submission

Submission by Privacy NSW on the

Review of the Privacy and Personal Information Protection Act 1998

Issue date: 24 June 2004

privacynsw

EXECUTIVE SUMMARY

This submission reviews why we have the Privacy and Personal Information Protection Act 1998 (the PPIP Act), its genesis, and objectives. It asks whether the Act meets its objectives, and how it could be improved.

Part 1

Part 1 reviews why we have privacy legislation, and whether we still need it.

Commitment to the protection of individuals' privacy is not only important for organisations because of their legal obligations. Privacy protection is integral to trust, and trust is the cornerstone of effective relationships. This is true no matter what kind of relationship we are talking about: from personal and family relationships, to commercial transactions, to e-government initiatives involving the relationship between the citizen and the state.

The challenge for government is to build on the balance of privacy, accountability and transparency. People must have confidence in this balance. On one hand, they must know that government is working effectively to provide services and security in a transparent manner. On the other, we must also be able to trust the government to uphold the respect of each individual's rights, including the right to privacy.

From the debates surrounding passage of the PPIP Act can be identified several drivers of the need for legislated privacy protection:

- to meet the challenges posed by the rapid pace of technological change
- to prevent corruption risks as identified by the ICAC
- to meet international expectations and thus ensure fair trade
- to meet public expectations and thus ensure trust in government

Part 1.4 in particular asks: is the PPIP Act improving privacy protection?

The PPIP Act has provided enforceable remedies against State and local government for the first time. However it is difficult to answer the question as to whether or not peoples' privacy is better protected since the introduction of the PPIP Act.

Part 1.4.1 reviews the adequacy of the law, and concludes that the PPIP Act has many loopholes and gaps.

The number and breadth of the exemptions to the information protection principles is detailed elsewhere, but particularly concerning are those exemptions which have the potential to undermine, rather than merely modify, the protection supposed to be afforded under the Act. (For example the ability for the exemptions in sections 4(3)(b) and 28(3) to work together to allow 'information laundering' is discussed in detail in part 3.1.2.)

The ease with which the privacy protection afforded by Parliament the PPIP Act may be overridden either by Parliament itself, or by the government of the day through subordinate legislation and other statutory instruments, has ensured that the level of privacy protection is a moveable feast, but only moving in one direction – away from the highest standards of privacy protection.

Furthermore the PPIP Act has itself been amended without any consultation with the Privacy Commissioner, as has the PPIP Regulation. These amendments have provided further exemptions from the privacy protections afforded by the Act, and diminished the accessibility of an enforceable remedy for people who suffer breaches of the legislated standards.

In short, we argue that the PPIP Act now provides less privacy protection now than it did on the day it fully commenced, 1 July 2000.

Part 1.4.2 reviews the enforcement of the law.

It should be noted that in the four years since the PPIP Act fully commenced, there has not been a single prosecution of the criminal offence provisions in Part 8 of the PPIP Act. This outcome is not because no matters have come to our attention, but because we have not had the ability to deal with such matters adequately.

Part 1.5 looks at the continued need for privacy protection.

We review whether the need for the PPIP Act, as identified in 1998, still exists, and whether there are any new needs. Our conclusion is that six years later, the global environment is such that the need for legislated privacy protection is even greater. We have identified three main aspects of the continued need for the PPIP Act:

- to respect human rights as a way of ensuring security and stability
- to continue to meet the challenges posed by the rapid pace of technological change
- to meet public expectations and thus ensure trust in government

The shock of the terrorist attacks in the United States on 11 September 2001 has in many instances overwhelmed our ability to think dispassionately, to critically analyse the causes of terrorism, and possible solutions to it. The rush to strip away key liberal values such as the rule of law, civil liberties and human rights may be a politically popular way to achieve an illusion of security, but will likely have little positive effect on the threat of terrorism, and may in fact exacerbate it. It is our submission that instead of a threat or 'barrier' to achieving national and international security, human rights are a necessary precondition to global stability and security.

The principles and rights developed over many years by the global community, embodied in documents such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, have served the global community well in the past. They can deliver wisdom and balance in a time of fear and insecurity, in which the immediate and intuitive reaction, formulated in the 'heat of the moment', may not serve democracies well.

This submission argues that the pursuit of universal human rights as a means to achieving a peaceful and stable world is a necessary precondition to better national and international security. The PPIP Act is a small but important link in the accountability framework underpinning human rights in New South Wales.

The pace of technological change is another component of the continued need for the PPIP Act. In these early years of the new millennium, we seem to be bombarded with stories from the frontiers of science and technology – the possibilities of human cloning, even tinier and cheaper hidden cameras, the rebuilding of damaged spinal cords from embryonic cells, iris-scanning machines, cars that know how to navigate streets and whether the driver is falling asleep. Each new development brings with it ethical dilemmas, concerns about abuse of power, and questions about accountability for the use of personal information. Where technological change brings with it the potential to diminish the privacy of individuals, we require careful examination and weighting against other public and private interests.

The third area is with respect to public expectations and trust. The role of a statute such as the PPIP Act is for Parliament to determine where the balance lies between privacy and fair information practices on the one hand, and efficient and effective government and a lawful and safe society on the other.

The question therefore becomes: what level of privacy protection is expected by the public? Has it changed since 1998?

Our submission concludes that Australians place great value in the protection of their privacy, and are unlikely to want their privacy to be traded off for other interests. The implications for government, as it seeks to increasingly conduct government business online through such projects as Health e-Link, are that privacy protection will be paramount in ensuring the public's expectations are met.

Yet we also conclude that public expectations about what constitutes a 'breach of privacy' may not always be reflected in the law. In short, we argue that the PPIP Act provides a lower level of privacy protection than people often think it does.

Thus part 1 argues that although the PPIP Act has worked to improve the protection of privacy for the people of New South Wales, the protections envisaged by Parliament six years ago have not been fully realised. There is certainly room for improvement in both the legislation and in enforcement of the legislation. Furthermore we argue that the pursuit of 'best practice' privacy protection remains an important objective for any government in a modern democracy.

Parts 2 and 3 then attempt to answer the obvious next question: how can the PPIP Act be improved?

Part 2

Part 2 reviews the 'big picture' policy issues relating to the role of Privacy NSW, and the role of privacy laws within the wider context of information management law and policy, with recommendations as to how these issues may be clarified and improved.

Part 2.1.1 examines the Privacy Commissioner's role in government policy. Resources permitting, we prefer to be involved up-front in the design of policy, so that privacy compliance (and indeed best practice) can be 'built-in' rather than 'bolted on'. Early consultation is beneficial for government, as proper policy and project design can minimise reputation risk and other costs to government. In providing policy advice, our aim is to assist

government agencies in meeting their main objectives, while minimising or removing any negative impacts on privacy.

We have found that there is a need for a more formalised role for the Privacy Commissioner in providing comment on government policy proposals that may create a privacy impact. In particular we suggest that the mechanism of Privacy Impact Assessment would bring benefits to the development of policy.

Part 2.1.2 examines the role of the Privacy Commissioner in granting exemptions to the privacy standards set out in the Act, through codes and public interest directions. We have suggested that it would be preferable, in terms of transparency and accountability, for agencies to seek their own legislative authority for any conduct that would otherwise breach the IPPs or public register provisions of the PPIP Act.

Nonetheless we recognise that temporary directions do allow flexibility, and can incorporate a balancing 'public interest' test. However we suggest that the aim of a temporary direction should only be to allow an agency time to achieve compliance, such as a change in their practices, or to seek specific legislative authority through their own legislation. We therefore recommend retaining the power for the Privacy Commissioner to issues public interest directions, but in a slightly amended form.

Part 2.2 reviews the wider framework of information management laws, and concludes that this review of the PPIP Act should examine options for more closely aligning the various information management strands of privacy, FOI and records management. Education, advice and assistance are of paramount importance for organisations trying to understand and implement their obligations under the various Acts.

Part 3

Part 3 provides a comprehensive analysis of each aspect of the PPIP Act, with recommendations for how the objectives of the Act could better be met, in ways which balance the public interest in privacy protection with other public interests, such as the maintenance of law, ensuring public safety, and the efficiency of government services.

Part 3.1 reviews the privacy standards in the Act - the IPPs and the public register provisions. We are particularly interested in the flexibility of the IPPs. The PPIP Act is an instance of principle based legislation being applied in a legal system which is more familiar with applying legal rules. Principle based legislation requires an approach to interpretation which treats the principles as a reference point and guide to seeking particular outcomes but recognises that they can not be imposed absolutely and that their application may need to take into account other principles. The application of legal rules requires a much closer fit between conduct and the rules governing it.

Yet the drafting of the PPIP Act does not consistently reflect the principle based approach inspiring the legislation. The difficulties this creates for interpretation extend to the arrangement and substantive provisions of the Act itself, as many of the exemptions which are necessary to the practical operation of the Act are expressed in a rule based form. Defining the scope of the information protection principles is also affected by the enforcement process under the Act, which unlike similar legislation in other jurisdictions, gives the Tribunal a primary enforcement function and accords a more limited role for the statutory privacy authority.

The drafting of a mandatory 'principle' is thus a difficult task. In effect, the IPPs contain a mix of both core privacy principles, and the prescriptive mechanisms by which each principle is to be obtained. It is our submission that while the core privacy principles are sound, the *mechanisms* by which those principles are expected to be achieved can sometimes be too rigid.

Privacy is a right that affects how individuals interact with organisations, and in that sense is about regulating relationships. This is a complex task to achieve - covering the full spectrum of citizen to government interactions in 12 sections.

Information privacy laws are not one-way or passive laws; they assume some level of responsibility on the citizen to participate in the protection of their privacy. They create a citizen-focussed framework, in which the citizen is expected to give or refuse consent to how their personal information will be collected, used or disclosed. The law therefore assumes that all people are equally capable of exercising their privacy rights within this framework. Yet the law is a blunt instrument, and often cannot take account of the realities of people's lives.

