerning video surveillance" in *A Compilation of Materials on the Privacy Act 1993 and the Office of the Privacy Commissioner February 1994-December 1994* (vol 2) at 252–253; and Privacy Commissioner *Case Note 0632* [1994] NZPrivCmr 27 and *Case Note 16479* [2001] NZPrivCmr 6.

However, even if surveillance is covered under the Privacy Act, the legislation would be of little avail in the workplace, to judge by the few reported cases on workplace surveillance. In these cases, the Privacy Commissioner found workplace surveillance to be a permissible practice. In the earliest case,[34] the Commissioner dealt with an employee's complaint about surveillance of a work changing room in order to detect theft. The Commissioner found that the employer was not obliged to take reasonable steps to ensure, in accordance with principle 3 ("Collection of information from subject"), 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 in addressing surveillance activities. The Commissioner found that:

- It was not reasonably practicable to draw on 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));
- 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)); and
- 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 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 a similar subsequent case,[35] a union complained on an employee's behalf that a video camera had been installed in a locker room. The union was concerned that employees had not been notified before the camera was installed. The Privacy Commissioner, however, formed the view that none of the collection principles had been breached. The purpose of installing the cameras was to identify the persons responsible for thefts from the lockers. A notice was displayed at the entrance to the worksite, advising that hidden cameras might operate there. The employer also explained that previous warnings to workers about theft had been unsuccessful as a

[32] See *Harder*, above n 14, which found that surreptitious voice recording over a telephone did not constitute a "collection" of information, but was the receipt of unsolicited information, which is excluded from the Privacy Act s 2 definition of "collect".
[33] Law Commission *Review of the Privacy Act 1993: Review of the Law of Privacy, Stage 4* (NZLC R123, 2011), recommendation 7.
[34] *Case Note 0632*, above n 31.
[35] *Case Note 32277* [2003] NZPrivCmr 25.

deterrent. The Commissioner therefore believed that the employer had a lawful purpose in installing the camera, and that the collection of the information was necessary for that purpose. The Commissioner, however, considered that the sign at the worksite warning employees generally of hidden filming was insufficient to alert employees that there was a hidden camera in the locker room, as employees would not expect that. However, an exception to the requirement of notification applied in the circumstances, in that the employer reasonably believed that compliance would prejudice the purposes of the collection.[36] The Commissioner also did not consider that the filming was unfair since there had previously been thefts from the locker room, and management had been requested to find the thief. Moreover, the Commissioner did not find that the filming was unreasonably intrusive into workers' privacy, despite the filming taking place in a locker room. This was on the basis that activities in the shower or toilet area were not filmed; the camera was activated only by movement near the target locker; it was necessary that the camera be able to record faces so as to identify the thief; and the camera was to be in operation only until the culprit was identified.

In another workplace case,[37] the Commissioner found it acceptable for an employee to surreptitiously film a colleague with a cellphone. Both worked as caregivers for young people with disabilities, and the worker was concerned about the complainant's conduct towards clients, which could be abusive and inappropriate. Believing the complainant posed a safety risk, he gave the recordings to their employer, who used them in disciplinary proceedings against the complainant that resulted in a warning. The Commissioner observed that the recordings provided the employer with the best evidence against the employee. The Commissioner recognised, however, that "covert recording is intrinsically intrusive, and needs strong justification for its use." While finding this to be a "difficult case", the Commissioner observed that the intrusion was justified in light of the safety reasons for collecting clear evidence of wrongdoing, particularly as the victims were not in a position to complain of mistreatment on their own account. Accordingly, the Commissioner remarked that:

> On balance, this was one of the rare occasions where it will be acceptable for an onlooker to make a covert recording to ensure that evidence of what was said is accurately captured.

As the relevant principle on the fairness of collection (principle 4) does not provide for any exceptions, the reasoning in this case note must depend on the Commissioner's duty under s 14 of the Privacy Act to balance privacy against other important social interests. The Tribunal, however, is not bound by the same requirement, so if the complaint had been taken further, the result might not have been the same.

The Privacy Commissioner did not find it acceptable to surreptitiously record an interview with an employee suspected of stealing stock.[38] The employee was dismissed, but found out about the recording in the course of proceedings contesting his dismissal. The Commissioner found that the employer had not breached the

[36] Principle 3(4)(d).
[37] *Case Note 101213* [2008] NZPrivCmr 4.
[38] *Case Note 16479* [2001] NZPrivCmr 6.

collection principle that covered the lawfulness and necessity for collecting the information (principle 1), as collecting information and evidence relevant to a possible termination of employment was lawful and reasonably necessary for a business. However, the employer had breached the collection principle that requires the individual to be informed of the collection of the information (principle 3), since the employer obtained an accurate reproduction of the exact words and inflections used by the employee when being interviewed. The Commissioner commented that "[t]he fact of recording an interview on tape, rather than merely relying upon written notes and memory, is a matter that the individual should be made aware of." The Commissioner also found that the collection of the information was unfair (principle 4), since the individual would not be aware of all "the minute details of what was said and how it was said" that could be recorded by taping, as opposed to recording by hand or through one's memory. The individual might also have responded to questions differently if he was aware of the recording. The Commissioner added that the nature of the relationship between the parties, being an employment relationship, and the circumstances in which the recording took place, also contributed to the unfairness.

