



Private Word

News from the Office of
the Privacy Commissioner

Following a decision of the Employment Court upholding Air New Zealand's right to test some employees for alcohol and drugs, the Privacy Commissioner has cautioned other employers to carefully consider the particular circumstances of that case if they are considering the introduction of a similar requirement. ROBERT STEVENS, who was counsel for the Privacy Commissioner, summarises the issues which arose in the case.

Facts determine scope of ruling

Last year Air New Zealand proposed to implement a new policy to carry out breath testing for alcohol and urine testing for drugs among its employees. The six trade unions whose members would be affected brought an action in the Employment Court challenging this policy, and the airline postponed implementation until the court ruled on the unions' claim.

The matter was seen as a test case, and was heard by a full bench of judges, Goddard, Travis and Colgan. (*NZ Amalgamated Engineering Printing and Manufacturing Union Incorporated and others v Air New Zealand Limited*, Employment Court, Auckland Registry, April 13, 2004, AC 22/04.) It is available at www.privacy.org.nz

The company's policy covered several different applications of

breath-alcohol and urine-drug testing, ranging from pre-appointment checks of job applicants, through to testing where there had been an accident or near-accident, testing prior to an internal transfer to a safety-sensitive post, and random testing of any and all employees.

The unions' challenge was three-fold. First, the policy was said to amount to a unilateral variation of the existing employment contract. This claim failed because the present contracts were silent on the question of drug testing, and the proposed policy was held not to be incompatible with the terms of the existing contracts.

Second, the plaintiff unions said that the policy was deceptive or misleading. This too was rejected by the court, which found that, to the contrary, the company had been direct and open about its intentions.

Third, the implementation of the policy was asserted to be unlawful and unreasonable. In this claim, the unions were partly successful.

The claim starts from the unchallenged proposition that an employer may give instructions so long as they are lawful and reasonable in the light of the employer's operation. It was alleged that the implementation of at least

● *Cont. on p.4*

Technology — it's everywhere

The Privacy Commissioner, Marie Shroff, has been "particularly struck by the huge developments, opportunities and risks in information technology and biotechnology," she told Auckland University students at a graduation ceremony.

"As a worker you will need to adapt to, exploit and master these; as a citizen you will need to do what is now called 'manage your identity'. You will move through a world where your every physical move, business transaction and life event will be both assisted and

invaded by technology," Ms Shroff said.

"Your challenge will be to manage and protect your personal dignity, information and identity within that complex information system."

The only constant in today's post-education world was change.

"Over your life you can expect to experience and be part of many changes — in technology, society, business and job opportunities," Ms Shroff told the graduates. ■

In this issue:

Drug test ruling	pp.1, 4
Technology challenge	p.1
Big brother awards	p.2
Complaints list	p.3
Act interpretation	p.3
Secret filming	p.3
APEC planning	p.5
Privacy tort	pp.6, 7
Mail opening	p.7
RFID tags	p.8
Educational role	p.8
Dog registers	p.8

Bouquets and brickbats handed out

The former Privacy Commissioner, Bruce Slane, and Assistant Commissioner, Blair Stewart, were joint winners of awards made by the Auckland Council Liberties for “long-term achievement, recognising long-term service to the protection of privacy.”

The judges, who were university lecturers and practising specialists in privacy law, said Mr Slane and Mr Stewart had formed a strong, cheerful and highly effective team over the first decade of the Privacy Act’s life.

“Bruce’s reputation as a Privacy Commissioner is without equal, as was so well represented in all accolades he received from home and abroad upon his retirement last year,” the judges stated.

Mr Stewart had always worked quietly alongside Mr Slane, they added.

“His encyclopaedic knowledge of privacy matters and his attention to detail have resulted in many small and large legislative changes to better protect privacy, and in the development of codes of practice, such as the Health Information Privacy Code, which are the envy of many other jurisdictions.

“Blair’s role in the process and production of the first review of the Privacy Act, in 1998, has also been of huge importance,” the judges stated. “His contribution to privacy in New Zealand has been, quite simply, vast.”

Other “Big Brother” awards made at the ceremony were not so flattering.

Auckland University law lecturer Tim McBride said the awards had been established to give well-earned prominence to people and organisations who had exhibited outstanding negligence or disregard for the public’s right to privacy. They would be an annual event.

“We predict that there will be a steady supply of individuals and organisations that stand out for special public recognition as Big Brother Award winners in future years,” Mr McBride said.