Yet to note that there has been difficulty in complying with the letter of law in terms of the *mechanisms* is not to suggest that the core *principles* themselves are unsound. Privacy NSW has therefore been particularly concerned to ensure that the solution to these challenges is not the creation of wholesale exemptions from the principles themselves. For example we have recently published a best practice guide: *Privacy and people with decision-making disabilities*, which attempts to provide more flexible mechanisms in which to achieve the core privacy principle at issue.

We therefore argue that there should be greater flexibility in how the core privacy standards in the Act can be achieved. We recommend in part 3.1.1 that the Privacy Commissioner be able to make statutory guidelines, with the approval of the Attorney General, which can allow modifications to the *mechanisms* by which privacy principles are to be achieved, but cannot modify the core *principles* themselves.

We have also looked at the structure of the IPPs within the Act. While the IPPs are found in sections 8-19 of the PPIP Act, exemptions to the IPPs are scattered across the Act. We suggest that to alter the structure of the PPIP Act to bring all Act-based exemptions directly under the general rule would be consistent with related legislation, and would make the IPPs easier to find, read, and therefore understand and apply.

Part 3.1.1 also includes a detailed examination of the IPPs, highlighting those IPPs which may not be clear in their intent or effect, and in some cases suggests revision. We also suggest that the Act should be amended to include the 'missing' privacy principle of anonymity, and should have specific provisions regulating data-matching and the use of unique identifiers.

Part 3.1.2 examines the various exemptions to the IPPs. Of particular concern are the exemptions to the definition of 'personal information' itself (see section 4(3) in the Act). It is our submission that while a case could be argued for excluding most of the categories of information covered by these exemptions from the operation of one or more of the IPPs, specific exemptions from the relevant IPPs would be preferable to the current situation, which takes these categories outside the scope of the Act altogether.

For example, information about a person collected from a publicly available publication is a category of information that might be considered reasonable and appropriate to exclude from the normal prohibition in IPP 2 on collection of personal information other than from the person themselves. However the current drafting of section 4(3) allows such information to be used or disclosed in ways which would be considered corrupt and be subject to the criminal offence provisions of the Act, were if not for the exemption.

When the potential scope of this exemption is considered and taken to its logical conclusion, the object of the Act itself – *an Act to provide for the protection of personal information and for the protection of the privacy of individuals generally* – is effectively undermined.

The risk of inaccurate information, or accurate information being misinterpreted or taken out of context, has only increased since the days of paper files. The power of the internet search engine should prompt a re-examination of exemptions relating to the collection, use and disclosure of information about a person from publicly available publications.

Likewise the employment context is one in which many and varied privacy issues arise, given the personal information likely to be held about employees – details of their bank accounts and tax file number, records of sick leave, personal contact details, applications for employment, transfer or promotion, disciplinary information, criminal record or service checks, reference checks, health checks and so on. Not surprisingly, employees as a class commonly appear as complainants or internal review applicants. However the impact of section 4(3)(j) has effectively been to deny privacy protection to employees of government agencies for much of their personal information.

We also have concerns about some of the exemptions in Part 2 of the Act. For example section 25 provides an exceptionally broad exemption, as it effectively allows agencies to rely on even the hint of non-compliance under another Act or regulation to justify their non-compliance with almost all of the privacy principles. This has the effect of subordinating a privacy law intended to confer general rights and have general application, to laws limited to specific situations in a way which undermines public expectations and produces wide ranging uncertainty.

We argue that this exemption should be narrowed to a provision similar to that in the Victorian legislation, which gives priority to other legislation only in cases of express inconsistency. This would appear to have been the Government's intention, as set out in the second reading speech.

Members of Parliament are exempt from the PPIP Act, and so once personal information is in the hands of a minister or the Premier, its use or disclosure is not subject to the scrutiny of privacy law. However a reasonable person might assume that one of the objectives of privacy law is to prevent personal information, held in trust by government agencies, from being made available to a wider class of people not subject to that privacy law (such as ministers or MPs) except where necessary, so as to limit the possibility of such information being collected, used or disclosed in an inappropriate manner.

Yet section 28(3)(b) of the PPIP Act allows any disclosure of any personal information by any public sector agency to the Premier for any reason whatsoever. The result is that privacy law does not stand in the way of the Premier of NSW obtaining the medical records of the Leader of the Opposition or those of his family members, or the criminal history of a powerful media figure, or alcohol counselling notes about a senior public servant.

We argue that the exemption in section 28(3) should be narrowed in scope such as to allow proper briefings from public sector agencies to their respective ministers to continue, and possibly even expanded to clarify an agency's obligations when handling ministerial correspondence on behalf of their minister, while also protecting the privacy of personal information held by those agencies.

Another area of concern is with respect to private sector contractors to state government agencies. The Federal *Privacy Act 1988* does not regulate 'contracted service providers to State agencies' on the assumption that the States will deal with their handling of personal information under State law and/or contractual conditions. The PPIP Act in turn makes state and local government public sector agencies vicariously liable for the actions of their contractors.

However the wording of the PPIP Act does not match the wording of the Federal Privacy Act. There is a risk that some private sector organisations may effectively be caught by both Acts, with their differing privacy standards. However of even more concern is the prospect that some organisations' activities will fall into an unregulated 'gap' between the State and Federal Acts. Likewise we recommend that state-owned corporations, which currently fall into the gap between State and Federal privacy laws, should be covered by the PPIP Act.

Part 3.1.3 reviews the public register provisions of the Act. Typically, individuals have little choice over whether or not their personal information will be held on a public register. For example, it is compulsory to enrol to vote, and enrolled voters are put on the electoral roll; if one wants to build a new house, one must obtain a development consent, and development consents are listed in a register of consents.

Yet as rich sources of personal information, public registers can facilitate the abuse of people's privacy. In particular, once on the internet, the risks to the personal information contained in public registers is great. In the name of accountability and transparency, personal information is published to the world at large, with no control over its secondary use.

With the advent of the internet and its powerful search engines, the home address of a locum GP, or the name of the owner of a particular property, can be collected, used and disclosed by the person's neighbour, boss, bank manager or ex-boyfriend, or complete strangers with no connection at all to that person. This can be a risk not only in terms of privacy, but in terms of security of the person from theft, violence, or identity theft and fraud. We believe that the PPIP Act should prevent against public registers being published in such a way as to facilitate secondary uses of people's personal information without their consent.

At the same time, the current public register provisions of the Act can be seen as too strict, as there is no exemption if the person consents to their information being used or published more broadly. This has led to some fairly ridiculous situations which defy common sense. We therefore argue that the PPIP Act could better balance the accountability of both government agencies and individuals with the protection of privacy.

Part 3.2 looks at enforcement of the privacy standards.

The PPIP Act aims to protect 'personal information'. Enforcement of the privacy standards set out in the Act for information privacy (the IPPs and the public register provisions) is primarily through administrative review. Individual applicants may seek internal review of

conduct or a decision, with binding findings and enforceable remedies available on subsequent application to the Administrative Decisions Tribunal for a fresh review. The result is an adversarial / litigation model.

On the other hand, the PPIP Act also aims to protect 'the privacy of individuals generally'. This is primarily achieved by a complaints-handling and conciliation role for the Privacy Commissioner, not limited to information privacy matters subject to the privacy standards set out in the Act. This role – encompassing the resolution of complaints as varied as bodily privacy, territorial privacy and the privacy of communications – was inherited by the Privacy Commissioner upon abolition of the Privacy Committee, which existed from 1975 to 1999.

In using two models, the PPIP Act seems to be trying to have a bet each way: a specialist, free complaints conciliation service (Privacy NSW), and a mechanism by which complainants can obtain an enforceable remedy and/or large volumes of case law can be generated (external review by the Tribunal) while also acknowledging and trying to address the power imbalance faced by complainant litigants (independent role for the Privacy Commissioner in the Tribunal). Yet it is possible that in trying to please everybody, the processes in the PPIP Act serve nobody.

Our submission outlines some of the deficiencies in these two models - complaint conciliation, and administrative review - for the enforcement of privacy standards and bringing about systemic change. We also pose various options for reform.

In part 3.2.4 we propose an alternative model, in which complaints investigated by the Privacy Commissioner may then be reviewed by the Administrative Decisions Tribunal, as an alternative to the existing path of internal review then review by the Tribunal. This proposal is only in relation to complaints which could otherwise be dealt with by internal review – that is, a complaint about the handling of personal by a public sector agency. That is, we recommend that complainants may choose *either* internal review or an investigation by the Privacy Commissioner, but regardless of their choice they can seek a review by the ADT in order to obtain an enforceable remedy.

Finally, part 3.3 deals with miscellaneous provisions of the Act, including some recommendations for making Privacy Management Plans a more useful accountability tool for public sector agencies.

John Dickie
Acting Privacy Commissioner
23 June 2004

PART 1 OVERVIEW

This part of our submission reviews why we have the Privacy and Personal Information Protection Act 1998 (the PPIP Act), its genesis, and objectives.

1.1 What is privacy legislation for?

1.1.1 What is privacy?

Privacy is recognised as a universal human right. The 1948 Universal Declaration of Human Rights, Article 12, provides:

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

However the jurisprudence of privacy has a longer history than just the last 60 years. In 1362 the Justices of the Peace Act in England punished peeping toms and eavesdropping: those who 'listen under walls or windows, or the eaves of a house', while during the 18th and 19th centuries various European nations enacted laws to protect different aspects of privacy, such as disclosure of private information, and the need to ensure governments only use personal information for legitimate purposes[1].

In 1890 Louis Brandeis, later to become a US Supreme Court judge, and Samuel Warren wrote an essay on 'The Right to Privacy', published in the Harvard Law Review. Warren and Brandeis conceived of privacy as a legal principle - the right to an 'inviolate personality', as part of the more general 'right to be let alone'. They said:

> The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments and emotions shall be communicated to others[2].

However privacy emerged in the latter part of the 20th century as a more complex principle than just physical privacy concerns centred around search and seizure powers. With the advent of telecommunications came concerns about wiretapping, and with information technology in the latter half of the 20th century came concerns about the surveillance potential of computerised databases. The world's first data protection law was passed in Germany in 1970.

