

PERSONAL INFORMATION IN NEW ZEALAND: BETWEEN A ROCK AND A HARD PLACE?

KATRINE EVANS
ASSISTANT COMMISSIONER (LEGAL)
OFFICE OF THE PRIVACY COMMISSIONER, NEW ZEALAND

16 MAY 2006

Personal information is a key concept in data protection statutes, including our own. But deciding what is, and what is not “personal information” can be one of the hardest legal calculations in everyday privacy practice.

Personal information is defined in section 2 of the Privacy Act 1993 as:

“information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, and Marriages Registration Act 1995, or any former Act.”

“Individual”, in turn, is defined (again in section 2) as:

“a natural person, other than a deceased natural person.”

On occasion, health information about a deceased person is covered by the Health Information Privacy Code, (coupled with the Health Act). For example, the representative of a deceased natural person will in many cases have a right of access to personal health information about the deceased. However, representatives do not have a right to correct personal information about a deceased person.

“Information” itself is not defined. New Zealand’s leading authority on the meaning of information is *Commissioner of Police v Ombudsman* [1988] 1 NZLR 385, 402. The Court of Appeal in that case defined information as “that which informs, instructs, tells or makes aware.” It is not limited to documentary information but can even encompass information in the mind of a person (*Re application by L: information in a person’s memory* – an early Tribunal decision).

The New Zealand definition of “personal information” is therefore extremely wide. In fact, it might be easier to say what it is not:

- It is not information about a company (the corporate veil stays firmly drawn);
- It is not information about an organisation (unless it is also information about a particular individual within the organisation);
- Information that is not capable of identifying an individual is excluded;
- With very limited exceptions, information about deceased individuals is excluded.

Corporate information

The boundaries of what is ‘corporate’ information were tested in the early case of *C v ASB Bank Ltd*. The complainant, C, was engaged in a matrimonial property dispute with his estranged wife. He also ran a company (as sole shareholder and director), whose accounts were held with ASB Bank. His wife obtained access to some of the company bank account statements. Unfortunately for C, he had also used the company bank account for personal transactions; when his wife saw the bank

statements, she was able to find out information about his personal spending. The bank was aware that C used the accounts for personal transactions.

The issue for the Tribunal was therefore whether the bank disclosed personal information about C as well as information about his company. The company and personal transactions were, to some extent at least, visibly different. However, the Tribunal decided that it could not sever the personal information from the company information. The bank statements were in the company name, and the company was responsible for the account. It was all, therefore, information about the company, even if C had chosen to use that account for personal expenses. The Tribunal's view was that it could not lift the corporate veil and undo the certainty of over a century of company law by severing the information.

Some commentators and lawyers argue that corporate information is not so very different from information about individuals. Protection of that information from unwarranted disclosure serves similar ends to protecting information about individuals, argues Alan Westin in his book *Privacy and Freedom*. Corporations, like individuals, need privacy to contemplate decisions, and decide on future directions. They need to protect their interests (for example as regards trade secrets). Some members of the High Court of Australia (particularly Justice Kirby) have also expressed interest in these types of arguments (see *Lenah Game Meats*).

The New Zealand Parliament, however, has taken the view that privacy as such can only be enjoyed by natural persons. The interests of corporations are protected through such tools as breach of confidence, including trade secrets law, and intellectual property. Privacy, as a legal mechanism, is reserved for those with feelings to damage, and with human dignity to protect.

Information about organisations

Information about non-incorporated bodies can sometimes be personal information, if the information is actually *about* an identifiable individual. An example would be information about a sole trader's business – it may well be that information about that business would be information about the sole trader himself or herself. However, other situations are less certain. For example, information about a trust may or may not be information about the trustees.

Some guidance can be gained from considering defamation law here. Defamation requires the defamatory statement to be made *about* the plaintiff and has produced some useful cases to illustrate the point. For instance, in the *Knupffer* case, information about a political party was not information about the plaintiff: the party, though a fairly small group, had too many members for any reader reasonably to believe that the statements had been made about the plaintiff. It is difficult to produce a clear rule from such cases – a test that “the smaller the group, the greater the risk of a reader thinking the statement is about the plaintiff” is somewhat trite. However, it is difficult to do much better: each case simply (though unhelpfully) has to be judged on its own merits.

This therefore remains a contentious area in our investigations' jurisdiction.

Information that is not capable of identifying an individual

We had an interesting complaint recently (which we are case noting) on this question. The complainant was visiting an art gallery. A photographer was at work in the gallery, taking photographs of the paintings and some of the photographs were

later published. One of them showed a back view of a figure looking at one of the paintings. That figure happened to be the complainant – and the complainant recognised himself. He was upset at the fact that the photograph was taken without his consent.