Joint winners of the Person of the Year Award, for “outstanding abuse or disregard of privacy and civil liberties in New Zealand”, were all the ministers and politicians responsible for recent new anti-terrorism and surveillance legislation in New Zealand.

The legislation “allows additional, secret snooping — with little or no public accountability — into the private lives, transactions and communications of New Zealanders,” the judges stated. “While falling mercifully short of the United States Patriot Act, these various pieces of legislation result in significantly reduced privacy and civil liberties for all of us, but do little to reduce any actual terrorist threat.”

The Minister of Justice, Phil Goff, received an award for “the elected representative who has most neglected or abused their responsibilities to protect privacy”, for his part in fronting the counter-terrorism legislation. The Minister of Telecommunications, Paul Swain, was “a close runner-up” for “uncritically” pushing through new surveillance powers.

The Government Communications Security Bureau (GCSB) was declared the “government agency that has most systematically invaded privacy” for its surveillance work, “notably targeting our Pacific neighbours.”

Baycorp was declared the worst corporate organisation for its “history of failure to correct [credit record] information, even where blatant mistakes are made, and charging what many see as an unreasonable amount for people to access their own credit records.”

The judges gave public registers a “long-term menace” award, saying that although many registers fulfilled a necessary function, there was a vast amount of cross-checking among them and access to them was often unrestricted by reference to the purpose for their existence.

Professor Peter Wills, of Auckland University, received a congratulatory award for the stand he had taken against the proposed use of personal information in research conducted by the Tertiary Education Commission. ■

DIRECTORY

The Privacy Commissioner has offices in Auckland and Wellington

Commissioner: Marie Shroff

Assistant Commissioner: Blair Stewart
Manager Investigations: Phillipa Ballard
Senior Legal & Communications Adviser: Annabel Fordham

Auckland:

Tel: 09-302 8680 Fax: 09-302 2305
email: enquiries@privacy.org.nz

Wellington:

Tel: 04-474 7590 Fax: 04-474 7595
e-mail: enquiries@privacy.org.nz

Auckland privacy enquiries, telephone 302 8655

For enquiries from other areas, call the enquiries line: 0800 803 909

Postal address:

Privacy Commissioner, PO Box 466
Auckland 1, New Zealand

Website:

<http://www.privacy.org.nz>

Private Word— Not “The Word”

This newsletter is an informal newsy way of communicating the work of the Commissioner’s Office. Much of the material reported is truncated. Some is not qualified by reference to exceptions and to the different contexts in which matters can arise. Even statements attributed to the Commissioner may be drawn from longer documents or inapplicable to all situations. No legitimate expectation is created as to how the Privacy Commissioner will view or may deal with any specific set of circumstances by any material in Private Word. If it is intended to rely on anything in Private Word, confirmation should first be sought from the Commissioner or independent legal advice obtained.

Police, ACC draw most complaints

Eight out of the nine agencies against which most complaints were made last year to the Privacy Commissioner are government bodies.

As in the past, the Police, with 72 complaints against them, and ACC with 68, were the top two respondents.

The Police total was 26 per cent more than last year and ACC 36 per cent more - increases which cause concern because of their impact, the annual report to Parliament stated.

The top nine respondents account for 34 per cent of all complaints received. Some of the complaints will be reviews of requests for access — and these agencies tend to be large repositories of personal information. But they also reflect policies over which the Privacy Commissioner's office has no control.

The annual report noted that many of the complaints against ACC result from a breakdown in relationships often arising from the termination of long-standing benefits.

Noting that Baycorp is the only private sector agency on the list, the commissioner indicated concern about the use of credit data for purposes other than providing credit. A code of practice for credit agencies was to be issued.

The top nine respondents, with the number of complaints against each, were:

Police 72, ACC 68, Ministry of Social Development 36, CYFS 32, Department of Corrections 31, Baycorp Advantage 26, NZIS 21, Department for Courts 16, Capital and Coast DHB 10. ■



Upset over starring role

It came as a shock to a television repair man when he was told that he had been secretly filmed while he was on a job and that he was to feature in TV3 consumer affairs programme *Target*.

The repair man had been met at the house by a woman he believed to be the householder, but who was actually an actor. She left the house shortly after explaining the problem with the television set.

The TV production company told the technician he could view the unedited tape and provide any comments before the programme was screened. He was not, however, given the right to view the edited programme, and he felt he could not adequately respond without seeing the edited tape.

The repair man complained to the Privacy Commissioner, saying that the covert taping and subsequent broadcast (which he believed would be misleading as a result of editing the footage) amounted to an interference with his privacy.