There is no simple definition of privacy to cover all circumstances. A number of elements may be considered, including such things as the right to a sense of personal and physical autonomy, the right to have information about oneself used fairly, as well as the 'right to be left alone'.

Sometimes it is easier to talk about privacy in terms of what it is like to suffer a 'breach' of privacy. For example the Prosser test[3] treats the following as breaches of privacy:

---

[1] See Electronic Privacy Information Center and Privacy International, *Privacy & Human Rights 2001: An international survey of privacy laws and developments*, Washington DC 2001, p5.
[2] Samuel Warren and Louis Brandeis, "The Right to Privacy", *Harvard Law Review*, 4, 1890, pp 193-220.

- the intrusion upon a person's seclusion or solitude, or private affairs
- public disclosure of embarrassing facts about a person
- publicity which places a person in a false light in the public eye
- appropriation of a person's name or likeness.

Another way of thinking about privacy is to focus on the different dimensions to privacy. These different aspects of privacy are reflected in a variety of laws, policies and norms in our society[4]. For example:

- **privacy of the person** : spatial privacy is a concept in planning laws, territorial privacy is reflected in residential tenancy leases, physical privacy is reflected in the criminal laws of battery and assault and policies about bag searches in shops, and bodily privacy is an issue in relation to laws regulating the collection and use of human tissue and DNA samples and protection against other invasive procedures
- **privacy of personal behaviour** : some degree of a right to privacy is reflected in media and defamation laws, as well as laws which restrict the use of surveillance
- **privacy of communications** : this is reflected in laws governing listening devices and telephone and mail interception
- **privacy of personal information** : this is usually the subject of 'privacy laws' which regulate the fair use of personal information, following the information life cycle from collection and storage through to use and disclosure.

In relation to information privacy, many people confuse privacy with secrecy or confidentiality, but privacy is broader than both of these. Information privacy protection focuses on the need to ensure the fair use of personal information. The fair use of information is an essential element of an information economy just as the fair use of money or honesty is an essential element of the financial economy.

So privacy *laws*, in the sense that we generally know them, are usually about how organisations handle personal information.

1.1.2 What are privacy laws about?

Privacy laws, like the Privacy and Personal Information Protection Act 1998 (the PPIP Act), are about ensuring organisations act fairly in the way in which they collect, store, use and disclose our personal information, as well as ensuring the accuracy of that information before it is used, and allowing us to see the information held by governments and businesses about ourselves. As organisations gather more and more data about us, control over its use and misuse becomes increasingly important.

As American author Jeffrey Rosen states,

> Privacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can be easily confused with knowledge.[5]

---

[3] The Prosser test refers to an influential definition of privacy developed by American legal academic William Prosser.

[4] See for example D Banisar, *Privacy and Human rights: an international survey of privacy laws and developments*, Electronic Privacy Information Center, Washington, 2000.

Privacy laws are about respecting people's choices; allowing each of *us* to be the best judge as to what information about ourselves we share with other people. In that sense, privacy is a right which underpins the sense of personal autonomy and individual dignity that make us free individuals. The protection of privacy is about shifting the locus of power away from governments and corporations, and back to citizens and consumers.

Commitment to the protection of individuals' privacy is not only important for organisations because of their legal obligations. Privacy protection is integral to trust, and trust is the cornerstone of effective relationships. This is true no matter what kind of relationship we are talking about: from personal and family relationships, to commercial transactions, to e-government initiatives involving the relationship between the citizen and the state.

The challenge for government is to build on the balance of privacy, accountability and transparency. People must have confidence in this balance. On one hand, they must know that government is working effectively to provide services and security in a transparent manner. On the other, we must also be able to trust the government to uphold the respect of each individual's rights, including the right to privacy.

When people's private information is involved, this trust can only be achieved through a commitment to the fair and responsible handling of personal information.

1.1.3 What is the PPIP Act about?

As noted above, what we tend to think of as 'privacy' laws generally only impose standards in relation to the privacy of personal information. The PPIP Act fulfils this role by imposing information privacy standards on State and local government agencies in NSW.

However PPIP Act is unusual in that not only does it impose standards in relation to information privacy, it also allows the Privacy Commissioner to deal with other matters that relate to the broader notion of 'privacy' described above at part 1.1.1 of this submission.

1.2 The genesis of the PPIP Act

1.2.1 The NSW Privacy Committee

In 1969 Sir Zelman Cowen delivered the Boyer Lectures, titled 'The Private Man'. In 1972 the Standing Committee of Attorneys General (SCAG) commissioned a report on privacy. In 1973 the Morrison Report was delivered to Hon J Maddison, the NSW Minister of Justice, recommending 'general legislative provision for the protection of privacy of the individual against threats existing and foreseeable'.

In 1974 the NSW Privacy Committee was established on an administrative basis, and in 1975 the NSW Parliament passed the *Privacy Committee Act*. The Privacy Committee had research and policy functions, as well as the power to conciliate complaints about breaches of privacy. The Act did not set out any standards or definitions by which privacy might be measured, and the Committee's decisions were not enforceable.

---

[5] Jeffrey Rosen, *The Unwanted Gaze*, Random House, New York 2000

In 1982 the NSW Privacy Committee, in its Annual Report, issued its first call for legislative protection of privacy. In 1988 the Federal *Privacy Act* was passed, largely in response to the Australia Card debate. The Federal Privacy Act was the first to establish legislated privacy principles.

In 1992 the NSW Independent Commission Against Corruption (ICAC) finalised its investigation into the unauthorised release of, and corrupt trade in, government information. The ICAC recommended privacy law as a precondition to rebuilding public trust in government:

> … efficient data security and protection, and … a consistent and effective body of law to control the handling of confidential government information … are necessary to overcome the corrupt trade that has developed. They are also necessary to meet the community's expectation that the Government will respect and maintain the confidentiality of the increasing amounts of personal and commercially sensitive information the Government and its agencies hold.[6]

During 1991 and 1992 the Coalition MP Andrew Tink introduced Private Member's Bills for privacy protection into the NSW Legislative Assembly. In 1994 the Coalition Government, through Attorney General John Hannaford, introduced the Privacy and Data Protection Bill, which was referred to a Select Committee of the Legislative Council. The Committee took evidence but no report was tabled before the Parliament was dissolved for the 1995 State election, in which the Coalition Government was defeated.

In 1996 a draft Privacy and Personal Information Protection Bill was circulated within government by Labor MLC Attorney General Jeff Shaw for comment. In 1998 the *Privacy and Personal Information Protection Act* was passed.

1.2.2 The OECD Guidelines

Information privacy legislation like the PPIP Act can only be understood within the context of international agreements and standards, which have led to the passage of broadly similar privacy legislation in most developed countries.

The agreement which did most to shape privacy law prior to 1995 was the 1980 OECD *Guidelines on the protection of privacy and transborder flows of personal data.* The OECD Guidelines were developed by a group of government experts under the chairmanship of the Hon Mr Justice Michael Kirby, then Chairman of the Australian Law Reform Commission.

The explanatory memorandum to the 1980 OECD Guidelines states:

> The remedies under discussion are principally safeguards for the individual which will prevent an invasion of privacy in the classical sense, i.e. abuse or disclosure of intimate personal data; but other, more or less closely related needs for protection have become apparent. Obligations of record-keepers to inform the general public about activities concerned with the processing of data, and rights of data subjects to have data relating to them supplemented or amended, are two random examples. Generally speaking, there has been a tendency to broaden the traditional concept of privacy ("the right to be left alone") and to identify a more

[6] Ian Temby QC Commissioner, Independent Commission Against Corruption, *Report on Unauthorised Release of Government Information*, August 1992; see Chapter 12 : The right to privacy, page 176 in Volume 1.

> complex synthesis of interests which can perhaps more correctly be termed privacy and individual liberties.[7]

The OECD Guidelines were intended to promote the free flow of information between member states of the OECD, while also being consistent with the protection of personal information within states, some of which had already adopted data protection or information privacy laws. They sought to achieve this by establishing minimum standards (Article 6) in the form of a set of principles on how personal information should be collected, stored, used, and disclosed (Articles 7 to 14). Exceptions to the principles were to be as few as possible (Article 4).

Consistently with this purpose, and in response to advances in computerisation of information, the Guidelines adopted a wide definition of personal data designed to cover all forms of information through which individuals were personally identifiable:

> 1(b) "personal data" means any information relating to an identified or identifiable individual (data subject)

This broad definition reflected the varying social and cultural views on privacy held by OECD member states and the impossibility of achieving consistent standards for international flows of information if each state imposed a different interpretation of the subject of regulation.

The increasing importance of international conventions as a source of local law has seen an expansion of principle-based approaches in common law jurisdictions. Thus Articles 2 and 3 of the OECD Guidelines provide that a purposive and principle-based approach should be adopted to the application of the Guidelines to personal information which takes into account the context in which they are intended to operate.

The OECD considered the purpose of member states' information privacy laws to be:

> to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.

1.2.3 The European Union Directive

In 1995 the European Union adopted *Directive 95/46 /EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (the EU Directive). The EU Directive required all EU members to adopt a consistent set of principles for the protection of personal information. The EU Directive added some additional principles to the OECD principles, and extended the obligations to manual as well as computerised record systems.

Article 25 of the EU Directive restricted disclosures of personal data from EU states to external jurisdictions which did not have an adequate level of legal protection for such data. Article 25 was seen as applying pressure on the trading partners of EU states to adopt broadly similar forms of legislative protection. This proposition was particularly persuasive in jurisdictions which wanted to emphasise their advantages as centres for global information technology, through a demonstration of EU adequacy.

---

[7] See http://www.oecd.org/document/18/0,2340,en_2649_37409_1815186_1_1_1_37409,00.html

1.2.4 Adoption of OECD principles into Australian jurisprudence

A version of the OECD principles was adopted by the Australian Law Reform Commission in its 1983 *Report on Privacy*, and these were adapted as the information privacy principles in the Federal *Privacy Act 1998* (Cwth) in relation to Australian Government agencies.

