Data Protection Litigation in New Zealand: Processes and Outcomes

Gehan Gunasekara[à] and Erin Dillon[*]
The University of Auckland

Enforcing Information Privacy Laws Symposium, Sydney, July 3, 2007

New Zealand's Privacy Act often gets much bad press, especially from the business standpoint but how much is there to fear in practice? An examination of data protection litigation to date reveals a great deal about the nature of claims and who they were against as well as the likelihood of complainants being successful.

The blood running through the veins of twenty-first century commerce increasingly consists of information about individuals.[1] The spread of technology around the world, globalization and security concerns have led to unprecedented amounts of information about individuals being collected and processed by the private sector and by governments. Data outsourcing, data mining and the profiling and tracking of individuals is already occurring on an alarming scale.[2] The ability to track and predict individuals' behavior is not only important for governments (for security and other reasons) but can provide businesses with an unrivalled competitive advantage.

The branch of the law that governs the processing (meaning collection, use and disposal) of personal data is called "data protection" law. It is a part of the wider field of privacy law which covers everything from drug testing to the rights of citizens to keep facts concerning their private lives from being publicized (the latter may overlap in some instances with data protection). As indicated by its title, this paper is concerned only with data privacy and not with these other aspects of privacy law. Regrettably, New Zealand's data protection statute is called the "Privacy Act 1993" (the Act) which has the potential to cause misunderstanding as to the precise nature of its coverage.

In this paper we examine New Zealand's data protection experience to date. When it was enacted, in 1993, the Act was relatively advanced by the standards of the time. It applied the same standards to both private and public sectors and applied to all personal data (with relatively few exceptions) regardless of the media in which the data is contained (the Act applies to electronic as well as to paper-based records). A relatively inexpensive

---

[◊] Senior Lecturer, Department of Commercial Law, University of Auckland.
[*] Researcher, Department of Commercial Law, University of Auckland. We are grateful for the assistance given to us by the Office of the Privacy Commissioner especially for the helpful comments of Blair Stewart and Katrine Evans, Assistant Privacy Commissioners. The responsibility for all errors of course rests with us.

[1] Gunasekara, G. (2007) "The 'Final' Privacy Frontier? Regulating Trans-border Data Flows" Forthcoming article in the *International Journal of Law and Information Technology.*

[2] See Information & Privacy Commissioner for British Columbia *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing*, British Columbia, 2004; available at: http://www.oipcbc.org/sector_public/archives/usa_patriot_act/pdfs/report/privacy-final.pdf

dispute resolution procedure, underpinned by the Office of the Privacy Commissioner and avoiding the need to resort to the courts has seen a large number of cases resolved since the Act has been in force. We examine the history of dispute resolution thus far with particular attention being given to outcomes from the complainants' point of view. We have also undertaken a statistical analysis which sheds light on, amongst other things, the nature of defendants, and nature of the remedies achieved as well as the areas of data protection which generated the most disputes.

The international context

The privacy implications of information technology, particularly automatic data processing and transmission, were understood at first in the more advanced western economies. The use, in these countries, of data processing in the delivery of social services and in law enforcement was accompanied by the corresponding concern, by their citizenry, about the potential for all-pervasive surveillance and the profiling of individuals by the State. As a consequence, legislation governing how such data was processed and allowing for access, by citizens, to data held about them by government was adopted, in the 1970s, in many European nations and in the United States.

A divergence that has persisted to this day was presaged by the fact that while the Europeans enacted legislation covering both their public and private sectors the United States passed legislation that applied only to information held by the federal government.[3] While this legislation still exists the application of similar principles to other sectors in the United States has proceeded only in a piecemeal fashion, with some sectors such as health information,[4] banking and credit information[5] being covered whilst others have been included as a response to particular lapses (such as the Video Privacy Protection Act 1988 as a consequence of the release of Judge Robert Bork's video rental records during his failed Supreme Court nomination).

The wisdom of the all-encompassing European approach was to be proved in the decades that followed with the proliferation in the use of computers by the private sector and the development of the internet which allowed individuals, as well as businesses and government to access the information superhighway. The reality that information can easily be transmitted between sectors and the difficulties in preserving public/private sector boundaries in an age of outsourcing and contracting out of public services meant that a "seamless" data protection regime was preferable to one that differentiated between sectors.

The potential for differing standards in the protection of personal data prompted the Organisation for Economic Cooperation and development (OECD) to issue its 1980 Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (the

[3] Privacy Act 1974, 5 USC S 552(a) (1988).
[4] Health Insurance Portability and Accountability Act 1996.
[5] Right to Financial Privacy Act 1978; Fair Credit Reporting Act 1970.

OECD Guidelines).[6] Although the OECD is an organization usually involved in promoting trade and investment between the most developed economies, not one primarily concerned with promoting individual privacy rights, it nevertheless recognized the implications for trade should the free flow of information to be disrupted on the basis of individual jurisdictions' laws for safeguarding personal data. The OECD Guidelines remain a benchmark against which individual nations' laws and international agreements concerning data protection can be measured: they were a major stimulus for the Australian and New Zealand statutes[7] and the more recent APEC Privacy Framework in the Asia- Pacific region.[8]

Moves toward harmonizing data protection norms within the European Union were taken to new and entirely higher level with its 1995 Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (the EU Directive).[9] Not only did the EU Directive require all member states of the European Union to adopt the Directive in their domestic law but it also prohibited the transfer of personal data from a member state to a third country where the third country could not ensure an "adequate" level of protection for the data after transfer.[10] This accelerated moves in other jurisdictions towards ensuring that data protection rules in the private sector were sufficient to comply with the EU Directive's "adequacy" standard.[11] One of the key rights stipulated in the EU Directive was the right of a data subject to a judicial remedy.

The refusal, by the United States Government, to adopt a mandatory data protection regime covering the private sector led to a lengthy dispute with the European Union which was finally resolved, in March 2000, with the adoption of a set of voluntary principles, called the "Safe Harbor Principles", which subsequently received the approval of the European Commission as satisfying the adequacy standard of the Privacy Directive. The Safe Harbor scheme is not mandatory (although at present over 1000 organizations are listed as subscribing to the principles, these include many companies such as Microsoft that do business in the European Union[12]) but those businesses that subscribe to it are bound by its principles and are subject to penalties for non-compliance imposed by the United States Department of Commerce.[13] Other countries have not had the leverage over the European Union to negotiate their own "safe harbor" and have opted instead to attempt to align their law with the EU Directive so as to secure an adequacy finding from the European Commission.

---

[6] Available at: www.oecd.org.
[7] See preambles to the Privacy Act (C'th) 1988 and the Privacy Act 1993 (NZ).
[8] Available at: www.apec.org
[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.
[10] Ibid, Article 25.
[11] For example the Privacy Amendment (Private Sector) Act 2000 (C'th, Aust).
[12] The list is available at: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.
[13] United States Department of Commerce, *Issuance of Safe Harbor Principles and Transmission to European Commission*, 65 Fed Reg 45666 (2000).

New Zealand's initially complacent attitude (following the Act's enactment in 1993) was later followed by the realization that refinements and additional provisions were needed to bring the Act fully into line with the EU Directive's standards.[14] However the technical amendments needed have not yet been enacted a full decade after they were mooted. These amendments do not go to the substance of the Act's content, rather they deal with peripheral but internationally significant issues such as preventing the re-export of personal data where New Zealand is used as a "data haven" to circumvent the EU Directive. The adequacy or otherwise of the solutions put in place to address these issues are beyond the scope of the current paper.

The nature of data protection principles and the significance of process: the focus for this paper

The OECD Guidelines and subsequent developments all have something in common: instead of cast iron rules they are structured as open-ended "principles", which have come to be known as "fair information practices" or "data/information protection principles". These are to be found, for example in the ten privacy principles contained in Canada's federal privacy law,[15] in the twelve information privacy principles (IPPs) in New Zealand,[16] and in the ten National Privacy Principles in Australia.[17] In the words of Jennifer Stoddart, the Privacy Commissioner of Canada, the nub of the principles is that:[18]

> "people should be told what information is being collected about them, by whom, for what purposes: they should be told what is being done with it and who it is being disclosed to; they should be able to control the collection, use and disclosure of the information through the power of granting or withholding consent; the information should be securely held….people should have a right of access to their information, and a right to correct it where necessary."

These principles are remarkably consistent across most jurisdictions which enhance the opportunities for comparisons between them.[19] While rules formulated as open-ended principles or guidelines have the advantage of flexibility, as they can be applied to new technologies as they emerge and are therefore less likely to become obsolete over time, they suffer from the disadvantage of uncertainty: consumers and businesses might be in doubt as to the scope of the principles and as to the manner in which they should comply: for example how much detail needs to be conveyed as to the purposes for which

---

[14] Office of the Privacy Commissioner, *Necessary and Desirable: Privacy Act 1993 Review*, Wellington, 1998.
[15] Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c5.
[16] Privacy Act 1993, s 6.
[17] Privacy Act 1988 (C'th), Schedule 3.
[18] Privacy Commissioner of Canada, *Annual report to parliament 2003-2004* (available at: http://www.privcom.gc.ca/information/ar/200405/200405_pa_e.asp)
[19] There are also slight differences though between jurisdictions that makes comparisons dangerous. For example NZ separates the use of personal information (IPP 10) from its disclosure (IPP 11) unlike National Privacy Principle 2 in Australia. Definitions also differ; for example the Australian definition of "personal information" avoids many of the issues that have concerned the courts in New Zealand.

information is collected and how securely should it be held (no system is completely immune to hackers and the like). In addition, a system of data protection principles on its own is meaningless unless data subjects have recourse to a meaningful remedy for infringements: voluntary or self-regulatory industry codes are no match for legally stipulated judicial remedies including the right of a data subject to receive compensation from a data controller for damage suffered as a result of breach of a data protection principle.

It is these two areas that are the focus of this paper. To what extent have the bones that constitute the information principles been fleshed out by the rulings in actual cases? Which areas of data protection generated the most litigation and what were the outcomes for litigants? One of the most useful tools by which the effectiveness or otherwise of a country's personal data protection regime may be assessed is the degree to which its privacy law provides real remedies in concrete instances affecting real people. In New Zealand such a tool exists in the reported case law of the dedicated tribunal that hears privacy complaints. Originally this was the Complaints Review Tribunal but it is now the Human Rights Review Tribunal (the Tribunal). Breaches of the Privacy Act ultimately end up here not in the regular courts and there now exists a body of specialized jurisprudence interpreting the Information Privacy Principles (IPPs).[20] A small number of cases resulted in further litigation before the courts and the significance of these cases will also be briefly examined.