The Privacy Commissioner, however, formed the opinion that the programme fell within the category of news and current affairs and was thereby specifically excluded from the provisions of the Privacy Act.

The technician would have been entitled after the broadcast to complain to the Broadcasting Standards Authority if he thought that the item breached broadcasting standards, including those concerning privacy.

Court clarifies interpretation

The High Court has issued a ruling which makes it clear that s.66(2) of the Privacy Act, describing actions which constitute an interference with privacy when access to personal information is requested, stands alone. Adverse consequences or harm set out in s.66(1)(b) are not required.

The court, which had been hearing the case of *Winter v Jans*,

upheld the long-standing view of the Privacy Commissioner concerning the correct interpretation of the section.

The Human Rights Review Tribunal had previously ruled otherwise — that is, that harm had to be established, as described in s.66(1)(b), before a finding of interference with privacy principle 6 could be made. ■

Continued from page one

Facts determine scope of ruling

some aspects of Air New Zealand's policy would be a breach of statute and common law, and an unreasonable imposition upon the employees.

Part of this argument alleged that the policy would breach the Privacy Act, or would be a tortious breach of common law privacy rights. The two parties were directly opposed on this head of the argument, and the court invited the Privacy Commissioner to assist the court with submissions on these points.

The commissioner's submissions are set out at some length in the court's judgment. As to the tort of privacy, the commissioner submitted that the position of New Zealand law was unclear at that time (the High Court in *Hosking* had cast doubt on earlier authorities, and the Court of Appeal's judgment in that case was still awaited) but that the only part of the American tort of privacy actually at issue in the *Hosking* case was not applicable to the Air New Zealand case because here there was to be no "public disclosure of private facts".

The commissioner said New Zealand courts had not yet recognised the tort of privacy in cases not involving disclosure. The Employment Court's judgment was issued soon after the Court of Appeal's judgment in *Hosking*, and refers to it. The court held that the Air New Zealand drug testing policy raised no issue with the tort of privacy as recognised by the New Zealand courts to date.

The Privacy Commissioner submitted that the Employment Court did not have jurisdiction to decide that any action was or was not an interference with the privacy of the individual in terms of the Privacy Act because that was the exclusive province of the Privacy Commissioner's opinions and the Human Rights Review Tribunal's decisions.

Nevertheless, the Employment Court could properly consider the extent to which the company's alcohol and drug testing policy appeared to involve breaching the Privacy Act's provisions, so as to take this into account in judging whether the company's actions were lawful and reasonable.

The commissioner submitted that it seemed the policy could generally be operated in a manner consistent with the Act's provisions, except that there were potential problems under information privacy principle 1 in the random testing of employees who did not work within "safety sensitive areas."

(Principle 1 provides that an agency may not collect personal information unless the information

Random testing only for employees in safety-sensitive jobs

is collected for a lawful purpose connected with a function or activity of the agency, and the collection is necessary for that purpose.)

The commissioner submitted that the need to collect personal information by random drug and alcohol testing in any individual case, in the absence of accident or other cause to suspect consumption of (and impairment by) alcohol or drugs, was open to doubt where the employee concerned was not in a job exhibiting particular sensitivity to such impairment.

An argument often raised in relation to the present technology for drug testing is that even a positive drug test result does not prove actual impairment. The airline pre-empted this by arguing that a positive result showed that the individual had consumed the drug and so was more likely than others

to do so again and was more likely than others to be impaired by drug use in future.

The court had to weigh the intrusive nature of drug testing procedures against the employer's need to know the test results in order to operate its business safely and efficiently. It held that both breath-alcohol and urine-drug testing were warranted for use by the airline in:

- a. pre-employment testing for any job applicant;
- b. testing of any employee "for cause";
- c. testing of any employee involved in an accident or incident;
- d. pre-transfer testing for appointment to a job in a safety-sensitive area; and
- e. random testing of employees working in a safety-sensitive job or area.

The court held that it was not lawful and reasonable for the airline to require random testing of employees whose jobs were not safety-sensitive. This part of the policy had to be removed before the proposed policy could lawfully be implemented. The airline was also required to negotiate with the unions to achieve a better demarcation of safety-sensitive positions. The judgment stresses that it is limited to the facts and circumstances before the court.