The PPIP Act was enacted against the prospect of the EU Directive coming into force in 1998 and at a stage when the Australian Government had postponed proposed privacy legislation to cover the private sector. Although the OECD Guidelines and the EU Directive were not directly mentioned, the intention to conform to international standards was clearly indicated by Attorney General the Hon J R Shaw said when introducing the Bill for the PPIP Act:

> The purpose of the bill is to promote the protection of privacy and the rights of the individual by the recognition, dissemination and enforcement of data protection principles consistent with international best practice standards.[8]

The PPIP Act adopted, with few modifications, the same principles as contained in the Federal Privacy Act. In the case of the PPIP Act, the principles are known as the information protection principles (IPPs) - see Part 2 Division 1 of the PPIP Act. The broad definition of 'personal information' also reflects the OECD Guidelines.

The fact that Parliament adopted information privacy legislation in the form of the PPIP Act is a clear indication that it intended to protect the privacy of personal information held by the public sector by imposing responsibilities on agencies rather than on their employees as individuals. It continued the established tradition in Australian law of treating privacy as a statutory rather than a common law right[9].

1.2.5 The need for the PPIP Act

From the debates surrounding passage of the PPIP Act can be identified several drivers of the need for legislated privacy protection:

- to meet the challenges posed by the rapid pace of technological change
- to prevent corruption risks as identified by the ICAC
- to meet international expectations and thus ensure fair trade
- to meet public expectations and thus ensure trust in government

For example in his second reading speech, the Attorney General the Hon Jeff Shaw QC MLC stated:

> … it is now apparent that more detailed and extensive legislation is needed in order to address the demands of evolving information technologies, community and international expectations for effective privacy safeguards…

---

[8] NSW Legislative Council Hansard Article No.44 of 17/09/1998 at page 7598.

[9] Aggrieved individuals have no avenue at common law to take civil action against individual public servants for breaches of personal information privacy. An agency does, however have the power, and in appropriate cases the responsibility to discipline staff for breaches of the IPPs, or refer them for prosecution for a breach of the offence provisions contained in the Act.

> Information technology has made records of personal information more vulnerable to abuse as it enables the storage of vast amounts of personal data at low cost for indefinite periods of time …
>
> The government is itself one of the main collectors and users of personal information. I consider that effective safeguards in relation to that information are a vital part of government's compact with the community.[10]

The Attorney General also referred to the 1992 ICAC report, outlined above at part 1.2.1 of this submission, and to national moves to regulate the private sector.

1.3 Recent developments in other jurisdictions

Since the PPIP Act commenced, there have been five major developments within Australian jurisdictions:

- national information privacy laws for the private sector[11]
- information privacy laws for the Victorian public sector[12]
- health-specific information privacy laws for the Victorian public and private sectors[13]
- information privacy laws for the Northern Territory public sector[14]
- health-specific information privacy laws for the NSW public and private sectors[15]

Other jurisdictions, including South Australia and Western Australia, have also been reviewing how information privacy laws might work in their States.

Each of these developments is evidence of the continued and growing need for legislated privacy protection, in the form of fair information handling principles for both public and private sector organisations.

1.4 Is the PPIP Act improving privacy protection?

At a very simple level the answer must be 'yes', because the PPIP Act has provided enforceable remedies against State and local government for the first time. Yet it is actually difficult to answer the question as to whether or not peoples' privacy is better protected since the introduction of the PPIP Act.

On one hand it could be argued that the volume of complaints against State and local government agencies now dealt with through the internal and external review mechanisms

---

[10] NSW Legislative Council Hansard Article No.44 of 17/09/1998 at page 7600.
[11] The Federal Privacy Act 1988 was extended to cover the private sector from 21 December 2001.
[12] The Victorian Information Privacy Act 2000 commenced its regulation of the Victorian public sector in September 2002.
[13] The Victorian Health Records Act 2001 commenced its regulation of the handling of health information in Victoria in July 2002**.**
[14] The Northern Territory Information Act commenced its regulation of the Northern Territory public sector on 1 July 2004, with local authorities covered from 1 July 2005.
[15] The NSW Health Records & Information Privacy Act 2002 (HRIP Act) is due to commence on 1 September 2004.

unique to the PPIP Act are a measure of success[16]. On the other hand it could be argued that successful privacy protection should be measured by the absence of complaints. (For more on this point see part 3.2 of this submission.)

In the absence of any baseline data as to perceptions of privacy protection before the Act commenced, even a survey of community attitudes now would not answer whether or not people *believe* their privacy to be better protected now than it was in 1998.

Nor could a survey of public sector agency information-handling practices, to determine whether those practices have improved since July 2000, provide a complete picture of the effectiveness or otherwise of the PPIP Act. As noted above, the PPIP Act is unusual in that not only does it impose standards in relation to information privacy, it also allows the Privacy Commissioner to deal with other matters that relate to the broader notion of 'privacy' described above at part 1.1.1 of this submission. The Act's objectives include not only the protection of personal information, but the protection of privacy generally. Therefore it would be an artificial exercise to attempt to survey the impact of the PPIP Act with respect to information privacy alone. The protection of privacy is being achieved, or at least attempted, through a myriad of laws, including not only the PPIP Act but the Workplace Video Surveillance Act, the Listening Devices Act, the Federal Privacy Act, and so on.

In the absence of empirical data, we provide this submission by way of an answer to the key question. We have endeavoured to make this submission as comprehensive as possible, incorporating and synthesising the results of Privacy NSW's experience in dealing with the PPIP Act day-in, day-out, since its inception.

1.4.1 The adequacy of the law

From the perspective of Privacy NSW, the PPIP Act has many loopholes and gaps.

The number and breadth of the exemptions to the information protection principles is detailed in part 3.1.2 of this submission. Particularly concerning are those exemptions which have the potential to undermine, rather than merely modify, the protection supposed to be afforded under the Act[17]. Furthermore the essentially adversarial nature of the model of complaints-resolution introduced in the PPIP Act provides an incentive for government agencies to ensure that each one of these exemptions is pushed to its limit, rather than construed narrowly[18].

The ease with which the privacy protection afforded by Parliament the PPIP Act may be overridden either by Parliament itself[19], or by the government of the day through subordinate legislation and other statutory instruments[20], has ensured that the level of privacy protection is a moveable feast, but only moving in one direction – away from the highest standards of privacy protection.

---

[16] For more about the volume of matters generated under the PPIP Act see Privacy NSW's 2002-03 Annual Report page 10, which analyses the trends since the Act commenced on 1 July 2000.
[17] See for example the ability for the exemptions in sections 4(3)(b) and 28(3) to work together to allow 'information laundering', discussed in part 3.1.2 of this submission.
[18] See more on this point at part 3.1.2 and part 3.2 of this submission.
[19] See section 25 of the PPIP Act.
[20] See section 25 of the PPIP Act in relation to other laws, section 29 in relation to the ability of the Attorney General to provide exemptions through codes, and section 41 in relation to the ability of the Privacy Commissioner to provide exemptions through public interest directions.

Furthermore the PPIP Act has itself been amended without any consultation with the Privacy Commissioner[21], as has the PPIP Regulation[22]. These amendments have provided further exemptions from the privacy protections afforded by the Act, and diminished the accessibility of an enforceable remedy for people who suffer breaches of the legislated standards.

In short, the PPIP Act provides less privacy protection now than it did on the day it fully commenced, 1 July 2000.

1.4.2 Enforcement of the law

The enforcement of the PPIP Act rests with the NSW Privacy Commissioner. In this respect the Commissioner's functions include:

- assisting members of the public understand their rights under the Act
- assisting public sector agencies on implementing and complying with the privacy standards set out in Parts 2 and 6 of the Act
- oversighting the internal review mechanism for complaints resolution established under Part 5 of the Act
- assisting the Administrative Decisions Tribunal in its external review of complaints under Part 5 of the Act
- investigating and conciliating other complaints about breaches of privacy under Part 4 of the Act
- conducting inquiries into privacy related matters
- investigating and prosecuting breaches of the offence provisions in Part 8 of the Act (the crimes of corrupt disclosure, etc)

The work done by Privacy NSW in carrying out most of these functions is described in more detail our 2002-03 Annual Report. However the final two functions perhaps provide the best litmus test of how adequately the PPIP Act is being enforced.

In the four years since the PPIP Act fully commenced, there has not been a single prosecution of the criminal offence provisions in Part 8 of the PPIP Act. This outcome is not because no matters have come to our attention, but because we have not had the ability to deal with such matters adequately.

Privacy NSW has not been resourced to the level necessary to attempt the level of forensic investigations or examinations necessary to consider mounting a prosecution of criminal offences, which require particular skills, time[23], facilities[24], and powers[25]. Likewise the

---

[21] The Privacy and Personal Information Protection Amendment (Prisoners) Act 2002 withdrew the ability for prisoners, their family members and associates from seeking compensation for any breach of their privacy. Privacy NSW was not consulted about this amendment.

[22] The Privacy and Personal Information Protection Regulation 2000 was amended in December 2003 to exempt the Attorney General's Department from the public register provisions in relation to the register of JPs. Privacy NSW was not consulted about, or notified of, this amendment.

[23] In the past four years, depending on the budget available each year, Privacy NSW has employed between one and three fulltime investigations officers to handle complaints and the oversight of internal reviews, as well as (with other officers) answering telephone enquiries, answering requests for advice, and participating in inter-departmental working parties and the like.

Privacy Commissioner has held no public or private hearings, despite having the powers to do so.

Attempts to seek the cooperation of other agencies with the powers and resources to conduct investigations and/or prosecutions of the offences in Part 8 of the Act (such as NSW Police, the Police Integrity Commission, the ICAC and the Director of Public Prosecutions) have not to date been fruitful. There are some good reasons why these agencies cannot resolve our difficulties; for example the ICAC only regulates public sector officials. By contrast the offences in Part 8 of the PPIP Act relate in some cases to public sector officials (such as corruptly disclosing or using personal information), but in other cases relate to people outside the public sector (such as inducing a corrupt use or disclosure). Nonetheless two matters referred to the ICAC for investigation as possible breaches of the ICAC Act and/or Part 8 of the PPIP Act by public sector officials were declined[26].