In the specialist employment law jurisdiction, on the other hand, covert recordings of interviews between employers and employees have been found to be admissible as the best evidence of what was said. For example, in the Employment Relations Authority, an employee's covert recording of a conversation with his employer was accepted as evidence in his constructive dismissal case.[39] The Authority held that it would be unfair to deprive the employee of being able to prove the "resign or be dismissed" attitude of his employer. Both sides in that case relied on a Court of Appeal decision on an appeal from the Employment Court that dealt with the admissibility of a telephone conversation that had been covertly recorded by one of the parties.[40] The Court of Appeal held that there could be cases where such recordings could breach the duty of fair dealing between the parties, but the ultimate criterion is fairness in the circumstances. In that case, the recording was found to be admissible.

The position regarding surveillance in the workplace in New Zealand may be contrasted with that in Hong Kong. The case law indicates that Hong Kong's approach is somewhat more strict than in New Zealand, with emphasis placed on the proportionality of the practice in the circumstances.[41]

In one case,[42] a government department installed pinhole cameras at different locations in its regional office, including near the toilets and changing rooms. The purpose of these was to detect crime, since there had been a series of thefts in the office. The Privacy Commissioner referred to his publication *Privacy Guidelines: Monitoring and Personal Privacy at Work*, and stated:

[39] *Simms v Santos Mt Eden Ltd* ERA Auckland AA 254/05, 21 August 2003.
[40] *Talbot v Air New Zealand* [1995] 2 ERNZ 356, [1996] 1 NZLR 414 (CA).
[41] The Office of the Privacy Commissioner for Personal Data (HK) has produced a publication to assist employers who propose to monitor employees: *Privacy Guidelines: Monitoring and Personal Data Privacy at Work* (December 2004). It is not legally binding, nor does it purport to set out definitive statements of the law, but it is in the nature of recommendations for best practice.
[42] Office of the Privacy Commissioner for Personal Data (HK) *Case No 2005C06.*

> … covert monitoring is not to be used unless justified as last resort measures and being absolutely necessary in detecting or gathering evidence of unlawful activities, and the monitoring should be limited in scope and duration. Further, the employer should formulate a clear employee monitoring policy by making known and communicating to the employees the purposes of the monitoring, the circumstances under which monitoring will take place and the kind of personal data that will be collected.

The Commissioner found that, although the employer had a legitimate purpose in protecting property from theft, the evidence did not show so great a risk of loss as to justify large scale hidden filming activities, which was highly privacy intrusive. The Commissioner remarked that:

> The dimension and extensiveness of the monitoring activity carried out was out of proportion to attaining the purpose of collection, and the department was intent upon engaging in continuous and universal preventive monitoring.

Moreover, there was no definite plan or policy regarding its duration. Other, less privacy intrusive means or overt monitoring could have been considered instead. Accordingly, the Commissioner found that the monitoring was carried out in an unreasonable and unfair manner.[43]

In a subsequent case,**[44]** the Commissioner also found that surreptitious recording was inappropriate in the circumstances. Two employees of a residential estate were dismissed for unauthorised absence from duty after a pinhole camera filmed them lingering for more than an hour in a changing room. The camera had been placed in the staircase leading to the changing room, its purpose being to monitor employees and enhance security. No notice was posted in the area being monitored to inform people that it was under surveillance. The Commissioner did not accept that the camera was installed on the property for security purposes, because it was covert rather than overt. The Commissioner also found that the collection of information about the employees without their knowledge was unfair in the circumstances, and so breached the collection principle.**[45]** The employer had no privacy policy on employee monitoring, and so employees would not reasonably expect to be monitored by a hidden device. The Commissioner commented that "[c]overt monitoring is generally regarded as highly privacy intrusive. Employers should not adopt covert monitoring unless it is justified by the existence of special circumstances and reasons."[46]

The Commissioner stated that, even if the employer suspected employees of dereliction of their duties, the lack of seriousness of their misconduct did not justify the highly privacy intrusive measures taken. Other, less privacy intrusive means were available, such as a surprise check. If it was considered that monitoring devices were necessary, overt rather than covert ones would achieve the same result.

Collecting Information from Workplace Computers

[43] Accordingly, there was a breach of Data Protection Principle (DPP) 1(2) ("Purpose and manner of collection of personal data"). Moreover, there was also a breach of DPP 5 ("Information to be generally available") because of the lack of an employee monitoring policy.
[44] Office of the Privacy Commissioner for Personal Data (HK) *R12-4839* (14 February 2012).
[45] DPP 1(2).
[46] At [32].