The research for this paper was conducted over the southern summer and autumn of 2007 and examined all the reported decisions of the Tribunal in New Zealand from its inception until the end of 2006, a period spanning fourteen years. This allowed us to compile a statistical analysis of the cases from which we have ascertained, amongst other things, what percentage of defendants were from the private as opposed to the public sectors, which of the IPPs were litigated the most, the range and average amount of compensation awarded, the number of plaintiffs that were represented by counsel and the effect of representation on outcomes for them. The small number of cases that were further appealed to the courts and their significance is also briefly examined.

It must be stressed that the present study does not purport to be a comprehensive overview of New Zealand's privacy law. Reference should be made to standard works on privacy in New Zealand which cover data protection as well as other privacy related areas.[21] Instead, our aim has been to concentrate on those areas which occasioned the greatest difficulties in interpretation and enforcement – the presumption being that a significant proportion of cases which proceeded as far as the Tribunal must evidence genuine disagreement as to what the IPPs mean. In addition, since only the Tribunal can hand down binding rulings concerning the interpretation of the IPPs, this case law is important from the standpoint of precedent: again this is not to belittle the useful guidance given from time to time by the Privacy Commissioner, through its website,[22]

[20] All cases from 2002 are available at: http://www.nzlii.org/nz/cases/NZHRRT/2002/.
[21] See for example Roth P, *Privacy Law & Practice* , Wellington, N.Z., Butterworths, 1994-
[22] www.privacy.org.nz.

through issuing "selective" case notes[23] and through various other publications. All these play a vital educative role and, in the case of the Privacy Commissioner's investigative function, form part of the enforcement and dispute resolution mechanisms of the Act in New Zealand. However the Tribunal marks the endpoint of the enforcement and dispute resolution process and is the focus for much of what follows.

Data protection in New Zealand

Concern over use of new technologies by government agencies first arose in New Zealand in relation to the Police Law Enforcement System which centralized law enforcement data retrieval and management in a dedicated centre: from 1976 to 1995 these services were operated by a mainframe computer located in the city of Wanganui.[24]In response to these concerns legislation was enacted to control use of the information which allowed for access by citizens to their data and a dedicated privacy commissioner to investigate alleged violations of privacy.[25] This early data protection measure was supplanted, in 1991 by the Privacy Commissioner Act which created, for the first time, a national data protection official.[26]

The main purpose of the 1991 legislation was not, however, data protection but to assuage citizen concerns over the introduction of information matching between government agencies on a much wider scale. Information matching involves the comparison of one set of records with another, with the aim of finding records in both sets of data that belong to the same person (for example a list of people receiving welfare benefits with a list of people who have left New Zealand from customs records or who are deceased from the register of births, deaths and marriages).[27] The process is used to detect fraud in public assistance programmes, or to trace individuals who may be wanted; less frequently it is used to assist individuals (for example to identify someone who has not claimed an entitlement). In some matches it is the absence of a person in one set of records that is of interest. [28]

Information matching is potentially damaging to privacy interests for numerous reasons. Foremost among these is the lack of individual's control over automated processes, the potential harm that can result from errors and the reversal of normal evidential presumptions (those found in a matching sweep are presumed to be committing fraud despite the fact there may be a completely innocent explanation for the match). There is also the potential for further "black listing" of those found to be cheating and the indefinite stigmatization and surveillance of individuals. The 1991 legislation addressed these concerns by providing safeguards that were carried forward to the current Act

[23] Available at: http://www.nzlii.org/nz/cases/NZPrivCmr/.
[24] In 1982 anarchist Neil Roberts detonated a gelignite bomb in its entry foyer, New Zealand's only known case of a suicide bombing!
[25] Wanganui Computer Centre Act 1976.
[26] Privacy Commissioner Act 1991.
[27] Privacy Commissioner *Report of the Privacy Commissioner Year Ended 30 June 2006,* Wellington, 2006 p 31.
[28] Ibid.

which replaced it.[29] These include oversight by the Privacy Commissioner, stringent reporting requirements, procedural safeguards such as notification prior to adverse action, technical standards and the application of a cost/benefit evaluation as justification for such programmes.[30] The reassurance provided by these measures has meant that there has been relatively little public disquiet about the widespread use of data matching by the public sector.

A significant step in the evolution of New Zealand's data protection regime was the enactment of its freedom of information law, the Official Information Act 1982 (OIA) and the Local Government Official Information and Meetings Act 1987 (LOGOIMA). This legislation was also one based on broadly drawn principles, subsequently fleshed out by individual rulings. They opened up large areas of public sector information to public access and scrutiny. Individuals were, for the first time, given a legal right to access *all* personal information about them held by public sector bodies. Like the later privacy legislation the statutes applied to "information" irrespective of the media on which they were contained rather than to files or documents. The OIA and its local government counterpart have generated considerable jurisprudence and academic commentary in New Zealand.[31] However, unlike the United States Freedom of Information Act on which they are based, the dispute resolution process does not require recourse to the courts: an independent mechanism for complaints was provided through the existing office of the Ombudsman. The latter's rulings are binding though[32] and government agencies are required to comply with them except in exceptional circumstances.[33]

The first comprehensive law addressing all aspects of data protection in New Zealand was the Act which came into force in 1993.[34] In addition to regulating information matching, outlined above, it contained twelve IPPs governing the entire information processing spectrum: the collection, use and disposal of personal information.[35] The OIA and LOGOIMA's provisions giving access to personal information held in the public sector were transferred to the Act. Furthermore, the Act extended the OIA and LOGOIMA's right to access personal information held in the government sphere to the private sector as well.[36] The freedom of information statutes now cover only information other than personal information.[37] The Act therefore represents a "one size fits all" regime for governing personal data. It governs both the rules for access to personal information as well as how personal information is collected, used and disclosed.

---

[29] Privacy Act 1993, Part X and see the information matching rules contained in the Fourth Schedule.
[30] Ibid.
[31] Eagles I et al *Freedom of Information in New Zealand*, Auckland, Oxford University Press, 1992.
[32] Official Information Act 1982 s 32 (public duty to observe recommendation).
[33] Ibid; s 32A allows the Government to veto the Ombudsmen's recommendation but s 32 B allows this to be challenged through judicial review in the courts: to date the administrative veto has yet to be exercised.
[34] The application of certain portions were delayed until 1996.
[35] Privacy Act 1993, s 6.
[36] Ibid, Part 2.
[37] However Part 4 of the Official Information Act 1982 still applies to information about individuals who are not natural persons, that is to companies which is held by public sector organizations.

The Act applies to all "agencies" which are widely defined[38] to cover the public and private sectors and individuals (except information collected or held by individuals mainly for their personal, family or household affairs).[39] Excluded from the definition are the legislature, the judiciary (including tribunals and the like) and the news media in relation to their "news activity". The latter exclusion does not extend to the media's non news related activities (for example employees' personal information, advertising and subscription lists). It will be seen that the precise ambit of these exclusions have been the subject of litigation in several cases before the Tribunal and the courts. Intelligence agencies are also excluded from the Act's coverage except in relation to the right of citizens to access personal information held by them.[40]

The Act applies to "personal information" which is defined to mean information about identifiable natural persons as opposed to artificial persons such as companies.[41] Although both the Act and the earlier freedom of information legislation are "information" based and therefore technologically neutral – it can be said that in theory they apply even to telepathically communicated information – the issue as to what they include has concerned a good deal of the litigation before the Tribunal as well as the only case to proceed as far as the Court of Appeal. Likewise both freedom of information and privacy jurisprudence in New Zealand have long struggled with whether it is possible to grant access to information that is not recorded in physical form but is held in the memory of officials and whether this is capable of being retrieved.[42]

These reservations aside the Act is a convenient "one stop shop" regulating both access to personal information as well as providing remedies for its misuse. This fortuitous turn of events has undoubtedly been made possible because New Zealand is a unitary state with a relatively uncomplicated legal system. In Australia, by comparison the federal constitutional structure has meant that access to personal information held by state governments is through state privacy laws.[43] In addition, it has been seen that in New Zealand there are very few bodies that are excluded from the Act's coverage: there is for instance no exception for "small business operators" or for information about employees as exists in Australia.[44] The existence of a "level playing field" has undoubted advantages not least of which are the reduction of compliance costs involved in dealing with multiple agencies and sets of rules.

---

[38] Privacy Act 1993, s 2.
[39] Privacy Act 1993, s 56.
[40] Privacy Act 1993, s 57; s 72 B allows complaints to be made to the Inspector General of Intelligence and Security.
[41] Ibid, s 2.
[42] See for instance *R (a police officer) v Harvey* [1991] 1 NZLR; in *L v N* (CRT 27/96) a "signpost" on a file ("for information on individual refer to Executive Manager") suggested that a manager held undocumented information about the plaintiff which was accordingly held to be retrievable. Where it is possible to ascertain the outcome of a meeting or hearing the practice of both the Ombudsman and Privacy Commissioner has been to require this to be put in recorded form as soon as possible.
[43] For example in New South Wales the Privacy and Personal Information Protection Act 1998 deals with the way public sector agencies in NSW manage personal information.
[44] Privacy Act (C'th) 1988, s 6 C and s 7 B(3) respectively.