The result is that Privacy NSW is aware of several instances where conduct may amount to a criminal offence, but to date has not been able to progress those matters.

1.5 The continued need for privacy protection

As outlined above at part 1.2.5 of this submission, the need for the PPIP Act, as identified in 1998, were:

- to meet the challenges posed by the rapid pace of technological change
- to prevent corruption risks as identified by the ICAC
- to meet international expectations and thus ensure fair trade
- to meet public expectations and thus ensure trust in government

The question posed here is whether those needs still exist, and whether there are any new needs.

It is our submission that each of the above needs does still exist six years later, and indeed the global environment is such that the need for legislated privacy protection is even greater. We have identified three key drivers in 2004:

- to respect human rights as a way of ensuring security and stability

---

[24] Although the PPIP Act provides the Privacy Commissioner with Royal Commission-type powers to conduct public or private hearings, Privacy NSW has no budget allocation to facilitate the hiring of hearing rooms, interpreters, transcribers, counsel assisting, and so on.

[25] Unlike the Independent Commission Against Corruption, Privacy NSW does not have surveillance capacity, or the power to issue or seek search warrants, listening devices, or telephone interception.

[26] One of these matters was referred to the ICAC by Privacy NSW once we became aware, through media reports, that the ICAC was investigating a similar incident (unauthorised disclosure of personal information to the media) by the same public sector agency. However the ICAC returned the matter to Privacy NSW on the basis that the ICAC had determined not to take any action in respect of the matter, because the agency concerned had investigated itself, and had found that the disclosure was not 'motivated by improper or corrupt conduct'. The second matter was referred to the ICAC by a local council following its internal review of a complaint. The ICAC declined to deal with the matter on the basis that the matter was already with Privacy NSW. However our only role was to oversight the internal review process; we had no formal complaint to invoke our investigation functions. For a full description of that case see pp 33-35 of the Privacy NSW 2002-03 Annual Report.

- to continue to meet the challenges posed by the rapid pace of technological change
- to meet public expectations and thus ensure trust in government

1.5.1 Human rights and global security

David Loukidelis, the Information and Privacy Commissioner for British Columbia, Canada has expressed well the link between privacy and healthy democracies:

> privacy is not just a matter of individual rights. Our ability to keep our thoughts and beliefs private is of course crucial to the health and success of our communities and our democratic way of life. Citizens need to be free to think about issues and express themselves privately without fear of state surveillance, in the ordinary course, in order to participate fully and freely in public life. Without an appropriate sphere of privacy for each of us as individuals, we cannot have healthy and free societies.[27]

Privacy is thus a right which underpins other human rights and values upon which liberal democracies are founded, such as freedom of speech and expression, freedom of association, equal opportunity and the peculiarly Australian notion of 'a fair go'. These rights and values are necessary for societies to pursue representative government and peaceful change, through democratic means of expressing dissent under the rule of law, and thus maintain security and stability.

Yet in recent years many people have come to see privacy in particular, and human rights and civil liberties in general, as somehow opposed to security and stability. In social and political terms, the single biggest challenge to the protection of privacy since the PPIP Act commenced has been the aftermath of the terrorist attacks in the United States on 11 September 2001.

Fear of terrorism and of crime has been used, often without critical analysis, as the justification for increasing government powers of surveillance and control over individuals. Yet we submit that privacy and security need not be seen as an either/or proposition.

In the mid 19th century, Frederick Douglass said, in relation to the enslavement of African-Americans:

> Where justice is denied … neither persons nor property will be safe.

The same sentiment is true of any situation in which the rule of law is supplanted by the dictates of mob rule, driven by populism and fear.

The rhetoric of 'law and order' and terrorism politics suggests that 'if you've got nothing to hide, you've got nothing to fear'. In a sense that is true. However we believe there is no such creature as a person who has nothing to hide. People naturally draw distinctions between the parts of themselves they share with a neighbour or friend, and what aspects of their lives they may display to their doctor, their employer, the government or a stranger.

---

[27] David Loukidelis, Information and Privacy Commissioner for British Columbia, "Privacy and law enforcement - getting the balance right", speech at the 24th Annual Training Symposium of the BC Crime prevention Association, Surry BC, 19 September 2002.

The need for private space, hidden from view of others, is an inherent aspect of being human; it does not mean we are doing anything 'wrong'. The freedom to conduct ourselves, to think, speak and express ourselves 'in private', is essential to human dignity, personal autonomy and identity.

The danger of laws and practices which erode our privacy, whether they be street surveillance or the sharing of personal information between government agencies, is that they treat the average person as a suspect rather than a citizen. In such circumstances the government treats us all 'as if we are hiding something'[28].

As then Professor Zelman Cowen said in the 1969 Boyer lectures,

> A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars[29].

The shock of the terrorist attacks in the United States on 11 September 2001 has in many instances overwhelmed our ability to think dispassionately, to critically analyse the causes of terrorism, and possible solutions to it. The rush to strip away key liberal values such as the rule of law, civil liberties and human rights may be a politically popular way to achieve an illusion of security, but will likely have little positive effect on the threat of terrorism, and may in fact exacerbate it[30].

The framing of debate over law enforcement is often couched in terms of a trade-off between liberty and security. Yet there has equally been historical opposition to such a notion. Benjamin Franklin, in the Historical Review of Pennsylvania, 1759 stated:

> They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.

One recent review of counter-terrorism theory and practice suggests that there is near unanimity amongst terrorism experts that

> any campaign against terrorism, if it were to be successful, (must) adhere strictly to liberal democratic principles and the rule of law[31].

The rule of law – embodied in laws and practices such as the exposure of government decisions to public scrutiny and judicial or administrative review – is not only about protecting individual rights. Public accountability

> can produce a fuller record, expose faulty assumptions, and slow the rash decision making of elected officials acting under pressure[32].

---

[28] Dr Caoifhionn Gallagher, "Nothing to hide, nothing to fear? Privacy v. Government", in *Liberty*, Autumn 2003.
[29] Zelman Cowen, 1969, 'The Private Man', *The Boyer Lectures*, Australian Broadcasting Commission, pp 9-10.
[30] See for example the current debate in the UK in relation to identity cards, in particular the report from Privacy International in April 2004, "Mistaken identity; exploring the relationship between national identity cards and the prevention of terrorism".
[31] Christopher Michaelsen, "International human rights on trial – the United Kingdom's and Australia's legal response to 9/11", *Sydney Law Review*, Vol 25 : 275, 2003, p 276.
[32] James X Dempsey, "Civil liberties in a time of crisis", *Human Rights*, Vol 29(1), 2002.

Jenny Hocking, an academic at Monash University, Melbourne, critiqued the then proposed dramatic expansion of Australia's domestic security powers under the various bills put to the Federal Parliament in March 2002, thus:

> These proposals are unprecedented and dangerous, they reveal an impatience with and a lack of confidence in the criminal justice system, proposing a primitive, militaristic, notion of justice in its place. These counter-terrorism measures would immensely expand Executive power, imperil the rule of law, offend established political and civil rights, compromise the separation of powers and weaken established judicial procedures. As such, these contemporary counter-terrorism developments represent a most significant threat to the proper relations between the arms of governance, in particular between the Executive and the judiciary, in a way not seen since Liberal Prime Minister Robert Menzies' several failed attempts to pass the Communist Party Dissolution Act 1950 at the height of the cold-war[33].

It is our submission that instead of a threat or 'barrier' to achieving national and international security, human rights are a necessary precondition to global stability and security. William Shultz, of Amnesty International, has stated:

> To insist that global threats be met by global responsibility is at the heart of the human rights ethos.[34]

The global commitment made to upholding universal human rights, born in the wake of the horrors of World War II, which were far greater in scale than any events of recent years[35], has fresh impetus now. The principles and rights developed over many years by the global community, embodied in documents such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, have served the global community well in the past. They can deliver wisdom and balance in a time of fear and insecurity, in which the immediate and intuitive reaction, formulated in the 'heat of the moment', may not serve democracies well.

It is thus our submission that the pursuit of universal human rights as a means to achieving a peaceful and stable world is a necessary precondition to better national and international security. The PPIP Act is a small but important link in the accountability framework underpinning human rights in New South Wales.

1.5.2 Technological change

In these early years of the new millennium, we seem to be bombarded with stories from the frontiers of science and technology – the possibilities of human cloning, even tinier and cheaper hidden cameras, the rebuilding of damaged spinal cords from embryonic cells, iris-scanning machines, cars that know how to navigate streets and whether the driver is falling asleep. Each new development brings with it ethical dilemmas, concerns about abuse of power, and questions about accountability for the use of personal information. Where technological change brings with it the potential to diminish the privacy of individuals, we require careful examination and weighting against other public and private interests.

---

[33] Jenny Hocking, *Counter-terrorism: securing the state or the death of democracy?*, presentation at the Activating Human Rights and Diversity Conference, Southern Cross University, July 2003.
[34] William Schulz, *Tainted Legacy: 9/11 and the Ruin of Human Rights*, Nation Books, 2003, extracted in *The Human Rights Defender*, Vol. 23(2), April 2004.
[35] For example one writer has suggested that World War II caused more than 1 million deaths per month, equivalent to a Bali bombing every 10 minute for four years; see Chris Leithner, "The Terror Trap", *Policy*, Vol 19(1) : 34-36.

It is fair to say that the privacy risks and challenges posed by technological developments in 1998 have not lessened since 1998. Some of the applications either proposed or implemented in NSW government agencies in recent years, with considerable privacy implications, include:

- the use of 'smart card' technology across publicly and privately owned public transport
- the use of iris recognition to identify visitors in gaols
- the use of electronic tolling on Sydney roads
- the introduction of point-to-point speech cameras
- the development of electronically-linked health records
- the DNA testing of decades-old blood samples taken from newborn babies for medical screening purposes
- the introduction of voluntary photographic identification cards
- the provision of fingerprints and DNA samples of NSW suspects to a national database

It is therefore our submission that there is a continuing need for the PPIP Act, as a way of guiding government agencies in the fair information practices to be followed when applying new technologies to social goods and services.