There are a few employment law cases involving the collection of information from workplace computers by employers, but the Privacy Act plays no significant role, if any, in these. Such cases tend to turn on the justifiability of subsequent disciplinary action. There are no privacy rights per se in respect of employees' workplace email or other internet use, but the justifiability in terms of employment law of any disciplinary action for misuse may turn on whether the employee had a reasonable expectation of privacy in the circumstances, and other factors. For example, there have been cases that turned on whether there had been employer training and policies regarding internet use,[47] the nature of the use (messages containing sexual innuendos and surfing the net for pornography being particularly frowned upon),[48] the length of service,[49] and rights of free expression during industrial negotiations.[50] The emphasis has been on fairness and due process, rather than reliance on the Privacy Act.

One could raise the technical issue of whether an employer who gathers information about an employee's internet use is actually "collecting" information in strict terms of the Privacy Act. This is because the employer already "holds" this information in its computer system, which is a prerequisite for the use and disclosure of it. Much information will also likely be "unsolicited" information (and so it falls outside the Act's limited s 2 definition of "collect").[51] Therefore, the rules relating to individual notification (principle 3), and the requirement that the retention, use and disclosure of such information must relate to the original purpose for collecting it, do not apply. Any rights that an employee has in this area in respect of the collection of personal information therefore arguably stem from employment law, not from the Privacy Act, which technically may not apply.

A Privacy Commissioner's case note on the collection of personal information from a worker's computer by means of monitoring software proceeded on the basis that the employer was indeed "collecting" the information in terms of the Privacy Act.[52] The monitoring took place in the context of an employment investigation, and the information collected included emails sent to and from the computer, and key-stroke logs for the computer. The key-stroke logs were used to access the worker's personal web-based email account, and several emails were copied. The Commissioner dealt separately with the information collected directly from the work computer, and the information collected from the worker's personal email account. The Commissioner considered that the collection of information directly from the work computer did not breach the Privacy Act, since computer monitoring was provided for in both the employment agreement and work rules.

One matter that was not covered, however, was notification that detailed information was being collected through key-stroke logging, and this was a breach of the Privacy Act collection principle that requires making an individual aware of the fact that information is being collected (principle 3(1)). The Commissioner also found that the employer's use of the worker's password through key-stroke logging to gain access to the worker's personal email account breached the Privacy Act collection principles. The access to a significant number of emails sent over a number of years "was

[47] *Clarke v Attorney-General* [1997] ERNZ 600 (EmpC).
[48] *Clarke*, above n 47; *Allerton and Offord v Methanex (NZ) Ltd* WC 23/00 (EmpC).
[49] *Clarke*, above n 47.
[50] *Howe v The Internet Group Ltd (IHUG)* [1999] 1 ERNZ 879 (EmpC).
[51] The definition of "collect" excludes unsolicited information.
[52] *Case Note 229558* [2012] NZPrivCmr 1.

unnecessary and disproportionate to the employer's needs";[53] and workers were not notified that the employer could use key-stroke logging to obtain their passwords to collect further personal information about them that was not held on their work computer.[54] Moreover, given that there was a high expectation of privacy in a password-protected account, "it would require exceptional circumstances to justify an employer directly accessing it". As there were no such circumstances in the present case, "this method of collection was unreasonably intrusive".[55] This complaint was subsequently settled through mediation.

Another Privacy Act case,[56] decided in the Tribunal, concerned an employer who pressured an employee to access Facebook so that a screenshot could be taken of a photograph taken and uploaded by a former employee that was insulting to the company. The Tribunal did not deal with any issues relating to the collection of this information because the complainant's case on this point was "bound to fail" because she would not have been able to prove a causal connection between the alleged breaches of the collection principles and the eventual harm she suffered when the former employee's photograph was disclosed to local employment agencies, harming her chances of finding employment.[57] This was a surprising finding, since, but for the collection of the information, it could not have been subsequently disclosed.

In a Hong Kong case,[58] a worker complained that her employer logged into her computer to collect cookies without notifying her. She had been assigned a username but was able to set her own password. The complainant's supervisor asked for her password for "emergency use". The supervisor later found that she used the computer to play online games during work hours, and the supervisor collected her browsing history (the cookie data). The Commissioner first found that the cookies contained personal data about the complainant, since they contained her name and the websites browsed by her. The Commissioner went on to find that, since the cookies were records gathered by the supervisor to determine whether or not the complainant was breaching work rules, there had been a collection of her personal data by the supervisor. The Commissioner found that the collection of information in the circumstances was unfair,[59] noting that "[t]he employer had not taken any practical measures to stop or prohibit the Complainant from using the Computer for private purposes or storage of private data." The complainant had a reasonable expectation of privacy, given that passwords were private to employees. The supervisor's use of the password was therefore inconsistent with the professed reason for asking for it, which was for "emergency use". Consequently, the Commissioner issued an enforcement notice to stop the employer using employees' passwords to log into their computers and collecting employees' browsing histories unless the employer had their prior consent. The Commissioner also found a breach of the openness principle,[60] in that the employer:

[53] There was therefore a breach of principle 1.
[54] There was therefore a breach of principle 3.
[55] There was therefore a breach of principle 4.
[56] *Hammond v NZCU Baywide* [2015] NZHRRT 6.
[57] At [133]. In the result, the former employee was awarded $168,000 for this harm, the amount stemming from the employer's disclosure of the information (under principle 11), but not from the dubious manner it was collected in the first instance.
[58] Office of the Privacy Commissioner for Personal Data (HK) *Case No 2006C14* (September 2010).
[59] In breach of DPP 1(2).
[60] DDP 5 ("Information to be generally available").