The Act also contains a built in flexibility because it gives the Privacy Commissioner the power to issue codes of practice that become part of the law.[45] Such codes may modify the operation of the Act for specific industries, agencies, activities or types of personal information. They often modify one or more of the information privacy principles to take account of special circumstances which affect a class of agencies (for example credit reporters) or a class of information (for example health information). The rules established by a code may be more stringent or less stringent than the principles they replace.[46] Proposals for issuing a code of practice may be made by a body representing the interests of a particular class of agency or industry, or by the Privacy Commissioner herself and are usually adopted after public consultation.[47]

Codes of practice are a flexible means of regulation and can be amended or revoked by the Privacy Commissioner at any time. However, as they are deemed regulations, they must be presented to the House of Representatives and are subject to careful scrutiny by the Regulations Review Committee. At present there are six codes of practice.[48] By far the most important of these is the Health Information Privacy Code which has generated around fifteen percent of litigation before the Tribunal. In addition to codes of practice the Act also allows for specific exemptions to be applied for and granted by the Privacy Commissioner.[49]

It should also be noted that the IPPs are themselves subject to a number of exceptions: for example where non-compliance is necessary for the purposes of law enforcement, the conduct of legal proceedings, to prevent serious and imminent health and safety threats[50] or for statistical or research purposes where the individual will not be identified. Requests for access to information can also be denied for numerous reasons including where disclosure would involve the unwarranted disclosure of the affairs of another individual, or where disclosure of the information or information identifying the person who supplied it is "evaluative material"[51] which would breach an express or implied promise to the person that the information or their identity will be held in confidence.[52]

Finally, the Act also regulates the manner in which information in public registers is used. Instead of the IPPs a separate set of public register principles[53] applies to these registers which are accessible to members of the public and in New Zealand increasingly available through the internet. The public register principles[54] stipulate that personal

---

[45] Privacy Act 1993, Part 6.
[46] For example, in the case of health information disclosure is permitted, where it would otherwise be forbidden, to next of kin or members of the patient's family.
[47] www.privacy.org.nz
[48] They are: the Credit Reporting Privacy Code, the Health Information Privacy Code, the Justice Sector Unique Identifier Code, the Post Compulsory Education Unique Identifier Code, the Superannuation Schemes Unique Identifier Code and the Telecommunications Information Privacy Code.
[49] Privacy Act 1993, s 54.
[50] The provisions of New Zealand's whistle-blowing legislation, the Protected Disclosures Act 2000, also override all other provisions where its mechanisms are employed.
[51] For example confidential employment references.
[52] Privacy Act 1993, s 29.
[53] Ibid, Part 7.
[54] Ibid, s 59.

information is only available from a public register by search references consistent with the manner in which the register is indexed or organised, that information obtained cannot be re-sorted or combined with personal information obtained from any other public register for the purposes of making available for valuable consideration personal information assembled in a form in which that personal information could not be obtained directly from the register and also prohibits electronic transmission of personal information from public registers except for the purpose of making information available to a member of the public searching the register. These restrictions have prevented the development by business of "value added" databases drawn from public registers. No litigation has arisen over the principles and as far as we could discover neither have there been any complaints concerning breach of them.

The dispute resolution process

As is the case with New Zealand's freedom of information legislation the Act sets up an inexpensive dispute resolution procedure that avoids recourse to the courts.[55] However it is underpinned by the backstop of the Tribunal, which has the power to grant legally enforceable remedies including the award of significant monetary damages, by New Zealand standards.

The starting point is the Privacy Commissioner: any person may complain to the Commissioner about an interference with privacy: this does not have to be the person who suffered the interference.[56] Complaints can be made orally or in writing although in the former case the Commissioner will assist in putting it into written form (a downloadable form can be obtained from the Commissioner's website).[57] The role of the Commissioner is both inquisitorial and conciliatory: in the former role the Commissioner is empowered to investigate the complaint in private [58] and her powers include being able to obtain documents,[59] to examine witnesses under oath[60] and override any statutory secrecy requirements.[61]

In the conciliatory role, on the other hand, the Commissioner has a statutory duty to use her best endeavours to secure a settlement where this is possible and is empowered to call a compulsory conference to this end.[62] The duty to exert best efforts to secure a settlement exists even where the Commissioner finds that the complaint has substance.[63]

---

[55] Ibid, s 11(2); despite s11(1) providing that IPP 6 (access to personal information) held by the public sector is a legally enforceable right in only a handful of cases has this been exercised all of these being in the context of other litigation.
[56] Ibid, s 67.
[57] Ibid, s 68.
[58] Ibid, ss 69, 90.
[59] Ibid, s 92.
[60] Ibid, s 91.
[61] Ibid, ss 94, 95.
[62] Ibid, ss 74 and 76.
[63] Ibid, s 77(1).

The practice of the Privacy Commissioner indicates that settlement of complaints is the main priority. In recent years a three-person team (known as the Assessment and Conciliation Team) make an initial assessment of all complaints, identify issues, gather any further information needed and make an early decision on whether the complaint should proceed or not.[64] Complaints not closed by the team are assigned to investigating officers for further action.[65] Appendix I contains a table with the number of total complaints in the period studied as well as the number of complaints closed. Since complaints can remain open from one year to the next the number of complaints closed can be greater or less than the number received in any current year. Closed complaints reflect a range of outcomes from the Commissioner deciding to take no further action through to the complainant being satisfied with the involvement of the Office and a voluntary settlement being reached.[66] Unfortunately, unlike other jurisdictions, no statistics exist for the remedies obtained on the settlement of complaints.[67] It has been suggested that the omission is the result of a conscious policy that parties to a dispute should themselves decide on appropriate remedies rather than being influenced by previous outcomes.[68]

The results thus far demonstrate the extremely high success rate of the conciliation process. Of the 11,610 complaints received in total the vast majority, 9367 or 81 percent have been settled. It can also be seen from Appendix I that the great majority of complaints have been settled even *before* either a provisional or final opinion by the Commissioner as to whether a contravention had occurred. This indicates that most agencies, when faced with a complaint, are either ready to accept their mistake or in any event prefer to settle privately rather than incur the adverse publicity that further litigation is likely to bring. The making of the complaint and the fact of being investigated have in most case been sufficient to induce a settlement.

Of the total number of complaints only a small proportion, 497 or four percent resulted in a finding by the Commissioner that the complaint had substance and that there had been an interference with privacy. It is important to note that this does not signify the number of cases where the complainant has succeeded in obtaining a remedy: as explained above the majority of cases were settled where there was a mutually acceptable outcome often involving the payment of compensation to the complainant.

---

[64] Privacy Commissioner *Report of the Privacy Commissioner Year Ended 30 June 2006*, Wellington, 2006 p 19.
[65] Ibid.
[66] Ibid.
[67] For example in the Australian Commonwealth (federal) jurisdiction in the 2005-2006 period compensation was a feature in 27% of complaints following conciliation and a table records that for example 8 complaints resulted in compensation between A$2000 and 20,000: see Office of the Privacy Commissioner *The Operation of the Privacy Act Annual Report* 1 July 2005- 30 June 2006 pp 33-34.
[68] K Evans "Show Me the Money: Remedies Under the Privacy Act" (2005) 36 VUWLR 475 p 479; reported settlements include a bunch of flowers, the gift of an overseas holiday to a couple, and the payment of several thousand dollars in compensation, see Privacy Commissioner's case notes 55528 [2003] NZ Priv Cmr 8; and 51765 [2003] NZ Priv Cmr 13.

When a finding of interference with privacy has been made and the parties have not managed to settle the dispute the Commissioner has discretion to refer the matter to the Director of Human Rights Proceedings (DHRP)[69] for consideration whether to bring proceedings against the defendant in the Tribunal.[70] The Commissioner has indicated there is now a presumption in favour of such referral unless other factors are present: for example all the information has been provided; there is no systemic issue that the agency has failed to address or where the complainant has not suffered a loss for which a remedy is required.[71]

This undoubtedly accounts for the relatively few referrals to the DHRP by the Commissioner, 47 in all as opposed to the number of complaints, 173 in all, pursued independently by the plaintiff (see Appendix II). However this pattern may be shifting; as indicated above there is now a presumption for referral where a complaint has been upheld and this is reflected in the number of cases referred in the last two reporting years (13 and 12 respectively).

When a complaint is referred to the DHRP it is considered afresh by the DHRP who has discretion as to whether to bring the complaint to the tribunal on the complainant's behalf.[72] The advantage, for complainants, is that when proceedings are brought on their behalf, the costs are borne by the Privacy Commissioner and not the individual. However the Act allows aggrieved individuals to bring proceedings before the Tribunal themselves where the Commissioner or the DHRP decides not to do so. As can be seen from Appendix II most of the cases that have been heard by the Tribunal were brought by aggrieved individuals themselves.

The number of cases where the complainant has been successful is very small. Indeed in only 34 cases brought before the Tribunal has it found that an interference with privacy had occurred.[73] This represents a miniscule 0.3 percent of the total number of complaints initiated which is a good indication as to how rare successful litigation is in New Zealand under the Privacy Act. However this is a very rough figure and does not indicate the nature of the complaints or the nature of the remedies obtained when an interference with privacy was found to have taken place. The remainder of this paper will focus accordingly on a more detailed investigation into the nature of outcomes for individual litigants before the Tribunal.

Finally, the number of cases that have been appealed further to the courts (the basis for these appeals is explained below) is even smaller. This is despite the existence of an automatic right of appeal, from the Tribunal, to the High Court which has the power to hear a case de novo (it will be seen that this power has been interpreted extremely narrowly by the Court).[74] There have been 14 appeals to the courts (including one to the

[69] Originally this was the Proceedings Commissioner.
[70] Privacy Act 1993, s 77(2).
[71] Above n. 64, p 24.
[72] Privacy Act 1993, s 77(3).
[73] This figure is drawn from our own research as the numbers reported in the annual reports may not be completely accurate.
[74] Human Rights Act 1993, s 123.

Court of Appeal) of which (using the same methodology we employ in analyzing the Tribunal jurisprudence) only 11 concerned substantive issues.[75] Of these cases the original complainant was successful[76] in only three whilst eight were unsuccessful. Likewise only in three instances was the outcome in the Tribunal reversed on appeal (that is a successful appeal by either the plaintiff or the defendant).

Litigants have a further right to appeal to the Court of Appeal: this is only allowed on questions of law and with the leave of the High Court and the issue involved must be one of general or public importance or there must be some other significant reason for the appeal.[77] The only case to make it thus far is considered below.

Litigation in New Zealand

Data protection litigation should be set in the context of other litigation involving individual rights. While a detailed comparison (for instance with human rights or employment litigation) is beyond the scope of this paper it can be observed that New Zealand is not generally a litigious society. Civil claims brought by individuals are few in number and usually do not involve exorbitant monetary amounts. This may be seen for example in New Zealand's no-fault scheme for accidents whereby the right to sue is replaced with State-guaranteed compensation for personal injury.[78] Under the scheme a person who suffers a permanent impairment such as the amputation of a leg below the knee receives a maximum of $13,409 in lump sum compensation whereas the maximum amount that may be claimed for substantial impairment such as paraplegia is $100,000.[79]

It is against the background of such facts that the award of damages in data protection litigation should be assessed: it will be seen that the highest sum to date, $40,000, is at the high end of civil litigation involving individuals. On the other hand defamation proceedings in New Zealand have frequently resulted in the award of much larger sums sometimes exceeding a million dollars.[80] It can be observed, however, that the latter invariably involved plaintiffs who were celebrities or public figures of one kind or another. Data protection litigation, by comparison, is usually pursued by lesser mortals and concerns the occurrences of everyday life: privacy litigation before the Human Rights Review Tribunal should be measured against the former and not the latter.