However, his face was not visible, his clothing and his stance were not distinctive, and he was not the focus of the shot. Indeed, it was even difficult to determine if the figure was male or female from the angle at which it was taken. We therefore decided that this was not personal information. Although he recognised himself because he knew he had been in the gallery at that time, others would not be able to see that it was him. As a result, the photographer in this instance had not breached the privacy principles.

Perhaps the photographer was just lucky that he did not identify the man. It is not particularly good practice to take photographs of a person without their consent, at least where obtaining consent for use of the photograph is practicable. There are ways of informing the public that photography is occurring, even in public places (see our case note from March 2006 on photography in a shopping mall). We use complaints such as this to assist photographers and others to better understand their responsibilities and reduce their risks in future. However, we cannot find a breach of a principle unless the person is actually identifiable.

But when is a person identifiable? When can they recognise themselves? When members of their family or close friends can identify them? When more casual acquaintances or even strangers may recognise them?

There are some useful decisions from New Zealand's Broadcasting Standards Authority ("the BSA") on this issue. The BSA requires that the person be identifiable beyond their intimate friends or family before it will find that the privacy standard has been breached (see also *Proceedings Commissioner v Commissioner of Police* (16 December 1999, CRT decision 37/99 which reaches a similar conclusion). This is not uncontroversial, however. Again, it depends on the circumstances. The complainant may particularly want to keep the information from his or her close family and friends, for example. There can be a significant level of harm from such disclosures.

Limiting the concept of identifiability may make greater sense in the broadcasting context than in the data protection context. Concerns over freedom of the media may require a limit on how far the media should have to anonymise a person. It is extremely difficult both to successfully disguise a person from those who know them well, and also to ensure that those who know them well cannot guess their identity from the content of the story. Complete anonymity may be unachievable.

In the data protection context, on the other hand, one can afford to be more lenient in calculating when a person is identifiable. Identifiable means identifiable – at least if the person can be recognised by others than themselves (again, there are parallels with identification of the plaintiff in defamation law here). The limitations lie elsewhere in the law – for instance, in the requirement for harm in section 66, in the family affairs exception in section 56, in the exceptions within the principles themselves, in the definition of disclosure, and in the defence provided by section 126(4). Those limitations, or combinations of them, should ensure that agencies are not unreasonably found liable for breaches where the person was identified only to those who were extremely familiar with them, or with their situation.

The requirement for the individual to be identifiable is central to the concept of privacy in the Privacy Act. Again, however, this is not universally accepted, as is

illustrated by the privacy tort case of *L v G*. G took intimate close-up photographs of L during their sexual relationship, with L's consent. L was not recognisable from the photographs, even to herself. However, when G later published the photographs without L's consent (still without identifying L) in an adult magazine, she sued him successfully for breach of privacy in tort. Judge Abbott in the District Court took the view that non-consensual publication of intimate photographs was so offensive to L's dignity that she was entitled to succeed. He awarded her \$2,500 damages, the first damages award under the New Zealand privacy tort. This was on the grounds that G published private facts about the plaintiff (a similar concept to that of personal information, at least as far as it is relevant to this paper).

Information about deceased individuals

In privacy, as in defamation, arguments surface periodically about whether the dead can suffer a loss at all, let alone a remediable loss. Built as it is on such concepts as human dignity, sense of self, control over information and so on, it is difficult to see how the dead can enjoy a right to privacy as such. They are past caring – though their relatives are not.

The United States has taken tentative steps in some jurisdictions to creating a hereditary right of privacy, at least as far as appropriation of personality is concerned. The Australian Law Reform Commission and the McKay Committee on Defamation in New Zealand both considered (briefly) whether to allow estates to sue for defamation for a limited period after death, but the law did not change to permit this.

The rule, therefore, is that unless relatives are themselves identifiable from the information (so that the information is *about* them, not just about the deceased person), it is not personal information in New Zealand. There are some limited exceptions in the health arena, or as regards information on the Register of Deaths, as mentioned above. Privacy interests of deceased people can also be protected to some extent when a person requests access to information (section 9(2)(a) of the Official Information Act 1982 and section 29(1)(a) of the Privacy Act both provide withholding grounds where privacy of another (including a deceased person) might unjustifiably be compromised.