> …had not taken all the practicable steps to ensure that the Complainant was aware of the policy and practices of the Organization on recording employees' browsing history in its computers.

Collection of Workers' Bodily Substances

With the testing of bodily substances, one encounters a conceptual difficulty: are bodily fluids and cells "personal information", or are they merely, and literally, disembodied data that, when analysed scientifically, yield personal information, but are not personal information themselves? Accordingly, unless legislation specifically includes bodily substances in the definition of "personal information", the notion becomes contestable.[61] Thus, for example, the New South Wales Privacy and Personal Information Protection Act 1998 includes "bodily samples" in its definition of "personal information".[62]

The New Zealand Privacy Commissioner has opposed random drug testing in the workplace,[63] but there have been no published Privacy Act complaints on the issue.[64] Assuming that collecting a bodily sample such as urine would amount to the collection of "personal information", the testing would have to be for a lawful purpose connected with a function or activity of the employer and necessary for that purpose (principle 1), and it would have to be carried out fairly and without intruding unreasonably into the individual's personal affairs (principle 4). For better or worse, workplace testing can generally be viewed as reasonably necessary by employers insofar as it ostensibly addresses productivity and health and safety issues. Moreover, in principle at least, testing is a consensual activity, despite the likelihood that an unreasonable refusal to undergo testing will mean losing one's employment.

The permissibility of drug and alcohol testing in New Zealand has turned on employment law rather than privacy law. Unless specifically provided for in an employment agreement,[65] however, an employer would be faced with real difficulties

---

[61] For discussion of the issue, see Lee Bygrave "The body as data? Reflections on the relationship of data privacy law with the human body" (conference paper, Office of the Victorian Privacy Commissioner, Melbourne, 8 September 2003); Bruce Alston "Blood rights: the body and information privacy" (2005) 12(4) J Law Med 426; Rohan Hardcastle *Law and the Human Body: Property Rights, Ownership and Control* (Hart Publishing, Oxford, 2007) at 98.

[62] In Norway, on the other hand, which lacks such an inclusive definition, samples were found by the Norwegian Data Protection Tribunal not to be "personal data" under the Personal Data Act 2000 on appeal in Case 8/2002: see Bygrave, above n 61, at n 104.

[63] Bruce Slane "The Privacy Implications" in *Drug Testing: The Sporting Experience: the Employment Possibility* (Legal Research Foundation, Auckland, 1995) 89, and "Critical Privacy Issues for Employers and Employees" (Address to Industrial and Employment Relations' 10th Annual Conference, 19 March 1996).

[64] For discussion of how the Privacy Act might apply, see John Edwards "Workplace drug testing" (1995) 1(1) HRLP 43; Michael Webb "Workplace drug testing: Another perspective" (1995) 1(3) HRLP 131; John Edwards "Privacy Updates – Notes on Recent Developments" (1996) 1(4) HRLP 187 at 187–188; Cordelia Thomas "Drug Testing in the Workplace" (1997) 22(2) NZJIR 159; and Paul Roth "The Privacy Act 1993: Workplace testing, monitoring, and surveillance" (1997) 3(2) HRLP 113.

[65] In an early case concerning the legality of testing, a collective agreement providing for unrestricted random testing was found by the Employment Court to be "harsh and oppressive" under now-repealed industrial legislation: *Harrison v Tuckers Wool Processors Ltd* [1998] 3 ERNZ 418. The Employment Court found that clauses providing for random drug and alcohol testing, as well as medical examinations, were harsh and oppressive in terms of s 57 of the Employment Contracts Act 1991 insofar as they related to giving consent in advance, and the relevant clauses were struck out. On

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 decided to dismiss the worker, the issue would then become 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 reasonably necessary and undertaken in a fair and reasonable manner.[66] The only thing added by the existence of the Privacy Act is the background of upholding the societal value of an individual's freedom from unreasonable intrusion into his or her personal affairs unless there are sufficiently important countervailing considerations.

In an interim injunction case where the employee sought reinstatement pending substantive determination of his unjustifiable dismissal case,[67] the Employment Court considered drug testing to be prima facie acceptable if it was carried out in a procedurally fair manner and in a safety-sensitive context. The Privacy Act was not cited. In the absence of a contractual entitlement to require testing, it is more common for employers to carry out tests on job applicants rather than on current employees.

The issue of permissibility when introducing a drug and alcohol testing regime for existing workers was first determined by the Employment Court in 2004,[68] when the full Court found that an employer would be justified in introducing such a regime where health and safety were legitimate concerns. While the Court cautioned that its findings were specific to the case at hand, the points on which the case turned, and the conservative conclusions reached, could be easily generalised.