The Tribunal hears proceedings under the Privacy Act 1993, among other areas of the law.[81] It is a specialist body and consists of three members.[82] They are chosen by the

---

[75] One case, *Smits v Santa Fe Gold Ltd* (1999) 5 HRNZ 593, was an unsuccessful appeal against an order for *costs* in the Tribunal but we have included it even though we have excluded costs decisions by the tribunal itself.
[76] This includes where an appeal by the defendant was unsuccessful.
[77] Human Rights Act 1993, s 124.
[78] Injury Prevention, Rehabilitation and Compensation Act 2001.
[79] See: http://www.acc.co.nz/index.htm
[80] For example over a million dollars in *Television New Zealand v Quinn* [1996] 3 NZLR 24.
[81] Above n 64, p 24.

minister from a panel chosen for their experience in a variety of fields[83] only three of the 20 members being required to be legally qualified.[84] Although it is therefore most often the case that two of the Tribunal's members will have no legal background, the chairperson is required to be a barrister and solicitor with at least five year's experience.[85] The role played by chairpersons in the running of the Tribunal is indispensable as they are often called on to assist litigants in formulating their pleadings, a symptom it will be seen of the fact that the majority of plaintiffs represent themselves and when representation does exist it is usually by lay people. The Commissioner often appears in proceedings as an interested observer and in practice plays a crucial role, often acting as "de facto" counsel assisting the Tribunal.

As it is not strictly a court of law the tribunal is required to act according to the "substantial merits" of the case without regard to technicalities although in exercising its powers and functions it must act in accordance with the principles of natural justice in a manner that is fair and reasonable and according to equity and good conscience.[86] Despite these statutory injunctions an analysis of the Tribunal's decisions has revealed that a great many cases are indeed determined on the basis of technicalities and legal niceties routinely occur. On the other hand the normal rules of evidence are somewhat relaxed although the practice of the Tribunal has been to follow evidentiary rules as close to those observed in court as possible.[87] However evidentiary issues have pre-occupied many cases before the Tribunal and the outcome has hinged on them. Evidentiary difficulties have arisen where litigants have had to recall the content of conversations. In one case concerning disclosure it was stated that the:[88]

> "Tribunal will always have difficulty determining precisely what personal information is at issue if the disclosure is an oral one….the Tribunal is reluctant to find that an interference with privacy has occurred if there is doubt about the personal information which is the subject of the proceedings."

Thus it is evident that evidentiary concerns are essentially determining the very definition of "personal information" at least where alleged breach through inappropriate disclosure is concerned.

A case can be brought under the Act before the Tribunal if the Privacy Commissioner finds an interference with privacy has occurred and refers the case to the DHRP who then brings the case on the plaintiff's behalf. Alternatively, the plaintiff can bring their case before the Tribunal themselves:

- If the Commissioner finds no evidence of a breach of privacy or,
- If the commissioner finds a breach but does not refer the case to the DHRP or,

---

[82] Human Rights Act 1993, s 98.
[83] These include knowledge of cultural matters, public administration and socio-economic experience.
[84] Human Rights Act 1993, s 98.
[85] Ibid, s 99A.
[86] Ibid, s 105.
[87] Ibid, s 106.
[88] *L v L* CRT 11/01 (11 October 2001).

- The DHRP does not want to bring proceedings.

The Privacy Commissioner must first have investigated the claim for the Tribunal to have jurisdiction to hear it: the Commissioner provides a certificate of investigation and a final opinion to the complainant without which the Tribunal will strike out proceedings brought before it.[89]

It has been seen that the number of cases that make it to the Tribunal is relatively few in comparison to the number of complaints made every year to the Privacy Commissioner's office. On average there have been less than 10 cases a year.

Table 1

Year	No. of cases brought to the Tribunal
1993	0
1994	1
1995	0
1996	4
1997	10
1998	4
1999	10
2000	10
2001	5
2002	9
2003	7
2004	6
2005	5
2006	10
Total	**81**

For the statistical analysis 140 case notes were reviewed. From these notes the details of only eighty-one cases were used. Preliminary or interim decisions, cases that were struck out before they were brought to the Tribunal, directions, or any cases with jurisdictional issues preventing the plaintiff from bringing the case before the Tribunal were not included in the statistics. Also excluded are decisions solely relating to costs – as they invariably followed a substantive ruling their inclusion would have resulted in a double counting of the cases. However a very few cases (mostly in the early period of operation

[89] Above n 64, p 24 and as demonstrated in *M v The Ministry of Health* (1997) 4 HRNZ 79.

of the Act) have been included of cases that were decided "on the papers" (where parties did not appear but the substantive issues were dealt with by the Tribunal nevertheless). This study is only concerned with decisions relating to breaches of privacy made by the Tribunal. Other information found in the case notes was not included in the statistics, but will be referred to later on for different reasons.

While the total number of cases used here seems small at only 81 over the fourteen years the Tribunal has been in operation, the number would be even smaller if not for the insistence of some plaintiffs to have "their day in court". Although the settlement process appears to be effective in most cases, for some complainants the only acceptable remedy is to appear before the Tribunal. This is even more evident when the remedies sought by plaintiffs are taken into account: it will be seen that vindication, rather than monetary compensation is most commonly sought.

Although a few cases have the same name (such as two cases named *Pamela and Anthony Mayes v Owairaka School Board of Trustees*); they relate to different breaches of the Act and were brought separately and at different times. Such cases have been counted as separate and distinct from each other for this study.

The nature of defendants

Analysis of the cases revealed that public sector defendants appeared in fifty cases; accounting for sixty-two percent of the total number of defendants. For this study we have employed the statutory classification of public as opposed to private sector agencies. "Public Sector Agency" is defined by the Privacy Act 1993 as: (a) an agency that is a Minister, a Department, an organisation, or a local authority; and (b) includes any agency that is an unincorporated body (being a board, council, committee, or other body) which is established for the purpose of assisting or advising, or performing functions connected with any public sector agency within the meaning of paragraph (a) and; which is so established in accordance with the provisions of any enactment or by any such public sector agency.[90]

The six most common defendants in the Tribunal were:

- The New Zealand Police with fourteen cases bought against them.
- Second was the Accident Compensation Corporation with eight.
- The Department of Work and Income New Zealand tied with the Department of Corrections for third place with four each
- The Inland Revenue Department tied with the Department of Child, Youth and Family Services with three cases to defend each.

All of these are public sector organisations, accounting for forty-three percent of all cases bought to the Tribunal. We have adopted the statutory classifications of the public sector as opposed to, for example, a classification by sector (government, education, health,

[90] Privacy Act 1993, s 2 (1); this definition also includes Hospital Boards and School Boards of Trustees amongst others.

financial and insurance). This is because a classification by sector in New Zealand would span both public and private sectors: for example the health and education sectors as well as insurance (the biggest insurer in New Zealand is the Accident Compensation Corporation which is a statutory entity).[91]

The private sector, by contrast, accounted for forty-one percent of defendants, appearing in thirty-three cases. These percentages do not quite add up as there was often more than one defendant, and in a few cases (such as *Geoffry Ivan Hadfield v NZ Police and DJ Cartwright*)[92] one defendant was from the public sector and the other was from the private sector. In such cases the defendants were counted in both categories.

Out of the private sector defendants, thirty-nine percent were involved in the health sector; totalling thirteen cases in all. Most of these defendants were private doctors or psychologists. In one case (*Christopher Joseph O'Neill v Dispute Resolution Services Ltd*)[93] the defendant corporation although acting on behalf of the ACC was sued in its own capacity. Since the dispute related to the health sector it has been included in the private sector health category rather than in the public sector. The old doctrine that a doctor's notes on a patient were for the doctor's eyes only contributed greatly to this sector coming under the spotlight for breaches of privacy. Under the Act a patient has the right to review files a health practitioner holds on them, with some exceptions.

After removing defendants from the public and health sectors, twenty cases remain; meaning only twenty-five percent of cases were brought against the ***commercial*** sector. However, this figure also includes the many defendants that were clubs or non-profit organisations. The true figure for the commercial sector is even lower, but is difficult to ascertain as private sector defendants in some cases have name suppression. Private sector defendants have included banks, insurance companies, individuals and even funeral directors![94]

Twelve cases in total were brought under the Health Information Privacy Code, making up fifteen percent of the total. As explained below the principles of the Health Code are not distinguished from those of the Privacy Act.

Areas most litigated

A major point of interest for our inquiry was which of the Information Privacy Principles (IPPs) were litigated the most frequently. For the purpose of this study the principles contained in the codes of practice are not distinguished from those of the Privacy Act: the rules contained in them mirror the IPPs themselves. For instance Rule 6 of the Health Code grants access to health information whilst Rule 11 prohibits improper disclosure of

[91] Responsible for administering New Zealand's pioneering "no fault" accident insurance scheme which covers every individual in New Zealand at work or play.
[92] (1996) 3 HRNZ 115.

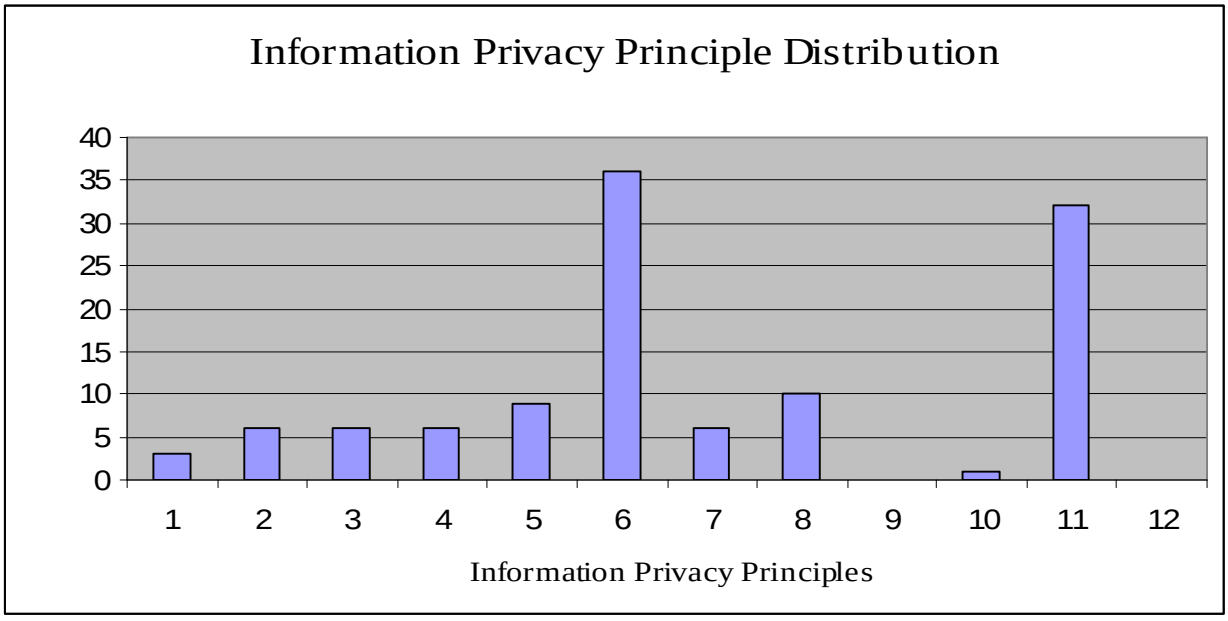
[93] HRRT 16/05, (10 April 2006).
[94] See *A & A v G* CRT 8/99 (13 July 1999).

health information: similarly IPP 6 grants access to personal information under the Act and IPP 11 governs improper disclosure. Likewise Rule 7 of the Credit Reporting Privacy Code gives individuals the right to correct information held about them: IPP 7 similarly applies to the right to seek correction generally. We have therefore treated claims brought under the code of practice rules as being part and parcel of breach of the IPPs themselves since they essentially cover the same subject matter.