● *The Privacy Commissioner notes that New Zealand employers contemplating the introduction of alcohol and drug testing would do well to bear in mind the fact that this is a major passenger airline, to consider the particulars of the test procedures and protocols to be applied by the company, and also to note the details of Air New Zealand's "just culture" policies and procedures for dealing with matters of staff training and discipline.* ■

N.Z. role in working out details

APEC's Electronic Commerce Steering Group (ECSG) convened a series of meetings of senior officials in Santiago in February 2003. Blair Stewart, the Assistant Privacy Commissioner, participated in the deliberations of the data privacy subgroup meeting, which completed the initial work on the data privacy principles and

in a further meeting of the ECSG itself which dealt with that item and others of interest such as regulating spam.

Additionally, Blair Stewart delivered a paper to an APEC Symposium on Data Privacy Implementation Mechanisms on the subject of cross-border cooperation

on enforcement matters.

The paper canvassed the principal international instruments and included illustrations of current cross-border cooperation within the APEC region. A number of suggestions were made to APEC as to how useful cooperation might be encouraged.

Developing regional privacy framework is an ambitious project for APEC

After decades of international privacy standard setting in Europe, the spotlight has now turned to our own vast region.

APEC – whose members span the Pacific from Russia and Asia through to Canada and South America — has set itself the ambitious task of developing a regional privacy framework. This is not entirely straightforward given the diversity of legal systems and approaches to data protection.

APEC's Electronic Commerce Steering Group (ECSG) recognises that lack of consumer trust and confidence in the privacy and security of on-line transactions is one element that may prevent member countries from gaining all the benefits from electronic commerce.

The idea is that having good common standards for the protection of information privacy, with mechanisms to ensure that they are adhered to, will tempt individuals into engaging in the exciting possibilities of the information age.

In early 2003, the ECSG established the APEC Data Privacy Subgroup, comprising officials and experts from 10 countries, inclu-

ding Blair Stewart, the Assistant Privacy Commissioner.

Blair Stewart acts as an expert adviser to the New Zealand delegation which is led by the Ministry of Justice (taking on this role from the Ministry of Consumer Affairs) and involving the Ministries of Economic Development and Foreign Affairs and Trade.

The first year of the project was devoted to developing a set of privacy principles. The starting point was the 1980 OECD Guidelines on the Protection of Privacy and Transborder Data Flows upon



Blair Stewart

which New Zealand's Privacy Act is based.

The subgroup worked through more than eight drafts of the principles in its attempts to redefine them for our region and to find a consensus. The work was conduc-

ted in exchanges of emails, teleconferences and only occasional meetings.

The project reached a significant milestone in February 2004 when the draft principles were presented back to the ECSG at a meeting in Santiago.

The ECSG released the principles for consultation amongst all APEC members and for wider public consultation. The draft principles are available on the ECSG website at www.export.gov/apececommerce.

They focus upon:

1. Preventing harm
2. Notice
3. Collection limitation
4. Uses of personal information
5. Choice
6. Integrity of personal information
7. Security safeguards
8. Access and correction
9. Accountability.

The subgroup has now turned its attention to a companion part of the proposed privacy framework which would provide guidance on matters of implementation.

This may touch upon issues such as transborder cooperation in dealing with emerging privacy problems or resolving complaints.

New Zealand's own tort of privacy — why?

KATRINE EVANS, Senior Lecturer in Law at Victoria University, outlines the recent Court of Appeal case involving television presenter Mike Hosking, his former wife Marie, and their twin daughters. The Hoskings were trying to gain an injunction to prevent New Idea publishing photographs taken of the twins in a public street without their parents' consent. The Hoskings' injunction application failed, but the majority of the Court of Appeal found that a tort of privacy did exist in New Zealand law.

Tort law is not necessarily the most practicable vehicle to protect privacy. The costs are very high, for plaintiffs and defendants alike; there are few precedents, which makes the outcome uncertain; and people have to be prepared to go to court, a public forum, to ask for privacy protection – without the guarantee of name protection.

Add to that the stress, time and trouble of appearing in court, and it is unsurprising that so few people are willing to take action. So should we have a tort at all?

First, to answer in the affirmative (as I do) one has to argue that privacy is a separate and coherent concept, capable of sufficiently certain definition to be protected by law.

This is hotly disputed by some, though privacy does receive considerable protection in international law instruments.

Secondly, protection of privacy must not already be completely provided by other areas of law including common law and statute.

Thirdly, it is important to carefully consider the interface between privacy and other important social interests, such as freedom of expression, public safety or law enforcement. Any impact of one on the other must be shown to be necessary and justifiable — and that impact should be minimised.