One case from the BSA indicates that, in exceptional circumstances, the BSA might be prepared to consider whether publication of information about a dead person might breach its privacy standard. This is despite the fact that, under the Broadcasting Act, the definition of privacy of the individual is specifically linked to the definition in the Privacy Act and therefore shares all its characteristics. The case involved publication of photographs of the body of a child, who had been beaten to death by a family member. The photographs, which screened on national television, showed his injuries. The child was Maori, and the complainants were also Maori. They argued that photographing a body was culturally unacceptable to Maori, and that this was part of the Maori concept of privacy.

The BSA took expert advice from a senior Maori adviser within the Ministry of Maori Affairs. On balance, the advice was that the public interest (in highlighting the case and therefore preventing further abuses of this nature) outweighed the privacy interest and therefore the public interest defence should succeed. Interestingly, though, the BSA did not firmly decide that privacy was irrelevant. Where particular cultural issues are at stake, it is therefore possible that there will be some flexibility. Against that, however, is the current unambiguous definition, excluding deceased natural people.

So what *is* personal information?

If that is what personal information is not, we are still left with the difficulty of what information *is* personal information. Usually, this requires an analysis of when information is truly *about* an individual, and when it is not.

A few years ago, in the only Privacy Act case to reach the Court of Appeal thus far (*Harder v Proceedings Commissioner* [2000] 3 NZLR 80), the majority considered (fortunately *obiter*) that personal information was, essentially, sensitive information. The case involved two tape-recorded conversations between a lawyer and a caller to his office (the former partner of his client, who was seeking a settlement of their dispute). The tape had gone missing, so the Court could not listen to what was said. However, it appeared that the conversations did not involve any highly sensitive information – instead they dealt with such matters as who could keep items of furniture.

Their Honours found it hard to believe that Parliament would have meant the definition to cover such conversations - they considered that having a very broad definition of personal information would lead to perverse results and open floodgates. “An unqualified approach to what constitutes ‘information about an identifiable individual’ will lead readily to breaches of one or more of the information privacy principles.” [23] In their discussion, however, they did not take account of the other limitations in the Act (a particular omission was the harm requirement in section 66 before a breach could be found). Also, with respect, they misunderstood both the intent behind the statute and the scheme of the Act – they did not interpret the Act as a whole.

Since the comments were only *obiter*, subsequent Tribunal panels have not had too much difficulty in avoiding the restrictions of the Court’s suggested approach. It is perhaps not overly cynical to suggest that they dutifully acknowledge the persuasiveness of the statement (because of its source) and then move to distinguish it as rapidly as possible (see for example *Apostolakis v Sievwrights* (14 February 2005) HRRT 44.03 at para 57. If the Tribunal had truly accepted the *Harder* approach, the result in the *Apostolakis* case may well have been very different – at the very least, the reasoning would have focused firmly on the sensitivity or otherwise of the information).

However, abandoning *Harder* still does not resolve the matter of when information is about a particular individual. In two recent cases, the Tribunal has had to address the point directly.

The first was *CBN v McKenzie Associates* (30 September 2004, HRRT 020/04, available on www.nzlii.org). The complainant requested a copy of his file, held by his solicitors. The file involved a dispute over care and protection of CBN’s son (he was in dispute with his former wife). The solicitors refused to give him a copy of the file because his account was unpaid. The solicitors later accepted that they should not have dealt with his request in the way that they did (the fact a bill is unpaid is not a valid ground to withhold requested information under the Privacy Act). The case largely concerned what remedy might be justifiable in the circumstances; the arguments focused on what harm, if any, CBN had suffered as a result of the defendants’ refusal of access.

As part of that discussion, however, the Tribunal considered whether CBN’s file was in fact personal information about him. The file itself was not available at the hearing.

However, the plaintiff accepted that it contained different types of information [para 30]:

- Information about his former wife (especially information about her living arrangements and the circumstances in which his son was placed when he was in her custody;
- Information about the mother's new partner;
- Perhaps information about the plaintiff's concerns about how his son might be treated by that man;
- Information about the plaintiff himself (some, but not necessarily all of which would have come from him in the first instance).

The information was "readily retrievable by reference to the plaintiff" (the test applied by an earlier Tribunal), because the file had his name on it. However, the Tribunal in this case adopted a more restrictive view. Not all the information on the file would actually be *about* the plaintiff, as illustrated by the list above. The Tribunal implicitly accepted that the agency would have to consider the file on a document-by-document basis (which can be an onerous exercise). Counsel raised an analogy:

[37] Suppose the price of a publicly listed stock is \$5. There is nothing about that information that could be described as 'personal' information about anyone. But now suppose that an individual has 20 shares in the company in question.