1.5.3 Public expectations and trust

The role of Privacy NSW and the Privacy Commissioner is not to be a one-eyed advocate for the protection of privacy against all other interests. We accept that the collection, use and disclosure of personal information by government is necessary for the proper functioning of government in many respects.

For example the role of privacy laws and policies has been explained thus:

> the choice is not between surveillance powers and no surveillance powers. … Instead, privacy advocates urge that those powers be focused and subject to clear standards and judicial review.[36]

Indeed the role of a statute such as the PPIP Act is for Parliament to determine where the balance lies between privacy and fair information practices on the one hand, and efficient and effective government and a lawful and safe society on the other.

'Balance' is thus a key concept in privacy legislation. When introducing the then PPIP Bill, then Attorney General Jeff Shaw stated that

> This bill will achieve an effective and reasonable balance in the circumstances.

The challenge for government is to build on the balance of privacy, accountability and transparency. People must have confidence in this balance. On one hand, they must know that government is working effectively to provide services and security in a transparent

[36] James X Dempsey, "Civil liberties in a time of crisis", *Human Rights*, Vol 29(1), 2002.

manner. On the other, they must also be able to trust the government to uphold the respect of each individual's rights, including the right to privacy. When people's private information is involved, this trust can only be achieved through a commitment to the fair and responsible handling of personal information, meeting the public's expectations for the reasonable protection of their privacy.

The question therefore becomes: what level of privacy protection is expected by the public? Has it changed since 1998?

Far from being the 'death of privacy', the few years since September 2001 has actually seen an increase in the volume of informal enquiries made to Privacy NSW, as well as rapid growth in the number of privacy complaints proceeding to the Administrative Decisions Tribunal for review. However these are not the only measures by which one can assess the state of public expectations or concerns about privacy.

Surveys conducted by the Office of the Federal Privacy Commissioner in 2001 indicated that 68% of Australians regard the use of their personal information for a purpose other than that for which it was originally intended as a breach of their privacy, while around 90% of Australians believe it is important that they know how their personal information might be used by the organisation collecting it, as well as to whom else it might be disclosed. The survey also suggested that 42% of Australians have refused to deal with organisations they felt did not adequately protect their privacy[37].

In the last Australian census, also conducted in 2001, there was a question about whether or not each person consented to the government keeping their individually identified census form and releasing it in 99 years, rather than having it pulped as soon as the statistical data was collected, as has been the practice before. Almost half of all Australians take their privacy so seriously that they refused to let the government keep their census forms for 99 years. It is interesting to note that the response rate differs across the population, according to both age and ethnicity. Less than 40% of people born in England said 'no', but almost 60% of those born in Vietnam said 'no'. The 'no' response rate also increased with the age of the respondent, with the exception of the 0-5 years old group.

A more recent survey, which compared Australians' attitudes and expectations about privacy with people in four other countries, suggests that Australians in general place greater store in the protection of privacy, and are less likely to want their privacy to be traded off for other interests[38]. The 2003 survey found Australians less likely than the total sample to agree that identity cards are necessary to main national security, or help to guard against either terrorism or illegal immigration[39]. Australians were also more likely to see identity cards as an infringement on their personal liberty, and to be unwilling to trade-off privacy for convenient services.

---

[37] Office of the Federal Privacy Commissioner, "The results of research into community, business and government attitudes towards privacy in Australia", 31 July 2001, available at www.privacy.gov.au

[38] Drs Milagros (Millie) Rivera Sanchez, Hichang Cho and Sun Sun Lim, from the Information and Communication Management Programme at the National University of Singapore, conducted the research, which was funded by NUS's Faculty of Arts and Social Sciences. The survey was carried out across five countries by AC Nielson in May 2003: Australia, Singapore, South Korea, the United States and India.

[39] The comments made in this submission reflect the author's analysis of the raw data provided by the NUS research team to Privacy NSW and the Office of the Federal Privacy Commissioner.

The same survey suggests that 93% of Australians, compared with 86% of the total sample across five countries, believe that the law should protect the privacy of consumers online. Furthermore the majority of Australians, at even higher rates than their counterparts in the other countries surveyed, are more likely to shop online if consent is required to the disclosure of their personal information (86% agree), and would be even more comfortable about conducting transactions online if vendors were required by law to notify their customers of any breach of security that could compromise their personal information (92%). Almost 80% of Australians believe that privacy laws help to make e-commerce safer.

These results have implications for the Government as it seeks to increasingly conduct government business online, through such projects as Health e-Link and the Government Licensing System.

Indeed the link between a prosperous economy and a government that inspires confidence and trust has been confirmed by the Australian Treasurer and the Productivity Commission[40].

Yet public expectations about what constitutes a 'breach of privacy' may not always be reflected in the law. For example of all the matters which proceeded to internal review in 2002-03, in 70% of cases the conduct complained of was found to have occurred, yet in only 18% of cases the conduct was found to have been in breach of the information protection principles without lawful excuse[41]. This suggests that many complainants' expectations about how the law is supposed to protect their privacy is not being met by the PPIP Act.

In short, the PPIP Act provides a lower level of privacy protection than people often think it does.

1.6 Room for improvement

This part of our submission has argued that although the PPIP Act has worked to improve the protection of privacy for the people of New South Wales, the protections envisaged by Parliament six years ago have not been fully realised. There is certainly room for improvement in both the legislation and in enforcement of the legislation. Furthermore we argue that the pursuit of 'best practice' privacy protection remains an important objective for any government in a modern democracy. The remainder of this submission attempts to answer the obvious next question: how can the PPIP Act be improved?

Part 2 of this submission reviews the 'big picture' policy issues relating to the role of Privacy NSW, and the role of privacy laws within the wider context of information management law and policy, with recommendations as to how these issues may be clarified and improved.

[40] Peter Costello, "Building social capital", speech to the Sydney Institute, 16 July 2003. The Treasurer suggested that "trust facilitates compliance (and) enhances efficiency".

[41] In 2002-03, 65 internal reviews were conducted by State and local government agencies, oversighted by Privacy NSW. A breach of the IPPs was only found in 18 cases (28%). In 12 cases the conduct complained of was found to have complied with the IPPs, and in a further 10 cases the conduct did not comply, but the non-compliance was authorised by a lawful exemption. Another 5 cases were finalised as 'no breach' on jurisdictional grounds, such as time limits. For further details see pp 27-30 of the Privacy NSW 2002-03 Annual Report.

Part 3 of this submission provides comprehensive analysis of each aspect of the PPIP Act, with recommendations for how the objectives of the Act could better be met, in way which balance the public interest in privacy protection with other public interests, such as the maintenance of law, ensuring public safety, and the efficiency of government services.

PART 2 THE ROLE OF A PRIVACY COMMISSIONER

This part of our submission reviews the role of a separate and independent Privacy Commissioner, and the role that their office plays in the wider context of information management laws and policies.

2.1 The role of Privacy NSW

2.1.1 Our role in government policy

The Privacy Commissioner's role, as set out in section 36 of the PPIP Act, includes the provision of advice and assistance to government agencies on adopting and complying with the IPPs, and on matters relating to the protection of personal information and the privacy of individuals generally.

In terms of new policy proposals (whether legislative or otherwise), sometimes our advice is requested early in the development of a new proposal, at other times during a Cabinet-confidential consultation phase, at other times during a public consultation phase, and sometimes not until a Bill is in Parliament. In many cases our advice is not sought at all, on matters which may have far-reaching privacy implications.

Resources permitting, we prefer to be involved up-front in the design of policy, so that privacy compliance (and indeed best practice) can be 'built-in' rather than 'bolted on'. It is our view that early consultation is beneficial for government, as proper policy and project design can minimise reputational risk and other costs to government. In providing policy advice, our aim is to assist government agencies in meeting their main objectives, while minimising or removing any negative impacts on privacy.

However we also understand that there is little clarity about the role of the Privacy Commissioner in providing advice to agencies, and whether, as an independent statutory position, he or she can or should be involved in Cabinet-confidential policy discussions. The PPIP Act would benefit from some clarity about the role of the Privacy Commissioner in the policy process. For example the Victorian Privacy Commissioner has a statutory function to advise the Attorney General on any legislative proposal that may interfere with, or have an adverse impact on, privacy[42].

We also have some concerns about consultation with the Privacy Commissioner (as opposed to seeking advice from the Privacy Commissioner) may be seen by some agencies as merely a 'tick box' exercise, rather than a genuine desire to take on board any suggestions we might make. We also hold some concerns about how the level of consultation with or involvement of this Office is described, for example in what circumstances agencies can claim they have the Privacy Commissioner's 'endorsement' of a project[43].

---

[42] See section 58(l) of the *Information Privacy Act* (Vic). For an analysis of the success (or otherwise) of this function see p 30 of their 2002-03 annual report.

[43] For example on 4 December 2003 the Minister for Education and Training, Dr Refshauge, described in the Legislative Assembly an MOU between various parties as having been "examined in detail and endorsed by the Privacy Commissioner". This was not a true reflection of Privacy NSW's involvement, which had only involved consideration of an earlier proposal, which was less broad in scope than the

In order to address these issues, we suggest that there is a need for a more formalised role for the Privacy Commissioner in providing comment on government policy proposals that may create a privacy impact. We also suggest that the mechanism of Privacy Impact Assessment would bring benefits to the development of policy, as well as preventing any misunderstandings about our views.

Under the PPIP Act, public sector agencies are required to prepare and publish Privacy Management Plans in relation to their compliance with the Act. However Privacy Management Plans do not embrace matters outside the regulatory scope of the PPIP Act, nor do they relate to specific projects, and there is no requirement to update their plans as new initiatives are being considered. Our success in getting agencies to measure privacy impacts before undertaking new practices or projects has mostly been limited to ensuring compliance with regulatory requirements.