As can be seen from the graph in figure 1, principles six (right to access personal information) and eleven (improper disclosure of personal information) generated the most litigation. Principles nine (retention of personal information for longer than necessary) and twelve (use of unique identifiers) were not litigated at all. Principle eight (ensuring accuracy before personal information is used) however generated a significant number of cases as did principle five (security of personal information). Apart from principles one (purposes of collection of personal information) and 10 (use of information for purposes other than those for which it was collected) the remaining principles were invoked in over five cases. These included principle two (collection of personal information directly from individuals), three (informing data subjects of the purposes of collection) and principle four (collection of personal information by unfair or intrusive means).

Since plaintiffs are able to complain about the breach of more than one principle to the Tribunal at a time the total number of principles shown on the graph does not correspond to the number of cases included in this study.

Figure 1



The predominance of complaints relating to the failure to grant adequate access to personal information marks a point of distinction between New Zealand's data protection litigation and those of other jurisdictions. For example, in the Australian Commonwealth jurisdiction, claims regarding improper disclosure of personal information have tended to be the most prevalent.[95] The explanation for this may well be, as pointed out earlier, the fact that access to much information in the public sector is managed under state as opposed to federal privacy laws. On the other hand in Hong Kong, a jurisdiction with a seamless regime not dissimilar to that of New Zealand's, disclosure is also the area most litigated.[96]

Nature of remedies obtained

An area central to our research was the nature of outcomes for plaintiffs from their claims before the Tribunal. The Tribunal is empowered to award one or more of five categories of remedy:[97]

- A declaration that an interference with privacy has occurred
- An injunction preventing conduct by the defendant
- Monetary damages
- An order requiring the defendant to perform conduct
- Other relief at the discretion of the Tribunal

In most cases successful plaintiffs were awarded more than one remedy. The most common remedies were; awards for damages[98] and/ or costs, orders for performance and orders for a declaration that a breach had occurred. The Tribunal is allowed to award other remedies at its discretion, although it is not clear if it has the power to order a formal apology.[99] As is clear from figure 2 the most popular remedies were awards for damages and declarations.

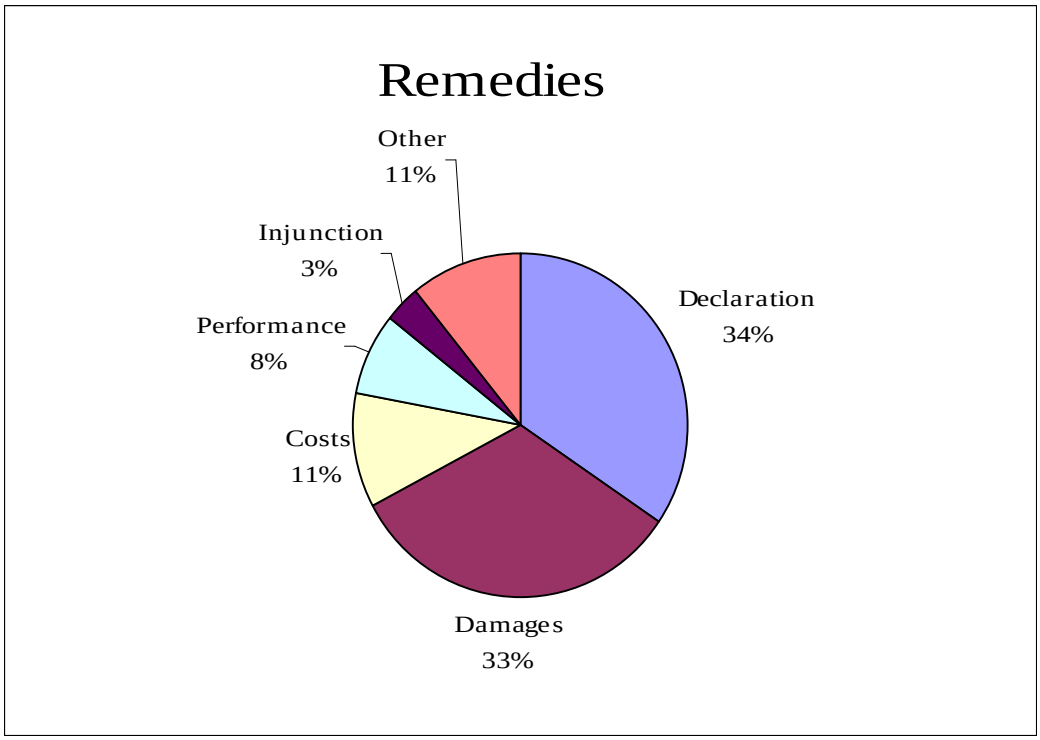
Although specific remedies such as injunctions and orders requiring the defendant to perform obligations were rare this is not surprising since a declaration that conduct constituted an interference with privacy, by an agency, was often sufficient to lead to a change in behaviour by it – the more so where a public sector agency was involved. The "other" category included instances where the defendant "agreed" to make a formal apology and one case where the plaintiff merely wanted an acknowledgment form the defendant that there had been an interference with privacy, no other remedy being sought.[100] In one case the plaintiff was successful but no remedy was granted.[101] In the few cases involving an order for performance, remedies granted included being granted

[95] See Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report 1 July 2004- 30 June 2005*, p 46 and *Annual Report 1 July 2004- 30 June 2005*, p 38.
[96] Office of the Privacy Commissioner for Personal Data, Hong Kong, *Annual Report 2004-2005* p 8.
[97] Privacy Act 1993, s 85.
[98] For a detailed discussion as to the basis on which damages have been awarded see K Evans "Show Me the Money: Remedies Under the Privacy Act" (2005) 36 VUWLR 475.
[99] Ibid p 483.
[100] *Poysden v Lower Hutt Memorial RSA, Inc.* (HRRT 35/01).
[101] *L v T* (1998) HRNZ 30.

access to files, the destruction of files and the modification of files (including where individuals requested their rights under IPP 7 to have a request for correction noted).

Due to more than one remedy being awarded to any plaintiff the percentage values as shown on the graph do not sum to one hundred. The percentages show the number of plaintiffs awarded a particular remedy regardless of if they were also awarded another remedy. For example; sixty-five percent of successful plaintiffs were awarded damages. Some of those plaintiffs would also have been awarded costs. Hence when these separate percentages are added they do not sum to one hundred.

Figure 2



The maximum monetary award that the Tribunal may grant is equivalent to that of the District Court: currently this is $200,000.[102] However the Tribunal has the power to refer

[102] Human Rights Act 1993, s 92 Q.

a case to the High Court where a higher award of damages is warranted.[103] Not only has such a referral not occurred but the highest amount of damages awarded to date has come no-where close to the upper limit allowed.[104]

Table 2 contains a break-down in dollar terms of the remedies awarded to the successful plaintiffs:

Table 2

Damages (21 cases)

Range	$200 - $40,000
Mean	$7,449.80
Median	$4,000

The figures are skewed somewhat due to the distorting effect of a single egregious case.[105]

The awards of costs where the plaintiff has succeeded have been modest as can be seen from table 3.

Table 3

Costs (7 cases)

Range	$121.33 - $1,338
Mean	$711.28
Median	$500

Fifty-eight percent of plaintiffs were unsuccessful in their claim for an interference with privacy. Where the plaintiff was unsuccessful in their claim the defendant had the opportunity to claim for costs. The Tribunal awarded costs against the plaintiff in twenty-one percent of unsuccessful claims. Table 4 contains a break-down: it can be seen that considerably larger awards of costs were made in these circumstances.

[103] Ibid, s 92 R.
[104] For a discussion on awards to date and suggestions as to reform see Evans, above n 98.
[105] *Hamilton v The Deanery 2000 Ltd* (2003) HRRT 36/02; this case is further discussed below.

Table 4

Unsuccessful Plaintiffs Ordered to Pay Costs of Defendant (10 cases)

Range	$500 - $12,500
Mean	$4,401.99
Median	$2,750

Representation for plaintiffs and effect on outcomes

An aspect of our research that proved somewhat elusive but nonetheless yielded unexpected results was the attempt to discover how many plaintiffs had legal representation. Unfortunately it proved impossible to ascertain how many plaintiffs were represented by persons who were *legally qualified*. This is because representation, for the most part, was by lay persons, albeit those who might have some expertise in the area.[106]

Proceedings under the Act differ in this regard from those under the Human Rights Act 1993: in the latter case, whilst parties may appear in person, they may only be represented by legal counsel.[107] The Tribunal, in its other jurisdiction, also hears claims under this legislation. The restriction as to who may represent plaintiffs was not, however, adopted by the Privacy Act.[108] Whether the distinction was deliberate or not, it might be subjected to critical scrutiny: although there are undoubted benefits, in terms of informality and lowering costs, of not granting the right of representation to lawyers alone, it is also the case that issues arising under the Act are at least as complex and technical as any relating to claims of discrimination under the Human Rights Act. Evidentiary difficulties have also been present as we have seen.