Does the share price become personal information, by association with the fact that the person has 20 shares? The Tribunal did not believe so. "[39] ... surely the personal information is the fact that the individual owns 20 shares, and not the fact that [the] publicly listed share price is \$5." "With respect" they continued at para 40:

"[t]he fact that information may become relevant to someone does not necessarily convert it into personal information 'about' that person. In the present case, for example, we think it safe to assume that the defendants' file for the plaintiff contained information about his former wife. That information may have been relevant to the plaintiff in the sense that it might either have limited or enhanced his chances of obtaining the custody arrangements that he wanted, but for all that we struggle to see that the information about his former wife thereby became personal information about the plaintiff."

They accepted that there was no bright line test: there might be factors indicating that though the person is not named in the information, there is a "sufficient connection" to justify a conclusion that it is personal information about that person. [41]

The difficulties of achieving anything approaching a bright line test were evident again in the case of *Apostolakis v Sievwrights* (14 February 2005, HRRT 44/03, **under appeal**, also available on www.nzlii.org). However, in that decision, the Tribunal found the "sufficient connection" to define the information as personal information.

This case again involved a request for access to information. The main issue was whether the defendants should have been able to withhold access to a particular letter. The defendants were her solicitors and wrote the letter to the mortgagee of a building that the plaintiff owned with her former husband. It mentioned her name in the letter's heading, but she was not otherwise mentioned. Instead, the letter read as follows:

"I write to confirm my telephone advice of 28 February, to the effect that it is my understanding the Fire & General Insurance on the Paradiso building may have been or is about to be cancelled by the Insurer.

I note your comment that this is all handled by the Guardian Trust Office in Auckland, and that your office may well have already received some notification of the cancellation of the insurance.

If we can be of any further assistance I am happy for you to contact me further to discuss. ..."

The Tribunal acknowledged that the Court of Appeal in *Harder* (above) had indicated a different approach to personal information. However, it took the view that it was dealing with a human rights issue, and that therefore the usual presumption should apply that the provision should be given a broad and liberal interpretation. The Tribunal went on to say:

[59] The matter is further complicated because the answer to the question 'Is this personal information?' can, we suspect, depend on how the question is asked. If one were to approach an observer and ask: "A owns a building which is insured. Is the fact that the building is insured "personal information" about A?" the answer might well be "no, it is information about the building." On the other hand, if one were to approach the same person but ask "Is the fact that A has insurance on her building "personal information" about A?" then the answer might well be "yes – it is information which tells me something about A's rights in respect of the building that she owns."

The Tribunal accepted in this case that the plaintiff's name appeared in the letter, and that it gave some information to the reader about the status of her insurance rights in relation to the building. [61]

The case was appealed to the High Court over a year ago, but it appears that no hearing date has yet been set. It is unclear whether the case is proceeding.

Current problems and queries for discussion

As can be seen in the Tribunal cases, the definition of personal information still causes some difficulties, particularly at the margins. Certainty about the concept is elusive.

For example, we have some current problems with the following (the facts have been changed where necessary to anonymise the parties):

- Letters that a person wrote in their official capacity while a member of an agency. Does a subsequent access request to that agency in the context of an employment dispute require consideration of all those letters the person wrote? They may state the writer's opinions, for example. They are certainly a communication made by the person (not that dissimilar to the *Harder* situation). Where they are relevant to the subject of the employment dispute, they should certainly be treated as personal information covered by the request. If they are not relevant to anything, as far as one can tell, practically

- speaking, we attempt to get the complainant to refine the complaint (thereby, with luck, excluding that material). But is it personal information at all?
- A sheep farmer (a sole trader, not a company director/shareholder) sent lambs to the abattoir. The carcasses were tagged with his grower number, put on pallets, and shipped overseas. The farmer had a dispute with the abattoir and the exporter. He requested access to all the documentation (pallet numbers, and export details) relating to the lamb carcasses. Is this personal information about him?
 - A couple's car broke down after being fixed by a mechanic. There was an argument about whether the repairs were adequate, or whether the car had a defect as a result of the way in which it had been driven and housed. The couple's insurance company got a report from one expert (supporting the mechanic's side of the story). It also got a report from another expert, suggesting that the mechanic may have been partially to blame for the breakdown. It discussed the mechanic's work, rather than anything that the couple might have been responsible for. The insurance company released a copy of the first report, but not the second. (We persuaded the insurance company that this was not particularly fair, and that it should give the couple the report, which it did very happily, and the complainants were delighted. But was the insurance report about the car personal information about the couple?)
 - Are exam scripts "personal information" about the students who wrote them? What about the marking guides? The latter information is somewhat similar to the stock price example in *CBN* above. (This is relevant because of the fact that some public sector institutions charge for providing copies of exam scripts, where, if they constitute personal information, this would be prohibited under the statute.)