Air New Zealand wanted to introduce a drug and alcohol policy into the workplace that included provisions for testing existing employees. The six plaintiff unions sought a permanent injunction and declarations restraining the implementation of the announced policy. Among the causes of action raised were that the policy constituted an impermissible unilateral variation of the employees' existing employment agreements, and that the requirement to submit to testing was both unreasonable and unlawful because the provision of bodily samples in such circumstances breached the New Zealand Bill of Rights Act 1990, the Privacy Act, and the Human Rights Act 1993.

---

appeal to the Court of Appeal, the case was remitted to the Employment Court to be reconsidered in light of the criticism that the lower court failed to refer in its judgment to "statistical, research or other empirical material in support of the proposition that particular terms of the contract are or are not 'harsh and oppressive'": *Tucker Wool Processors Limited v Harrison* [1999] 1 ERNZ 894; [1999] 3 NZLR 576 at [79]. Upon reconsideration on this basis, the Employment Court found that the requirement to undergo drug and alcohol testing on an undefined fair and reasonable basis was among a number of provisions which in combination rendered the contract "exceptionally burdensome": *Harrison v Tuckers Wool Processors* [2000] 1 ERNZ 572 at [63]–[64]. The Court commented that some of the provisions "could only have provided the satisfaction of exercising domination over the persons of others." The issue by that stage, however, was academic, as the company had gone out of business.

[66] Principles 1 and 4 respectively.

[67] *Philson v Air NZ Ltd* AEC 35/96, 3 July 1996.

[68] *NZ Amalgamated Engineering Printing and Manufacturing Union Inc*, above n 16.

None of these contentions were upheld. The dominant considerations in this case were the employer's statutory and common law obligations in respect of workplace health and safety. These, together with its right to manage, empowered the employer to promulgate relevant policies. The Court considered that testing was permissible in the following circumstances contemplated by the policy:[69]

- On reasonable cause to suspect that an employee's behaviour is an actual or potential cause or source of harm to others as a result of being affected by alcohol or drugs or both;
- On internal transfer to safety sensitive occupations (by analogy with pre-employment testing);
- In post-accident / incident / near miss situations; and
- In random testing in safety sensitive areas only, not across the board.

The issue for subsequent cases, therefore, is what constitutes a "safety sensitive" activity, as many jobs involve potential hazards of one kind or another. The Court acknowledged that defining what constituted a "safety sensitive" area was in itself problematic in the case at hand. It commented that the "exercise of defining it ... is not one for the Court to undertake", but for the employer to discharge in consultation with the plaintiff unions.[70] Although the Court's reluctance to become involved in such an issue is understandable, it is uncertain how this aspect of the case can be transposed to other enterprises or industries in different circumstances. The Court's approach to the permissibility of testing, however, should not mean that it will be a simple matter of justifying testing on real or imagined health and safety concerns. Considerable work and administrative commitment underlay Air New Zealand's introduction of its policy. Air New Zealand was able to satisfy the Court that the scope, means, and rationale of its testing policy were fair and reasonable, with the exception of random "suspicionless" testing of employees employed outside safety sensitive areas.[71]

In a subsequent case on workplace drug and alcohol testing,[72] the Employment Court held that the employer's intended introduction of a drug and alcohol policy would not breach collective and individual agreements covering union members and would be otherwise lawful. Such testing policies "must meet the twin tests of lawfulness and reasonableness if they are to be enforceable."[73]

Drug testing in Hong Kong has mainly been an issue in relation to testing in schools and by the Police. Workplace drug testing appears not to be an issue, and there is no information about it on the Privacy Commissioner's website. In one case,[74] an employer required its female employees to submit to a DNA test after discovering menstrual bloodstains in the female toilet. The employer wished to find the woman responsible and deter a recurrence. The employer proposed to match the DNA test results against the bloodstains found in the toilet. An employee who felt humiliated by being required to undergo such a test complained to the Privacy Commissioner, who upheld her complaint on the basis that the collection of information was neither

[69] At [254].
[70] At [255].
[71] At [262].
[72] *Maritime Union of New Zealand Inc v TLNZ Ltd* [2007] ERNZ 593 (EmpC).
[73] At [126].
[74] Office of the Privacy Commissioner for Personal Data (HK) *Case No 2004C01*.

necessary nor reasonable (DPP 1(1)). Such a collection was highly privacy invasive and was only justifiable in serious circumstances, such as in a criminal investigation.

In a recent United States District Court decision,[75] an employer was found guilty of breaching the Genetic Information Nondiscrimination Act 2008 (GINA) for illegally DNA testing employees in order to ascertain who was defecating in the company's warehouse during particular shifts.[76] The Act prohibits employers from using an individual's genetic information for employment decisions such as hiring, termination and promotions, or health insurance coverage. The DNA was collected through cheek swab samples. Two of the workers, who had tested negative, sued the company for breach of the GINA. The jury awarded the defendants $250,000 and $225,000 respectively for emotional harm, as well as $1.7 million in punitive damages because the company "acted with malice or with reckless indifference to the Plaintiff's federally protected rights".[77] The case seems somewhat unusual in that the DNA testing was not used to discriminate against the plaintiffs in relation to any employment decisions, and in fact the testing cleared them of any wrongdoing. Such testing might well be lawful in New Zealand, on analogy with drug testing, whereas it might well not be permitted in Hong Kong, on analogy with the DNA testing complaint above.