By contrast, a Privacy Impact Assessment (PIA) is

> a process whereby a conscious and systematic effort is made to assess the privacy impacts of options that may be open in regard to a proposal. PIA is an assessment of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated[44]

A well-conducted PIA can provide assistance not only in terms of compliance with relevant privacy law, but also guidance for measuring the privacy impact of projects and practices which are not governed by information privacy laws. PIAs would also heighten the awareness and importance of privacy generally, and will bolster efforts to make privacy consideration part of the 'mainstream' legal and policy landscape.

Privacy Impact Assessment has been mentioned in the privacy literature from the 1980s, and implemented in jurisdictions from the early 1990s[45]. PIAs have often been promoted by Privacy Commissioners as a way of encouraging more self-reliance by agencies, in terms of building expertise in privacy assessment outside of just the Commissioner's office.

> *Privacy and data protection commissioners have a central role in respect of the protection of privacy. However, they invariably have small budgets and few staff. It is absurd to expect that Commissioners can assess all the various technological initiatives likely to impact upon citizens' privacy in the coming years. The responsibility must be shared[46].*

The objectives of a PIA may be to:

- assess risks arising from a new technology or the convergence of existing technologies (for instance, electronic road pricing, caller ID, smart cards);

---

final version. Indeed our consideration of the earlier proposal had been quite critical of numerous aspects of the proposal, and we had not heard any more about the proposal until it was mentioned in Parliament in final form as something we had 'endorsed'.

[44] Blair Stewart, "Privacy Impact Assessments", *Privacy Law & Policy Reporter*, July 1996, p 61.

[45] Blair Stewart, "What is Privacy Impact Assessment?", Abridged and revised version of a paper presented to the Privacy Law & Business 9th Data Protection Authorities' Workshop, "Biometric Identification: Challenging or enhancing privacy rights?", Santiago de Compostela, 15 September 1998.

[46] Blair Stewart, *Privacy Impact Assessment: Towards a better informed process for evaluating privacy issues arising from new technologies*, http://www.privacy.org.nz/search.html

- assess risks where a known privacy intrusive technology is to be used in new circumstances (for instance, expanding data matching or drug testing, installation of video surveillance cameras in further public places);
- assess risks in a major endeavour or change in practice having significant privacy effects (for instance, a proposal to merge major public registries into a "super registry", to adopt a national ID card, to relax controls on telephone tapping or to extend powers of search of premises or persons);

and to develop strategies for minimising those risks[47].

PIAs, if published, can also address reputational risk areas for government, and can assist other similar projects by providing a ready-made analysis of likely risk areas and possible solutions.

In the last few years PIAs have become compulsory for large federal government projects in the United States and Canada, and they have also been undertaken voluntarily by agencies in Hong Kong and New Zealand[48]. A recent example from New Zealand, published on the Privacy Commissioner's website, related to the State Services Commission's project on authentication for e-government purposes[49].

In 2002 the New Zealand Privacy Commissioner published a *Privacy Impact Assessment Handbook* which provides guidance to both public and private organisations about how to conduct PIAs. The Handbook is an exemplar of guidance and leadership in the area of best privacy practice.

We understand that both the Office of the Federal Privacy Commissioner and the Victorian Privacy Commissioner are currently working on their own PIA handbooks, as they each recognise the growing importance of PIA as a valuable assessment tool for governments when developing new legislative and technological projects and policies.

We believe that PIAs are the best means by which government agencies can aim for best privacy practice as well as legislative compliance. It is our submission that ideally, a PIA would be a statutory requirement for any new Bill, regulation, or project significant enough to require Cabinet consideration.

One possible model would be:

- Privacy NSW to help set terms of reference for a PIA, including what external guidelines / standards to use
- PIA to be conducted by an independent consultant, who reports to Privacy NSW as well as the client
- final PIA report to be published

Recommendation:

❖ That the role of the Privacy Commissioner in the policy process be clarified.

[47] Blair Stewart, "What is Privacy Impact Assessment?", as above.
[48] For a comprehensive bibliography of PIA literature and a brief history, see http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html#Refs
[49] See http://www.privacy.org.nz/media/mediatop.html

❖ That Cabinet consider requiring a Privacy Impact Assessment on any new legislative or policy proposals.

2.1.2 Our role in law setting

There are four sources of exemptions to the PPIP Act:

- exemptions written in the PPIP Act itself
- exemptions written in a regulation made by the Attorney General under the PPIP Act
- exemptions written in a privacy code of practice, made by the Attorney General under the PPIP Act
- exemptions written in a public interest direction, made by the Privacy Commissioner under the PPIP Act

This plethora of exemption mechanisms has made the PPIP Act confusing for all those attempting to interpret and apply the law. (For a further discussion of this point, and discussion of the substance of the Act-based exemptions, see part 3.1.2 of this submission.)

Furthermore there are differences between each of the three subordinate mechanisms by which exemptions may be granted:

- Codes and regulations may create exemptions from the public register provisions, but public interest directions cannot.
- Codes and regulations may apply to a class of public sector agencies, but public interest directions cannot[50].
- Codes are made by the Attorney General but require consultation with the Privacy Commissioner; public interest directions are made by the Privacy Commissioner but only with the approval of the Attorney General; and the Privacy Commissioner has no formal role in regulations at all.
- Directions require a 'public interest' test to be satisfied, but codes and regulations do not.

There is also a lack of clarity in the Act about whether or not the Attorney Generals' approval is required to extend the time period of a public interest direction, if no other change is made. As a matter of both courtesy and caution, we have sought the Attorney's approval for each extension of a direction – a process that has caused more paperwork than is perhaps warranted.

Part of the difficulty experienced with the implementation of the PPIP Act has been the absence, within the Act itself, of exemptions or guidance in relation to common activities across the public sector, namely research and internal investigations (such as disciplinary investigations of staff). These difficulties were identified early in the piece by Privacy NSW, and work began in 1999-2000 on privacy codes to cover these activities. Due to the complexity of the proposed exemptions, and the need to consult widely, these codes were

[50] This means that each agency to be covered by a public interest direction must be named in the direction. As the existence of both State and local government agencies can be a somewhat moveable feast, this creates problems for Privacy NSW when drafting the exemptions. Sometimes agencies will miss out on an exemption if we do not know they exist, or of their new name.

not made in time for the Act's commencement. In preparation for the full commencement of the Act on 1 July 2000, then Commissioner Puplick made what were supposed to be temporary public interest directions. Those directions have been extended repeatedly for over four years, as no resolution was found on the draft codes.

Yet these same issues appear to have been resolved in relation to the Health Records & Information Privacy Act 2002 (HRIP Act) without difficulty. The HRIP Act has incorporated comprehensive exemptions in relation to both research and investigation activities, and in relation to the former has also incorporated statutory guidelines to be made by the Privacy Commissioner, to provide the more detailed guidance around subjective matters not well suited to prescriptive legislation.

We therefore submit that the PPIP Act should incorporate permanent Act-based exemptions for common and permanent sector-wide activities such as research and investigations (and that such exemptions should mirror the HRIP Act).

Recommendation:

- That the PPIP Act be amended to incorporate the research and investigations exemptions now in the HRIP Act.

One of the difficulties with respect to privacy codes of practice is that the Act states that codes are "for the purpose of protecting the privacy of individuals"[51] – yet they actually diminish the level of privacy protection previously granted by Parliament. The very name 'code' also causes difficulties, as the name suggests a 'codification' of the law, rather than an exemption from the law[52]. In cases where the law leaves grey areas that require further guidance, we submit that guidelines are a preferable solution. We therefore suggest deleting all code-making powers.

We also have concerns about the absence of a transparent process involved in each of the three exemption-granting mechanisms, although at least regulations are disallowable. Nonetheless, given the absence of any public interest test or consultation requirement for the making of regulations, this is the least satisfactory of the three options.

Recommendation:

- That all code-making provisions of the PPIP Act (sections 29 to 33) be deleted.
- That section 71 to amended to proscribe the granting of exemptions to the IPPs or the public register provisions by way of regulation.

[51] See section 29(1) of the PPIP Act.

[52] This view – that draft codes proposed by the Privacy Commissioner would make agencies' obligations more difficult rather than easier – seemed to permeate debates about the draft codes on research and investigations, regardless of how often Privacy NSW attempted to explain that without the codes, the activities in question could not occur at all. It would seem this common misunderstanding about the function of codes stems primarily from their name.

- ❖ Alternatively, that section 71 to amended to require consultation with the Privacy Commissioner before a regulation may be made, and that the Privacy Commissioner's comments in relation to the proposal form part f the Regulatory Impact Statement for that regulation.

Furthermore the existence of the power to provide 'instant' exemptions places the Privacy Commissioner under considerable pressure from agencies, and may cause a conflict of interest situation. Privacy NSW has often been approached by agencies seeking 'urgent' and 'last minute' exemptions, in situations where it is difficult to clearly and calmly assess how the public interest would best be served.

By contrast the Victorian Privacy Commissioner has no power to issue exemptions, and the Federal Privacy Commissioner can only make public interest determinations after a lengthy consultation and hearing process.

Given the breadth of the existing exemption under section 25 of the PPIP Act, we suggest that it would be preferable, in terms of transparency and accountability, for agencies to seek their own legislative authority for any conduct that would otherwise breach the IPPs or public register provisions of the PPIP Act.

Nonetheless we recognise that temporary directions do allow flexibility, and can incorporate a balancing 'public interest' test. However the aim of a temporary direction should only be to allow an agency time to achieve compliance, such as a change in their practices, or to seek specific legislative authority through their own legislation.

We therefore recommend retaining the power for the Privacy Commissioner to issues public interest directions, but in the following model:

- Directions must be one-off, non-renewable, with a 12 months maximum time limit before expiry
- Continued public interest test
- Continue the role of the Attorney General in approving the Privacy Commissioner's recommendation
- Specify that a *class* of agencies may be covered by the terms of the direction
- Allow public register provisions to be modified
- Require public sector agencies to incorporate in their Privacy Management Plans any public interest directions upon which they intend to rely

We also recognise that there should be greater flexibility in how the core privacy standards in the Act can be achieved. We recommend later, at part 3.1.1 of this submission, that the Privacy Commissioner be able to make statutory guidelines, with the approval of the Attorney General, which can allow modifications to the *mechanisms* by which privacy principles are to be achieved, but cannot modify the core *principles* themselves.