Fourthly, appropriate remedies need to be available to a successful plaintiff, in order to fulfil the objectives of having the cause of action in the first place.

The Court of Appeal in the case of *Hosking v Runting* was faced with

all these questions. The two minority judges, wary of a lack of coherence in the concept of privacy, argued that sufficient protection was given elsewhere in law (including in the Privacy Act), and concluded that privacy protection was an unjustified limitation on freedom of expression.

The three majority judges, though, decided that a publisher could be liable in tort if he or she published facts in relation to which there was a “reasonable expectation of privacy” and where the “publicity given to those private

Photographs taken in a public place were not embarrassing ...

facts ... would be considered highly offensive to an objective reasonable person” [para 117].

They gave considerable weight to the fact that privacy is protected in international law instruments, to which New Zealand is a signatory.

Also highly relevant was the now quite considerable body of law from overseas – much of it involving celebrities — in which privacy interests, by one name or another, have been recognised. Their Honours recognised the fact that related areas of law in New Zealand do not entirely provide protection for unwarranted publicity about people's private lives.

However, all the judges were unanimous that the Hoskings failed in their attempt to get an injunction preventing publication of photographs taken without consent of their baby twin daughters. The

photographs were not at all embarrassing, and were taken in a public place.

The *Hosking* case is the latest in a not particularly long line of privacy cases in New Zealand. The most famous are *Tucker v News Media Ownership* (publication of a man's past criminal record); *Bradley v* [the now very famous] *Wingnut Films* (a family monument used as a brief backdrop to a splatter movie scene in a cemetery); *Morgan v TVNZ* (publication of facts about an eight year old girl at the centre of an international custody battle); *Marris v TV3* (surreptitious filming of a doctor involved in a misdiagnosis case, early in the morning, simply to portray his refusal to be interviewed); *P v D* (a public figure with past history of mental health problems which the person wished to keep private); and *L v G* (consensual, highly intimate photographs involving an unidentifiable prostitute, which her client then had published in an adult magazine without her consent).

While the plaintiffs have not always succeeded (Tucker, the Bradleys and Marris all lost, though for very different reasons) the cases do illustrate the variety of situations in which privacy arises and that the tort has a lot of weight to bear – hence the need for maximum clarity, but also reasonable flexibility. The *Hosking* test goes some way towards fulfilling these requirements.

The test which the Court of Appeal has developed is, importantly, subject to a defence that it is in the public interest to publish the information in question. Public

● *Cont. on p.7*

Continued from page six

NZ's own tort of privacy — why?

interest is not defined, but incorporates some consideration of “what the public is legitimately entitled to know”.

It was just as well for *New Idea* that the court decided there were no reasonable expectations of privacy to protect, and that publicity of photos of the children in their push-chair would not be highly offensive.

Pleading that there is a viable public interest in publishing essentially gossip information about a celebrity or his family can be extremely difficult.

The exceptions are situations where there is some element of correcting hypocrisy (as with Naomi Campbell, publicly stating that she did not take drugs — a statement which the press was entitled to correct); or an impact on the person's ability to do his or her job (for example political credibility); or because the person had consented to that sort of information being publicised before (a point that was raised, but failed, in *Hosking* itself).

Even where there is no public interest in the individual item of information, though, the court must take account of the more general public interest in being able to publish and receive information (freedom of expression, as recognised in section 14 of the New Zealand Bill of Rights Act 1990).

Wider considerations of preserving freedom of expression are essential with any cause of action that involves placing constraints on publication — whether that be defamation, breach of confidence, contempt of court or breach of privacy.

Equally, though, courts cannot and should not ignore the public interest in preserving privacy, confidentiality, reputation and so on. Rules have to be worked out which ensure that important human rights such as privacy and freedom of expression each constrain the other to the least possible extent, on the occasions when they happen to conflict.

The way in which our Court of Appeal has ultimately resolved this balancing test has not, however, been completely beneficial for privacy. To properly protect freedom of expression, the court — unanimously — found it necessary to say that injunctions preventing publication would only be granted in very rare circumstances, where it was very evident that there would be a breach of privacy (according to the test above) and where there was obviously no public interest at stake.

This reverses the previous position where, to get a pre-trial injunction, a plaintiff only had to prove that there were potentially valid arguments to be made in privacy and that there would be no undue disadvantage to the defendant, or to other interests, from the grant of the injunction. This usually had the effect of maintaining the status quo until the matter could be resolved by full argument at trial which preserved the plaintiff's privacy at least in the meantime.