Use of Biometrics

There is one case where the Privacy Commissioner investigated but rejected a union complaint about the introduction of finger-scanning technology for an employer's payroll system.[78] 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 claimed that a scanner had become "necessary" in terms of the collection principle due to employee dishonesty in completing time sheets (principle 1). 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 for hospital cleaners 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 did not find the proposal to be unfair or unreasonably intrusive, even though he declined to consider the contractual issue. The Commissioner held that this issue fell squarely within the jurisdiction of the specialist employment law institutions, and remarked that "[i]t would have been quite improper for me to usurp the role of the Court by dealing with the matter." Given that the collection principle requires agencies not to collect personal information "by

[75] *Lowe and Reynolds v Atlas Logistics Group Retail Services* 102 F Supp 3d 1360 (ND Ga 2015).
[76] This apparently is not a unique type of occurrence. For a similar problem at the Denver office of the Federal Environmental Protection Agency, see Eric Katz "EPA Employees Told to Stop Pooping in the Hallway" (25 June 2014) Fedblog <www.govexec.com>.
[77] *Lowe and Reynolds*, above n 75.
[78] *Case Note 33623* [2003] NZPrivCmr 5. Similar complaints about finger scanning were also rejected by the Canadian Privacy Commissioner (*PIPED Act Case Summary No 185* (2003)) and the Irish Data Protection Commissioner (*Case Study 1* (2005)).

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. In effect, the Commissioner endorsed the lawfulness of the practice under the contract by declining to consider whether or not it was unlawful.

The union fared better before the Employment Court.[79] The Court found that the introduction of finger-scanning was unlawful in the circumstances because the employer breached contractual and statutory requirements to consult the employees concerned. The employees objected to having their fingerprints scanned, and advised that they would not comply until the dispute was resolved. The company maintained that its direction to the employees was lawful, and it sought a declaration to that effect. The Court found that the employees concerned were not breaching their contracts because the instructions they had been given were themselves unlawful. The Court held that the employer had a statutory good faith obligation to consult on changes in workplace practices.[80] The Court remarked that the requirement of consultation will depend on the context. The context here — and this was the key factor upon which the case turned — was that most of the nearly 50 employees concerned were Samoan. The evidence indicated that these particular workers regarded the introduction of the new technology as culturally offensive because it implied that, like criminals, they were not to be trusted. Expert evidence was introduced to show that the technology raised issues relating to Samoan beliefs concerning the sacredness of parts of the body and the concept of *Va Fealoia*, "the sacred space which governs and manages all relationships between people including employers and employees." The Court also noted that the legislation requires employers in the public health sector to be "good employers".[81]

The wider applicability of this case should be approached with some caution insofar as the Court's reliance upon contractual and statutory obligations is concerned. In particular, the case draws no clear line between workplace matters about which an employer is required to consult, and those which it is not. The Court also set out a number of broad propositions for determining the lawfulness of the introduction of new technologies into the workplace:[82]

1. Is the technology compatible with the contractual obligations of the parties?

[79] *OCS Ltd v Service and Food Workers Union Nga Ringa Tota Inc* (2006) 3 NZELR 558. An earlier, lower level Employment Relations Authority case found the use of finger-scanning was permissible, against the objection of an employee. This was on the basis that the employee's contract provided that he was required "to complete all time and wage records as required by the Company." This was held to be wide enough to encompass a finger scanning system: *PMP Print Limited v Barnes* ERA Auckland AA317/04, 28 September 2004. Among the employee's arguments was that use of the technology would result in his being stamped with the Mark of the Beast, as referred to in the biblical Book of Revelations, with the result that he would not be able to participate in the Rapture. The Authority, however, rejected this indirect discrimination argument. Among other things, the Authority noted that the technology does not actually stamp a mark on a person, or even store the image of a fingerprint; it merely stores a mathematical representation.

[80] Employment Relations Act 2000, s 4(1A)(b) requires "parties to an employment relationship to be active and constructive in establishing and maintaining a productive employment relationship in which the parties are, among other things, responsive and communicative".

[81] Employment Relations Act, sch 1B, cl 5. There was also a specific statutory requirement (via the New Zealand Public Health and Disability Act 2000, s 6(1) and the Crown Entities Act 2004, s 118(2)(f)) to recognise "the cultural differences of ethnic or minority groups".

[82] *OCS Ltd*, above n 79, at [95].

2. There is to be a balance between the need for the technology and the level of personal intrusiveness involved for the individual concerned.
3. The employer has the right to introduce different systems of timekeeping technology subject only to reasonable consideration of valid concerns raised by the union and / or employees.
4. The employer must take the appropriate steps to inform employees of the new measures and to obtain their consent.