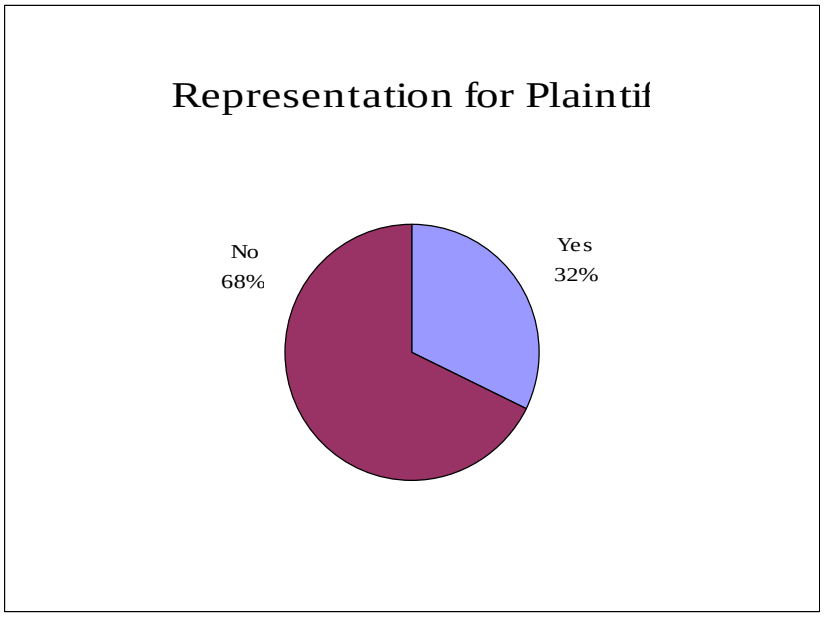
In at least some cases representation was by legal counsel, in some instances even by Queen's Counsel. Occasionally reference was made, in the Tribunal's ruling, as to whether representation was by legal[109] or non-legal[110] advocates. On occasion, legal counsel was retained at a late stage when the complexity of issues raised by the proceedings and evidentiary hurdles had become apparent: the lawyer who was briefed had not however been responsible for filing proceedings at the outset which imposed obvious constraints on the ability of the lawyer to argue the case to the best advantage of

[106] For example in *Lehman v CanWest Radioworks Ltd* [2006] NZHRRT 35 (21 September, 2006) the plaintiff was represented by James Harder, the son of Barrister Chis Harder, himself a defendant in proceedings under the Act as discussed below.
[107] Human Rights Act 1993, s 92 C.
[108] The Privacy Act 1993, s 89 only applies ss 92 Q to 92 W and Part 4 of the Human Rights Act 1993 to Privacy Act proceedings.
[109] See *Stevenson v Hastings District Council* [2006] NZHRRT 7.
[110] *Hamilton v The Deanery 2000 Ltd* (2003) HRRT 36/02, at para 55.

the plaintiff.[111] However we estimate that in the majority of cases the representation was by lay advocates who were not legally qualified.

Since it is not possible to gauge the exact number of plaintiffs who retained legal counsel, we have instead differentiated those cases where the plaintiffs represented themselves (whether or not they had assistance in doing so) from where they retained lay *or* legal counsel: the key distinction being whether the person thus designated was formally recognized as entitled to represent the plaintiff by the Tribunal. Figure 3 shows the relative proportions of these two categories.

Figure 3



From figure 3 it is clear that the majority of plaintiffs represented themselves. With regard to the efficacy of representation, there was no material difference in the percentage of successful plaintiffs with representation or without: the figure remains at about forty-

[111] Above n 109.

two percent in both groups. Out of the twenty-six plaintiffs with representation, eleven were successful. Of the fifty-five plaintiffs without representation, twenty-three were successful. In percentage terms this is very close; 42.31% and 41.82% respectively. It seems the outcome of a case is not affected by whether the plaintiff has representation or not.

However this does not tell the whole picture: there is a noticeable difference between the scale of remedies awarded to successful plaintiffs who had some form of representation, and successful plaintiffs who had none. Table 5 contains a break-down:

Table 5

Damages:

	With (7)	Without (14)
Range	$200 - $40,000	$500 - $20,000
Mean	$12,885.71	$3,303.27
Median	$10,000	$3,000

The inequality is also present in the award of costs for successful plaintiffs as can be seen in table 6:

Table 6

Costs:

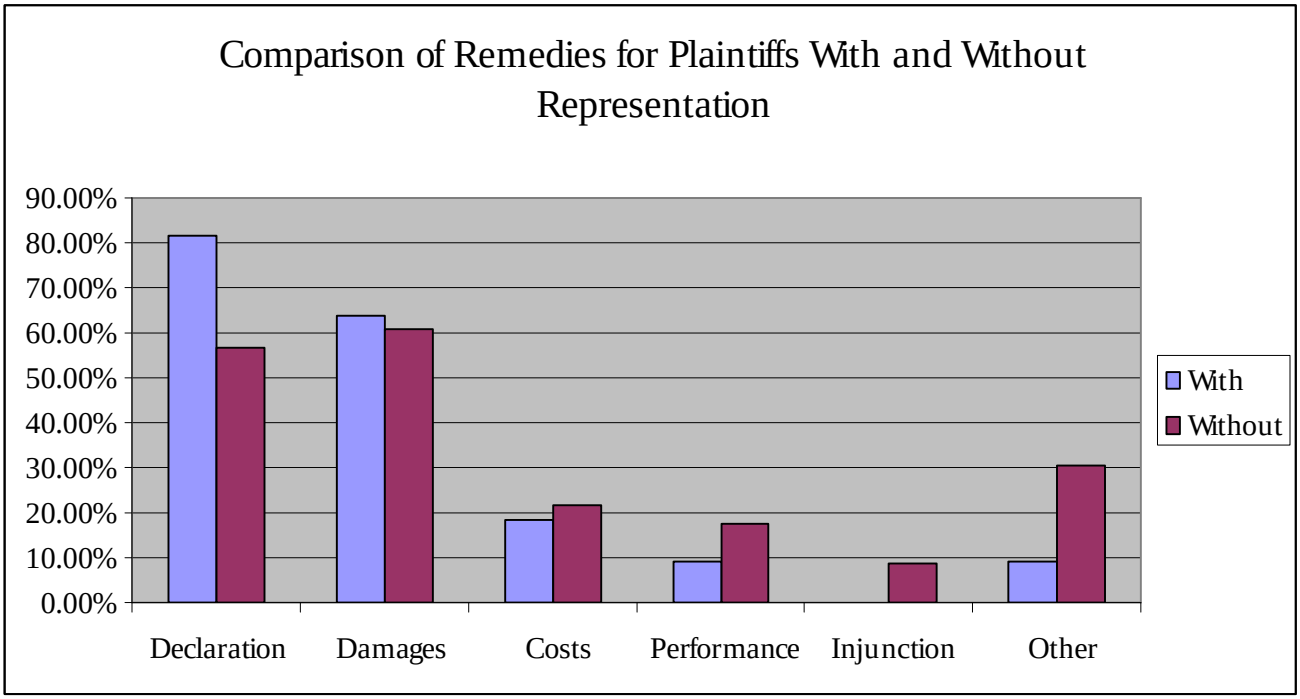
	With (2)	Without (5)
Range	$500- $1,338	$121.33 - $1,269.64
Mean	$919	$628.20
Median	$919	$500

There is clearly a great disparity in the amounts of compensation awarded in favour of plaintiffs with representation. One explanation might be that these plaintiffs employed representation primarily because of the large sums of money involved. The case of *Paula Christina Hamilton v The Deanery 2000 Ltd* [112]was one such high-profile case and involved such a serious breach of privacy that it would have been highly unusual for the plaintiff to have represented herself. In this case the plaintiff was awarded $40,000 in damages; the highest amount awarded to date.

Figure 4 compares the number of remedies awarded to successful plaintiffs with and without representation. For example; sixty-four percent of successful plaintiffs with representation were awarded damages, while sixty-one percent of successful plaintiffs without representation were awarded damages.

[112]*Hamilton v The Deanery 2000 Ltd* (2003) HRRT 36/02: this case is discussed further below.

Figure 4



This inequality holds where the plaintiff has been unsuccessful and ordered to pay costs to the defendant. Of the unsuccessful plaintiffs with representation, twenty-seven percent had to pay costs to the defendant; whereas of the unsuccessful plaintiffs without representation, only nineteen percent had to pay costs to the defendant. As can be seen

from the following chart, plaintiffs with representation, on average, were ordered to pay more in the way of costs than plaintiffs that had none.

Unsuccessful Plaintiff Pays Costs of Defendant:

	With (4)	Without (6)
Range	$1,529.86- $12,500	$500 - $10,000
Mean	$5,007.50	$3,998.30
Median	$3,000	$2,750

It is also worth noting that in two cases the plaintiffs were successful, yet were ordered to pay costs to the defendant for various reasons. These cases were *Pamela and Anthony Mayes v Owairaka School Board of Trustees* (ordered to pay $500) and *W v Christchurch Casinos Ltd* (ordered to pay $12,500). There was also one case in which the privacy commissioner was ordered to pay costs to the defendant (*O and others v N*. The Privacy Commissioner was ordered to pay costs of $668.95).

Significant cases

The decisions of the Tribunal have with few exceptions been non-technical and based on sound practical considerations. For example in *Mitchell v Police Commissioner*[113] it ruled that when access to personal information was sought, it was not sufficient to undertake a search however thorough: what was required was an "intelligent" rather than a "mechanical" search especially when an attempt was being made to trace a missing file which may have gone elsewhere.[114] Likewise where disclosure of personal information is involved the disclosure is not limited to the use of words: conduct which results in the information being disclosed can be sufficient.[115] Other rulings resulted in compromises which went some way toward addressing the complainant's grievance. For instance while supervisor's report on a doctoral thesis was withheld on the grounds it was evaluative material, the defendant accepted that some feedback from the supervisor instead of the report itself might be possible.[116]

Several early decisions concerned the scope of the Act's coverage and its exclusions. For example in one case it was held that disclosure by a lawyer of details concerning his client's matrimonial settlement concerning the plaintiff's children to a school principal

[113] CRT 2/94
[114] Ibid, the Privacy Commissioner will usually request an agency to provide a report on the steps taken to locate a missing file.
[115] *Proceedings Commissioner v Commissioner of Police* CRT 23/99.
[116] *Woodward v University of Auckland* CRT 18/96.

came within the ambit of the personal, family and household affairs exclusion.[117] In another case the publication of an annual "Rich List" with biographical details of the one hundred or so wealthiest individuals in New Zealand without their consent was found to fall within the "news activity" exclusion in the definition of "agency".[118]

In one of the few decisions to be further appealed to the High Court it was argued that the Inland Revenue Department (IRD) was entitled to disclose the level of the plaintiff's income in the context of varying a child maintenance agreement as it was acting judicially.[119] However it was held by both the tribunal and the Court that the IRD was acting administratively rather than exercising a judicial function and further that the Act was not overridden by other legislation that required the giving of reasons by the IRD: the disclosure of detailed information as to income was not a necessary part of the reasons for the decision in this case. It can be seen then that the Act must be taken into account when organizations comply with myriad other pieces of legislation: the IPPs must be complied with as far as is possible whilst meeting the requirements of the other laws.