In an area of law where publication *is* the damage (because privacy is then irretrievably lost) this ruling therefore removes the major benefit of using the tort at all.

Consequently, while it raises points of major academic interest, the tort is likely to have little impact on the ordinary citizens of New Zealand. Not only are the barriers to using it extremely high, but its potential for real usefulness has been curtailed.

Perhaps — as is largely the case in the United Kingdom — privacy law will be increasingly be seen as a vehicle for celebrities to protect their images, since they are the only ones who can afford (in all senses) to go to court.

Media stars and media freedom have both, perhaps, been the winners as a result of the *Hosking* litigation. ■

Who's to open mail when boss is away?

The letter from the Ministry of Social Development was addressed to the manager, but he was away at the time, so it was opened by another staff member.

Inside was a notice instructing the firm to deduct money from the wages of an employee who had received a benefit overpayment. She objected to the Privacy Commissioner.

Knowing that the notice would be coming to the firm, the employee had asked that it be addressed to the pay clerk.

However, the Ministry's usual practice is to send such notices to the manager, normally after explaining this to the person concerned.

The Ministry had no record of whether there had been such a conversation, but told the Privacy Commissioner that notices went to managers in order to avoid problems which had arisen in the past, where the person subject to the notice was in fact the pay clerk, or where the relationship between the pay clerk and the employee had led to steps being taken to avoid deductions being made.

Denying its actions had interfered with the employee's privacy, the Ministry told the Privacy Commissioner that it could not be held responsible for employers' mail-opening practices, and that the same issue could have arisen if the pay clerk had been absent from work.

However, the Ministry now marks envelopes sent to managers “Private and Confidential”.

The Privacy Commissioner passed on the Ministry's comments to the complainant, who did not ask for any further action to be taken.

Tags have major implications for privacy

Bar codes may be on the way out, replaced by tiny micro-chips called radio-frequency identification (RFID) tags. Most operate without batteries, listening to radio signals sent by transceivers and using the signal's energy to reflect and answer.

Applications include "smart shelves" in stores managing the supply chain, payment at check-outs linked to credit cards, theft reduction, document tracing and bank note authentication.

RFID tags have the potential to collect information about people, linking information with existing data bases, and to track the movements of a person who possesses or handles tagged objects.

An international conference on data protection has drawn up a list of basic privacy principles which should be taken into account when designing or using products with RFID. They propose that:

◆ Any controller, before introducing RFID tags, should first

consider alternatives to achieve the same goal without collecting personal information or profiling customers;

- ◆ If personal data are indispensable, they must be collected in an open and transparent way;
- ◆ Personal data may only be used for the purpose for which they were collected, and retained only as long as necessary; and
- ◆ Whenever RFID tags are in the possession of individuals, they should be able to delete data and disable or destroy the tags.

My date of birth — why do you ask?

When a man registered his dog, the council asked for his date of birth. Why? he asked. What authority did they have?

And another thing – who's going to be given that information? The man complained to the Privacy Commissioner.

The answer lies in the Dog Control Act 1996, which stipulates that territorial authorities must keep a register of dogs and that it must contain the name, date of birth and address of the dog owner. So, be-

cause it's a statutory requirement, the council did not breach the Privacy Act by asking for the owner's date of birth.

The Dog Control Act also provides that certain people, like police officers and SPCA inspectors, are entitled to be given details from the register.

Other people can ask for the name and address of dog owners, but not their date of birth. However, there is a presumption in favour of non-disclosure of information from dog

registers (unlike some other public registers, which the Privacy Commissioner would like to be subject to more stringent safeguards against improper or inappropriate information-gathering).

An application for a name and address from the council's dog register must be made on a specified form and be for a specific purpose, such as alleging an offence against the Animals Protection Act, claiming compensation for damage to property by a dog, or returning a dog to its owner. ■

Education role is important

Education plays an important part in the role of the Privacy Commissioner. In the 2002/03 year, the office provided 45 workshops and seminars for people including privacy officers, front-line staff and legal advisers. Tailored workshops were held for health, insurance and university staff.

Workplace training is a two-way process, with participants learning about the Privacy Act and code and the complaints process, and the commissioner's staff members meeting people who have to deal with Privacy Act requests or make decisions on disclosing information. ■



The Privacy Commissioner, Marie Shroff, is invested with the award of Companion of New Zealand Order of Merit (CNZM) by the Governor General, Dame Silvia Cartwright. Mrs Shroff was Secretary of the Cabinet and Clerk of the Executive Council for 16 years.