These principles were distilled from a number of overseas cases determined in a variety of contexts and under different legal regimes, and so their applicability to New Zealand employment law would need to be determined on a case-by-case basis.

In contrast to the position in New Zealand, Hong Kong privacy law is stricter in its approach to finger-scanning. In one case,[83] finger-scanning was introduced for time-keeping and ensuring office security. The Privacy Commissioner found the collection of personal data to be unnecessary and excessive.[84] This was on the basis that the employer failed to provide sufficient information to help employees understand the adverse impact on their privacy, and failed to implement adequate mitigating measures in relation to the system. The Commissioner observed that there had to be true consent, with no undue influence,[85] and stated:

> In situations where disparity of bargaining power exists, such as in an employer-employee relationship, any presumption of undue influence exerted on the part of the employer can be dispelled by the provision of genuine choices to the data subjects before they decide to provide their personal data.

No true consent had been obtained in the present case. A presumption of undue influence due to an employment relationship had not been rebutted; there was no free choice for employees to decline to provide their fingerprints to the employer; employees were not informed of the purpose of collection or of the availability of alternatives; and no balanced view was presented to employees to enable them to make an informed choice as to whether or not to provide their fingerprints to the employer.[86]

Similarly, in another case,[87] the Commissioner found that an employer's fingerprint scanning system constituted an unnecessary, excessive and unfair collection of personal information.[88] The complainant was a furniture installer and he was surprised that the employer collected and recorded his fingerprint data. The employer explained that it was for recording staff attendance. The employee apparently complained after he left his employment. The Commissioner found that there were less privacy intrusive options, such as passwords, available to the employer. Since there were 400 individuals subject to the system, there was a higher privacy risk due to possible breaches of information security. Because the employer could not reassure

[83] Office of the Privacy Commissioner for Personal Data (HK) *Case No 2008C04* (February 2009).
[84] In breach of DPP 1(1).
[85] The Privacy Commissioner referred to his publication on the topic, *Personal Data Privacy: Guidance on Collection of Fingerprint Data* (Office of the Privacy Commissioner for Personal Data (HK), May 2012), available at <www.pcpd.org.hk>.
[86] In the result, the Privacy Commissioner did not issue an enforcement notice because the employer subsequently offered its employees a less privacy intrusive alternative in the form of a password.
[87] Office of the Privacy Commissioner for Personal Data (HK) *R09-7884* (13 July 2009).
[88] In breach of DPP 1(1) and (2).

the Commissioner as to security concerns, the Commissioner found that there was a likelihood of accidental access or misuse of data. Moreover, the employees were not given sufficient information to form an informed choice as to whether or not to consent to the finger-scanning. There was also an evident element of informational "overkill", since there were also surveillance cameras to monitor against fraud in staff attendance. In addition, the Commissioner noted the disparity of bargaining power in the circumstances, which meant there was no freely given consent by the employees. The employer simply expected employees to cooperate by accepting the system without being offered an informed choice. Employees were threatened with immediate dismissal for failure to cooperate. The Commissioner observed that the scanning was merely for the employer's own administrative convenience, which could not justify such a compulsory collection of data. As a result, the Commissioner issued an enforcement notice to stop the collection of personal data in breach of the collection principles.

Wearable Devices

The new frontier of employment surveillance is the use of wearable devices. These devices measure or monitor bodily functions or activities, and have moved from mere consumer gimmicks for the health-conscious to being deployed for monitoring and maximising workers' health and performance. Some incorporate GPS systems to make monitoring of movements more precise, others have cameras to record what the wearer is doing or seeing. Blood glucose sensors are able to monitor eating habits. They can also measure sleep patterns. New developments are making wearable devices more useful and pervasive for a variety of workplace purposes, ranging from monitoring worker movement and conduct, monitoring and improving worker health and safety, picking up personal and environmental stressors, and performance optimisation.

For example, Fitbit is a company that manufactures a number of different wearables that can track activity, such as the number of steps walked, the quality of one's sleep, the number of steps climbed, and other personal metrics. This information can be combined with other information about the user to calculate distance walked, calories burned, heart rate, floors climbed, and activity duration and intensity. It can also measure sleep quality by tracking periods of restlessness, how long before the wearer falls asleep, and how long they remain asleep. These devices can be clipped to the wearer's clothing or worn as a bracelet. In one study, staff could be classified into two groups based on their shared patterns of behaviour: "busy and coping" and "irritated and unsettled".[89] Employers have been using such devices to "nudge" staff towards healthier lifestyles (particularly if they are contributing to their employees' health insurance),[90] and there can be incentives if certain activity targets are met. One

[89] Sarah O'Connor "Wearables at work: the new frontier of employee surveillance" (8 June 2015) Financial Times <www.ft.com>.