Although the Tribunal is to act without regard to technicalities it has in fact followed legal principles, rules and precedents. In *C v ASB Bank Ltd* [120] for example, although the plaintiffs alleged a breach of IPPs 5 and 11 through disclosing copies of bank statements of a company owned and operated by the plaintiff to his former wife, it was found that the information was not personal information about the plaintiff: the company was on established principles a separate juristic person and disclosure related to it and not the plaintiff.[121]

Similarly, the Tribunal has followed[122] earlier legal precedents concerning the disclosure of information, for example that there is a distinction between the disclosure of information and the re-publication of already known facts[123] and that disclosing information normally entails communicating it to someone who does not know it already.[124] These precedents were fatal to the plaintiff's case involving a funeral director where there had allegedly been publicity concerning the same facts in a popular women's magazine.[125] Evidentiary difficulties[126] also existed since the plaintiff's allegation that disclosure had occurred was rebutted by the defendant's "alibi" contained in the funeral records! There was additionally the problem of proving causation: damage (in the form of

---

[117] *S v P* CRT 27/97; the lawyer's disclosure was deemed not to be his own but for his client's purposes meaning he was also protected.
[118] *Talley Family v National Business Review* (1997) 4 HRNZ 72 (CRT)
[119] *Commissioner of Inland revenue v B* [2001] 2 NZLR 566.
[120] (1997) 4 HRNZ 306 (CRT).
[121] The disclosure had led to serious consequences for the plaintiff as additional claims brought against him by the wife resulted in the company being placed in liquidation.
[122] *A & A v G* (CRT 8/99).
[123] *Attorney-General v Associated Newspapers Ltd* [1994] 1 All ER 556.
[124] *Bank of Credit and Commerce International (Overseas) Ltd (in Liq.) v Price Waterhouse* [1997] 4 All ER 781.
[125] Above n 122.
[126] Similar standards appear to be applied as in the courts, for example corroboration being required when the sole evidence consists of recall of conversations and the like.

significant humiliation, loss of dignity or injury to feelings) could not be established since people were already aware of the facts relating to the plaintiff, it could not be the defendant's disclosure which caused the harm.[127]

In a similar vein the Tribunal, in considering the obligation in IPP 8 to take reasonable steps to ensure personal information was accurate, up to date, complete, relevant and not misleading prior to using it, adopted a ruling of the House of Lords that to pass information from one person to another involved its use.[128] It held, however, that there was no need to ensure that information was "accurate beyond any shadow of an argument".[129]

Despite accepting earlier freedom of information jurisprudence that "information" denotes "that which informs, instructs, tells or makes aware"[130] the Tribunal has continued to struggle with the outer limits of what information can include. While a wide view has prevailed in respect to the right to access information[131] a somewhat narrower interpretation seems to be applied to cases involving disclosure:[132]

> "The requirements of the Act are more suited to information which has been collected, held and stored in much more formal and precise ways than information which can be described as gossip and speculation…"

Such an approach may well be justified on pragmatic grounds but may not be correct legally: it is trite law that an opinion can amount to a statement of fact that that the opinion is based on facts within the knowledge of the person making the statement.

An issue frequently confronting the Tribunal has been the basis for granting a remedy where an interference with privacy has occurred and especially for awarding monetary damages. Fortunately, the Act provides that for an actionable interference with privacy to occur not only must there be breach of an IPP or code of practice but one of the criteria specified in s 66(1) (b) must also exist. These require:

- Loss, detriment, damage or injury[133] to the victim; or
- The rights, benefits, privileges, obligations or interests of the victim are adversely affected; or
- Actual or potentially significant humiliation, loss of dignity or injury to the feelings of the victim

---

[127] Above n 122.
[128] *R v Brown* [1996] 1 AllER 545.
[129] *Hederson v C.I.R.* (2004) HRRT 49/02.
[130] *Police v Ombudsman* [1988] 1 NZLR 385.
[131] Provided it is retrievable in some manner.
[132] Above n 122.
[133] In an early complaint that was settled a woman suffered domestic assault and violence as a consequence of a bank making disclosures to her husband regarding her spending! This is possibly a loophole around New Zealand's prohibition against suing for personal injury.

It is also important to note that a plaintiff must show a clear causal link between one of these adverse consequences and the breach of an IPP or rule. This was evident in a number of cases.[134] However an exception to this was clarified in an important High Court ruling. Section 66 (2) provides that the failure to make personal information available[135] to an individual requesting it is actionable if valid grounds did not exist for denying the access to the information. In *Jans v Winter* the Court held that where there has been a breach of principles six (access) or seven (correction) the plaintiff does not need to prove that he or she has suffered one of the types of harm specified in s 66(1): the breach will in itself amount to an interference with the plaintiff's privacy.[136] It is worth noting that the failure to give timely access to the file led to an award of damages of $15,000, a not inconsequential sum.

A particularly egregious case involving the disclosure of personal health information was that of *Hamilton v The Deanery 2000 Ltd*.[137] The plaintiff was a public figure[138] in the United Kingdom who sought treatment, in New Zealand, at a private alcohol treatment clinic which advertised itself as providing confidential discrete care for professionals. Initially the clinic formed a close relationship with its patient and considered employing her as an international consultant and assisted her towards obtaining residency in New Zealand. Subsequently, though relations soured and the clinic's director contacted immigration authorities alleging that the plaintiff was a drug-user: as a consequence she was questioned and suffered considerable humiliation on her return to New Zealand. After the plaintiff was reported in local news-media as having been convicted of drink-driving the clinic's director gave an interview to news-media in which he described her treatment and gave reasons as to why she had "failed" the programme. Finally he gave an interview to a United Kingdom tabloid newspaper which had a wide circulation in the United Kingdom and was also published on the internet. The interview was potentially defamatory as it included allegations of drug-taking by the plaintiff.

The Act allows damages to be sought under one or more of three categories: actual losses, loss of future benefits and humiliation, loss of dignity and injury to feelings.[139] Ms Hamilton claimed the maximum amount of $200,000 on the basis of the value of lost opportunities to work in the United Kingdom, the costs of storing her furniture and personal effects and the extra costs of legal advice and representation required to deal with the immigration issues she faced in New Zealand.

The Tribunal, however, was unable to establish a causal link between the undoubted interference of privacy that had occurred and most of these specific losses: the plaintiff had brought defamation proceedings against the United Kingdom newspaper that had resulted in a settlement which it regarded as addressing the first loss and although the

---

[134] For example *A & A v G* (CRT 8/99) and see *Hamilton v The Deanery* below.
[135] This includes inordinate delay in supplying the information, the refusal to correct personal information, the imposition of improper conditions or excessive charges for supplying the information.
[136] *Winter v Jans* Unreported, CIV – 2003-419-854, High Court, Hamilton, (6 April, 2004).
[137] HRRT 36/02 (29 August 2003).
[138] She had been a model, television presenter and actor and achieved fame as the "girl in the VW Golf commercials".
[139] Privacy Act 1993, s 88(1).

plaintiffs immigration application was complicated by the disclosures made by the defendant it was far from certain that all her difficulties with her application were attributable to them.[140] In the event the Tribunal was only able only to award compensation under the "humiliation, loss of dignity and injury to feelings" category although it added a caution that the proper approach in the case was to "look at the issue 'in the round' – i.e. to make an award that will cover all of the various interferences in one global sum".[141] The final sum awarded was $40,000, a significant amount by New Zealand standards but hardly likely one would think to serve as a deterrent for similar outrageous conduct in future.

High Court and Court of Appeal cases

As detailed earlier appeals to the courts from decisions of the tribunal are rare and the success rate of such appeals extremely low. Despite this some observations can be made concerning the cases that did come before the courts.

Although the High Court is empowered to hear a case afresh in practice it is extremely difficult to disturb the Tribunal's findings of fact on appeal.[142] Similarly when considering an appeal against an award of costs by the Tribunal the Court followed earlier legal precedents[143] that it should:[144]

> "…not interfere with the exercise of a discretion unless it can be shown that it was plainly wrong, because either that it proceeded on a wrong principle or that undue weight was given to some factor or insufficient weight to another."

On the other hand the courts have been less reluctant to challenge the Tribunal's discretion in awarding remedies. In a case where the plaintiff had sought access to personal information in order to facilitate the prosecution of an employment dispute, the Tribunal was found to have made an error of law which allowed the Court to interfere with its findings.[145] The plaintiff had suffered a loss of benefit of a non monetary kind in not having the information necessary to fully cross-examine in the employment litigation; the Tribunal had been wrong to conclude that the complainant was merely using the Privacy Act to carry on his dispute with his former employer in another forum.[146] This case may be contrasted with others where the plaintiff has indeed been found to be using the Act to continue a dispute which concerned a non-privacy related matter.[147]

---

[140] The Immigration authorities evidently realised there was an ulterior motive behind the disclosure and took them accordingly with "a grain of salt".
[141] Above n 137, para. 47.
[142] See for instance *L v T* (1998) 5 HRNZ 30 and *P v J* Unreported, HC 117/98, High court, Auckland, Fisher j, 27 October, 1998.
[143] *Fitzgerald v Beattie* [1976] 1 NZLR 265, 268.
[144] *Smits v Santa Fe Gold Ltd* (1999) 5 HRNZ 593.
[145] *Proceedings Commissioner v Health Waikato* (2000) 6 HRNZ 274.
[146] Ibid, damages of $8,000 and costs of $5,500 were awarded.
[147] For example *Smits v Santa Fe Gold Ltd*, above n 144, where the appellant had been pursuing a crusade against the adult entertainment industry and the nub of the complaint did not concern any breach of privacy: unsurprisingly significant cost were awarded against the unsuccessful plaintiff on account of this.