[90] For example, CVS Pharmacy in the US requires its 200,000 employees on health plans to submit their weight, body fat, glucose levels, and other health information or else pay a monthly fine of $50 to cover higher health insurance premiums: see Steve Osunsami "CVS Pharmacy wants workers' health information, or they'll pay a fine" (20 March 2013) ABC News <www.abcnews.go.com>.

of Fitbit's strategic goals is to penetrate this "corporate wellness market".[91] One advertised feature is that:[92]

> Employers who buy from Fitbit have the option of tracking their staff right down to the individual level, if staff agree to share their data, or just in aggregate. In other words, they can choose to see how many steps Bob in accounting is taking each week, or just how active the seven people in accounting are.

While promoting health and safety is one use of such devices, they can also be used to improve productivity or enhance performance. These functions inevitably mean that the information collected by the devices is to be accessed by the employer. They can be used to eliminate "sickies" if the employer is able to examine information collected by the device over the period that the employee claimed to be ill.[93] Employer use of such devices in some circumstances, however, may lead to employees "gaming the system"[94] through attempting to trick the technology by giving the wearable to someone else to wear who could produce the desired statistic, or by taking substances to produce a particular result. Wearables may also distract from productivity as employees become more concerned with producing favourable numbers. Wearables will normally require the employee's consent or cooperation. They can be perceived as highly invasive, and workers may well resent the constant monitoring that wearables involve.

Linking behaviour and physiological data collected from wearables to analytic tools can give employers in some industries an "edge", all else being equal. This area is known as "physiolytics", which is defined as "the practice of linking wearable computing devices with data analysis and quantified feedback to improve performance."[95] For example, a recent article has reported that some of the big hedge funds have been working to link physiological data to trading success.[96] As with athletes, such factors as diet and sleep can affect one's performance. Moreover, some hormones, such as naturally produced steroids and testosterone, can increase a person's confidence and encourage risk-taking behaviour, while stress hormones such as cortisol have the opposite effect. John Coates, a neuroscientist and former Goldman Sachs trader, is working with companies to link such biological signs to trading success. He has observed that:

> You need to figure out whether you should be trading or whether you should go home. If you are trading, should you double up your position because you're in the zone?…A lot of smart managers think their algos have gone as far as they can go. The next step is human optimization.

---

[91] See, for example, Parmy Olson "Fitbit on track to sell thousands more devices through Barclays, GoDaddy and other employers" *Forbes* (online ed, America, 20 October 2015).
[92] Olson, above n 91.
[93] Chloe Taylor "Wearable devices: the future of management?" *HRM New Zealand* (online ed, 15 June 2015).
[94] O'Connor, above n 89.
[95] H James Wilson "Wearables in the Workplace (2013) *Harvard Business Review* (online ed, Boston, September 2013).
[96] Olivia Solon "Why your boss wants to track your heart rate at work" (12 August 2015) Bloomberg Buisiness <www.bloomberg.com>.

The workplace privacy implications of such devices are obvious,[97] chief of which is whether or not the employee should be allowed to withhold consent to wearing such devices without any adverse repercussions. Furthermore, such devices will have security vulnerabilities. One commentator has remarked that "your personal data security is only as strong as the weakest link in your quantified ecosystem."[98]

Conclusion

There are three principal conclusions that follow from examination of the application of privacy legislation to the workplace. One is that such legislation is most important for providing employment law with a source of accepted standards of what society regards as fair and reasonable in relation to the handling of workers' personal information and their expectations of privacy. Secondly, it is clear that the effectiveness of privacy regulation as a control over employer practices very much depends on the particular country's data protection authority and the strictness with which it, and the legal forums above it, approach the interpretation and application of privacy law. Thirdly, the world is going to see more, not less, technological innovation that will have workplace applications, and so it behooves lawmakers and officials to actively defend and strengthen workers' human rights to privacy against managerial encroachment.

The modern day motivation for collecting personal information about workers can be traced back to the 'scientific' management techniques of Frederick Winslow Taylor at the turn of the last century. Underlying much of the perceived need for increased supervision was mistrust of the likelihood of workers doing an honest day's work. The current pairing of this outdated management attitude with increasingly sophisticated means of monitoring workers has resulted in a serious workplace imbalance. Meaningful regulation of this diabolical partnership – negative attitudes towards workers combined with technological advances – is not in prospect. Added to this mix has been the relatively recent extension of the common law duty of fidelity to capture worker conduct beyond the bounds of the workplace when what a worker says or does can be labelled as reflecting badly on the employer's business. The difference between today and Frederick Taylor's times is that the right to privacy enshrined in human rights instruments did not exist then, nor did the technological ability to monitor workers to the same pervasive degree.

[97] See International Working Group on Data Protection in Telecommunications *Working Paper on Privacy and Wearable Computing Devices* (Doc No 675.50.15, 57th meeting, Seoul, 27-28 April 2015), available at <www.datenschutz-berlin.de>; Research Group Report *Wearable Computing: Challenges and Opportunities for Privacy Protection* (Office of the Privacy Commissioner of Canada, January 2014), available at <www.priv.gc.ca>.

[98] Michael Carney "You are your data: The scary future of the quantified self movement" (20 May 2013) PandoDaily <www.pando.com>.