Issues of evidence and causation have also arisen on appeal. In one case where the plaintiff alleged that the disclosure by the defendant to the plaintiff's husband of the fact that she was undergoing surgery led to the breakdown of her marriage (as the husband failed to visit her!) the claim was found to be exaggerated, far-fetched and in some respects contradictory, a causal link not being able to be shown.[148]

By far the most troublesome case to reach the courts has also been the only one to come before the Court of Appeal. In *Harder v Proceedings Commissioner*[149] the Tribunal and the Courts had to decide what the open-ended requirements contained in the IPPs actually meant as well as the scope of what "personal information" covered. The defendant, a lawyer, had tape recorded, without consent, a conversation with the opposing party to litigation which his client was involved in. The recording was not itself used but the fact that it existed was used to embarrass the plaintiff in the subsequent court proceedings involving the client. The plaintiff brought a complaint against the lawyer alleging breach of two of the IPPs: IPP 3 (she had not been informed of the fact information was being collected and its intended purposes) and IPP 4 (the recording amounted to the collection of information by unfair means).

The Tribunal and the High Court[150] found that there had been an interference with privacy. Although several defenses were arguable (for example that the recording was necessary for the conduct of legal proceedings) the fact that the defendant did not give evidence in support of them proved fatal to his cause as did the fact that the lawyer's conduct violated the New Zealand Law Society's Code of Ethics. Nevertheless the High Court reduced the Tribunal's award of damages from $7,500 to $2,500.

The Court of Appeal found that the first recording had been made as a result an unsolicited call, by the plaintiff, to the lawyer and the "collection' of information under the Act did not include the receipt of unsolicited information. From a practical and theoretical standpoint this is a valid qualification: the Act cannot have been intended to cover all manner of receipt of personal information and IPPs 1-5 refer only to information that has been "collected". On the other hand the ruling opens a considerable crack in the otherwise seamless operation of the Act as well as a number of fine distinctions that may be impractical: for example there is nothing to prevent a company that receives unsolicited information from a customer from selling the information to a direct marketing firm but where the company has itself further elicited information from the customer this would not be able to be sold.

It should be observed, also, that IPPs 6-11 refer to information that is "held" or which has been "obtained" which suggests that where use and disclosure is concerned it matters not what the source of the information was. In any event in *Harder,* during the phone call the lawyer invited the plaintiff to make a second call and the Court therefore held the information elicited in the context of this conversation was indeed "collected".

---

[148] *L v L* Unreported, AP 95-SW01, High Court, Auckland, Harrison J, 31 May 2002.
[149] [2000] 3 NZLR 80 (CA).
[150] [2000] NZAR 104.

In reversing the Tribunal and High Court's decision,[151] the Court held that there had been no breach of IPP 3 as the plaintiff obviously knew who was collecting the information and why as well as the intended recipients (the lawyer's client). It held that the substance of IPP 3 was concerned with the *fact* of collection rather than the *means* of doing so (tape recording). Likewise the Court found that the making of the recording was not unfair as the purpose of IPP 4 was to prevent individuals from being induced by unfair means into supplying information they would not otherwise have supplied. The Court referred somewhat unrealistically to the analogy where a comprehensive hand-written note is made in which instance there can be no complaint. However the nub of the plaintiff's complaint was not the fact that a detailed record of what was said was kept but rather the potential of the means used (tape recording) to ambush her in subsequent court proceedings!

The waters were further muddied by passing comments made by several of the judges[152] that the information in question may not have been in any event "personal information" subject to the Act: views expressed by the plaintiff, her attitude towards her former partner and her denial of the possession of certain items may not be information about her. Reference was also made to s 14(a) of the Act which requires due regard, when considering whether an interference with privacy has occurred, to social interests that compete with privacy, including the general desirability of a free flow of information and the right of government and business to achieve their objectives in an efficient way.

The decision has been criticized, especially the dicta concerning the limitations to the ambit of "personal information".[153] It is quite possible that the members of the Court confused "personal information" as defined in the Act with "private information" or sensitive information protected at common law, either through the action for confidence[154] or the tort of disclosure of private facts.[155] This may be contrasted with the policy underlying data protection where technological imperatives that enable the tracking and profiling of individuals necessitate protection of even the most banal facts about them.

The relaxed approach of the Court of Appeal as to what is needed to inform data subjects when collecting information has also been criticized: IPP 3(1) should not be about whether or not it is reasonable to inform data subjects of their rights but whether the agency has taken "such steps (if any) as are in the circumstances, reasonable to ensure that the individual concerned is aware of their rights" meaning agencies should not have a discretion not to inform individuals of their rights at all.[156] From the data subject's perspective what would have been a reasonable disclosure would have been the fact the

[151] The defendant was awarded $10,000 in costs.
[152] There was, however, a strong dissenting judgment.
[153] See Roth, above n 21, p W/1910.
[154] *Douglas v Hello* [2005] HRLR 27.
[155] New Zealand has opted for the latter: see *Hosking v Runting* [2005] 1 NZLR 1 (CA).
[156] See Roth, above n 21, p W/1910.

information was being taped which would in itself have implied its potential use in court proceedings.

It may be concluded, with respect, that the Court of Appeal decision in *Harder* has not for the most part been helpful in resolving ambiguities in the Act and demonstrates, at the least, a lack of sympathy for the values underlying data protection law.

Conclusions

This paper has traced the evolution of New Zealand's data protection law from its inception up to the present against its international context. It has been seen that New Zealand's "one size fits all" regime and "one stop shop" dispute resolution mechanisms have on the whole proved able to deal effectively with breaches of data protection principles. The study has highlighted the outstanding success rate of conciliation of disputes which has minimized the need for litigation.

Where litigation has nevertheless occurred, its rate of success is low (although this is probably the case with all litigation) and the monetary remedies obtained modest (although not necessarily so by New Zealand standards). A major function of litigation, though, has been to allow litigants their "day in court" and vindication has been at least as important as monetary compensation.

The majority of litigation has been against the public sector. The reasons for this may vary but they could include the fact that most private sector defendants choose to settle rather than risk the publicity associated with an adverse ruling whereas public sector organizations, more used to bureaucratic procedures are prepared to test matters in the Tribunal. In Hong Kong, a comparable jurisdiction to New Zealand, complaints against the private sector outnumber those against the public sector by around ten to one.[157] Other reasons might be the disproportionate reliance by New Zealanders on the State as well as their suspicion of government and its motives but this is ultimately speculative. The study shows, at any rate, that businesses in New Zealand have not been the target of most data protection litigation.

Other points of differences with overseas experience have been the areas most litigated: denial of access to personal information has predominated whilst improper disclosure of personal information has been a close second. Overseas experience has been the other way around with disclosure being litigated more than the right to access personal data.[158] The reasons for this are, again, obscure but a factor at play might be the fact that a significant number of requests for access to personal information occur in the context of other litigation (frequently employment disputes) and access under the Act is a convenient alternative to the usual discovery process. The dynamics of disputes though often mean that a refusal to grant access results in this taking on a life of its own in substitution or in addition to the underlying or original dispute.

---

[157] Office of the Privacy Commissioner for Personal Data, Hong Kong *Annual Report 2004-05*, p 8.
[158] Ibid, p 9.

Most litigants in New Zealand have been lay litigants who represented themselves before the Tribunal. Where litigants employed representation this tended to be by non-lawyers. The study found that, while representation did not affect the result (a finding that an interference with privacy had occurred) it did substantially influence the monetary compensation awarded to plaintiffs as well as the award of costs. Unsuccessful plaintiffs had significantly higher costs awarded against them which may represent a further disincentive in New Zealand to litigate.

The jurisprudence contained in the body of decisions of the Tribunal provides an invaluable tool for those seeking to understand the scope and enforceability of the information privacy principles. However uncertainty still surrounds some areas and the limited contribution of the courts has, to some extent, not been helpful. The Court of Appeal, in particular, has demonstrated a lack of understanding of core data protection values, notably the meaning of "personal information". Its unduly legalistic approach perhaps vindicates the decision to employ a specialist body such as the Tribunal to consider data protection claims but, on the other hand, this very fact may explain the Court's own lack of experience and lack of sympathy for the policy underlying New Zealand's data protection statute. Despite this qualification there is no doubt that the performance of the Office of the Privacy Commissioner, where most disputes have been successfully conciliated and of the Tribunal, where most of the litigation has occurred demonstrates that the potential of New Zealand's data protection regime has been substantially achieved.

Appendix I

(Processes and Outcomes: Privacy Commissioner)

	30 June 1993-30 June 1994	30 June 1994-30 June 1995	30 June 1995-30 June 1996	30 June 1996-30 June 1997	30 June 1997-30 June 1998	30 June 1998-30 June 1999	30 June 1999-30 June 2000	30 June 2000-30 June 2001	30 June 2001-30 June 2002	30 June 2002-30 June 2003	30 June 2003-30 June 2004	30 June 2004-30 June 2005	30 June 2005-30 June 2006
Number of Complaints Received	513	877	993	1200	1082	1003	798	881	1044	928	934	721	636
Number of Complaints Closed	174	633	972	870	804	895	956	806	1049	915	1168	970	752
Total no. of Complaints Settled	112	583	915	852	765	839	956	770	1033	892	Na	930	720
Settled with Provisional Opinion	12	235	341	184	158	165	181	159	180	175	Na	293	261
Settled Without Provisional Opinion	100	348	574	668	607	674	775	611	853	717	Na	637	459

Appendix II

(Processes and Outcomes: Litigation)

	30 June 1993-30 June 1994	30 June 1994-30 June 1995	30 June 1995-30 June 1996	30 June 1996-30 June 1997	30 June 1997-30 June 1998	30 June 1998-30 June 1999	30 June 1999-30 June 2000	30 June 2000-30 June 2001	30 June 2001-30 June 2002	30 June 2002-30 June 2003	30 June 2003-30 June 2004	30 June 2004-30 June 2005	30 June 2005-30 June 2006
Privacy Commissioner held complaint had substance	16	26	41	27	28	42	44	49	47	52	Na	63	62
Final opinion issued		128	212	133	121	131	146	116	132	145	Na	247	220
Final opinion: complaint had substance	6	26	41	27	28	42	44	49	47	52	Na	184	158
Final opinion: complaint had no substance	30	102	171	106	93	89	102	67	85	93	Na	184	158
No. of Referrals to DHRP	0	0	2	4	7	2	4	0	0	3	0	13	12
No. Taken to HRT by plaintiff		2	4	15	11	13	27	28	22	23	19	9	Not clear
No. of cases HRT found breach		1			0	1	2	2	0	3	2	3	5