We further suggest that any existing codes should be reviewed following any amendments to the PPIP Act consequent on this review[53].

Recommendation:

- That section 41 be amended to set a non-renewable 12 months time limit, allow a class of agencies to be covered by the terms of a direction, and allow the public register provisions to be modified by the terms of a direction.
- That section 33 be amended to require agencies to incorporate in their Privacy Management Plan any public interest directions upon which they intend to rely.
- That the Act be amended to nullify all existing codes within 12 months of the amendment.

2.2 The wider framework of information management laws

2.2.1 Privacy and records management

We have identified only two areas where privacy and records management have appeared to come into any sort of conflict, and each of these has been resolved to our satisfaction.

While there was some initial lack of clarity as to how section 15 of the PPIP Act (IPP 8, in relation to amendment of personal information) interacted with agencies' record-keeping obligations under the State Records Act, this difficulty will shortly be resolved by way of a minor amendment to section 15 in the PPIP Act, which will come into effect when the HRIP Act commences on 1 September 2004[54].

Section 12(1) of the State Records Act requires agencies to 'keep full and accurate records of the activities of the office', and we advise agencies in the event of possible conflict to refer to the State Record Authority's *Standard on Full and Accurate Records*. We thus believe that the requirements of the Standard do not conflict with the requirement under section 11 of the PPIP Act (IPP 4) to take reasonable steps to avoid collecting information that is inaccurate, irrelevant, out of date, or misleading.

2.2.2 Privacy and FOI

Late in 2003, the Government introduced legislation to move the functions of the NSW Privacy Commissioner to the NSW Ombudsman[55]. However to date that Bill has not progressed in the Legislative Council.

[53] For example if our other recommendations with respect to the public register provisions are implemented, the Local Government Code should be reviewed as to whether it is still necessary.
[54] The amendment moves from s.20(4) to IPP 8 itself (s.15(4)) a provision which states that IPP 8 clearly overrides section 21 of the State Records Act, despite section 25 of the PPIP Act which otherwise would allow the State Records Act to override IPP 8.
[55] See the Privacy and Personal Information Protection Amendment Bill 2003.

For FOI and privacy to be regulated by the one body makes intuitive sense. They are two sides of the one coin of ensuring government agencies handle information in an accountable manner.

Reasons in favour of more closely aligning the responsibilities for FOI and privacy law include:

- the overwhelming majority of FOI requests are for access to the applicant's own personal information[56]
- one Information Commissioner is the trend in many common law jurisdictions, especially where FOI didn't already pre-date privacy legislation[57]
- the proposal that the Privacy Commissioner could take on the FOI role was initially promoted in the 1995 Australian Law Reform Commission (ALRC)'s review of FOI[58]
- the proposal was seen as 'attractive in so far as it would require a single individual to resolve any tensions between FOI and privacy'[59]
- the two reasons that the Australian Law Reform Commission found not to proceed at that stage[60] are not insurmountable
- the NSW Auditor-General[61] recently found that a comprehensive oversight, review and policy-development mechanism (beyond the complaints-handling role of the Ombudsman) is required for better management of FOI in practice[62]

However it is our submission that the one office to manage both FOI and privacy, if such an approach is taken, should be that of an independent Information Commissioner, rather than an Ombudsman.

An Ombudsman taking on the role of FOI Commissioner was specifically rejected by the ALRC, and the reasons for that view apply even more so to the notion of an Ombudsman taking on the role of Privacy Commissioner:

> the Ombudsman's role makes it important that he or she not become involved in policy development. The Ombudsman should be independent of the policy-making process and able to criticise defective policy. … The Ombudsman … requires arms length

[56] See Committee on the Office of the Ombudsman and Police Integrity Commission (Joint Statutory Committee), *First Report on the Inquiry into Access to Information*, 1 December 2002, page 13; see also ALRC Report #77, *Open Government: A Review of the Federal Freedom of Information Act 1982*, 1995, part 6.29

[57] In Australia: Northern Territory, and a Bill currently being developed in WA; overseas: UK, Canadian provinces of Alberta, British Columbia, Nova Scotia, Ontario, Prince Edward Island, Saskatchewan and Quebec.

[58] See ALRC Report #77, part 6.29

[59] See ALRC Report #77, part 6.29

[60] Privacy legislation was about to extend to the private sector; and FOI might be seen as the 'poor cousin' to privacy

[61] NSW Audit Office, *Auditor-General's Report : performance audit : freedom of information (non-personal requests)*, August 2003, page 48.

[62] The NSW Auditor-General recommended introducing a new review mechanism to routinely oversee FOI arrangements by way of collating data on all FOI decisions, auditing administrative arrangements in agencies, and disseminating information on developments in both law and policy (see p.48).

> scrutiny which would be compromised significantly if the Ombudsman had responsibility for administering particular legislation other than his or her own[63].

Further reasons for this view include:

- separation of the three roles (FOI / Privacy / Ombudsman) was a recommendation of the ALRC's review of FOI, although it argued for close co-operation between FOI and Privacy Commissioners
- better accountability can be secured through having two organisations, as each can be a check and balance on the other
- other jurisdictions which have an Information Commissioner (who does FOI alone or FOI and privacy) still have a separate Ombudsman to deal with more general misconduct and maladministration in government[64]
- in those jurisdictions where an Ombudsman regulates / manages FOI, the role is primarily limited to complaints-handling rather than wide policy-setting, advice or education roles[65]
- unlike FOI, 'privacy' does not fit neatly within a pure administrative decision-making and review model
- Privacy Commissioners' offices are generally not just complaints-handling bodies; for example at Privacy NSW we have a large and growing advice role, and we see ourselves as a resource to agencies, not just a 'watchdog'
- the privacy advice role is extremely specialist yet can incorporate a huge breadth of material; new technologies mean constant new challenges for information handling and privacy implications
- a recent survey of Privacy Contact Officers across every public sector agency in NSW shows high levels of demand for increased education / publication activities from Privacy NSW to assist agencies understand and implement their obligations

2.2.3 Conclusion

It is suggested that this review of the PPIP Act should examine options for more closely aligning the various information management strands of privacy, FOI and records management. Education, advice and assistance are of paramount importance for organisations trying to understand and implement their obligations under the various Acts.

One possibility, which Privacy NSW would like to explore further, is the use of assisted decision-making in terms of compliance with the various inter-acting information management laws affecting public sector agencies – the PPIP Act, HRIP Act, State Records Act and FOI Act.

---

[63] See ALRC Report #77, part 6.29

[64] See for example Queensland and the Northern Territory within Australia, and the Canadian Federal and provincial (BC, Ontario and Quebec) governments, and the UK.

[65] See for example NSW, Victoria, Queensland and New Zealand. The NSW model has some deficiencies (see Auditor-General's Report mentioned above), while in New Zealand the FOI regime specifically excludes the first party access / amendments provisions, leaving them to privacy legislation. For further reasons why an Ombudsman is not the best body to manage FOI see the ALRC Report, mentioned above. For further information on different regimes see the NSW Parliamentary Committee Report, mentioned above.

SoftLaw provides an electronic decision-making tool, based on legislative rules, mostly in plain English 'question and answer' format, in order to progress the user down a decision-making 'tree' or 'flowchart' to reach the right answer. It has an audit trail and the user can print out the 'path' taken to reach their answer, and see each legislative rule in detail if needed. Although mostly found in Commonwealth agencies to date, this model has recently been implemented by the NSW Premier's Department in the *HRExpert* database, accessible from the Premier's Department website.

This does not suggest that all decisions are made by a computer. The system guides decision-making, and may only be able to lead the decision-maker to a point where a subjective decision must still be made on a case-by-case basis. However it should at least ensure that decisions are transparent, supportable, and based on the correct criteria.

The benefits of such a system could include:

- for all agencies: guided decision-making for public servants should result in more consistent and accurate decisions; saved time in making initial decisions; and saved in-house and external litigation time and cost in reviewing any disputed decisions
- for the 'regulatory' agencies: more effective training tool, possible saved costs in repetitive education / training initiatives
- for the government: consistent, accurate and transparent decision-making by public servants should result in fewer matters proceeding to the Administrative Decisions Tribunal
- for better policy development: the model can be used to test for legislative gaps and overlaps of proposed Bills and so on
- for the public: a self-service model could result in immediate and transparent responses, plus fewer enquiries or complaints to agencies

Recommendation:

❖ That consideration be given to funding a project to produce an electronic assisted decision-making tool, covering all the information management laws

PART 3 SUGGESTIONS FOR AMENDMENTS TO THE ACT

3.1 The privacy standards in the Act

This part of our submission reviews what might be considered the crux of the PPIP Act – the privacy standards set for state and local government under the Act. By 'privacy standards' we mean:

- the information protection principles in Part 2 of the Act, and
- the public register provisions in Part 6 of the Act.

This submission examines:

- whether the privacy standards are clear in their intent and effect
- whether the privacy standards require revision
- whether the application of the privacy standards (to types of information, activities, or organisations) is clear
- whether the exemptions to the privacy standards require revision

3.1.1 The information protection principles

The 12 information protection principles (IPPs) form the backbone of the PPIP Act[66]. They govern the way in which personal information must be collected, stored, used and disclosed by public sector agencies, as well as providing for rights and access and amendment of a person's own personal information.

The IPPs are based on long-standing and accepted international principles first espoused by the OECD in 1980[67], which have been reflected in privacy laws around the world. Local examples include not only the PPIP Act but the Federal *Privacy Act 1988*, which has regulated Australian Government agencies for many years, the Victorian *Information Privacy Act* 2000 and the Northern Territory *Information Act*. The new *Health Records & Information Privacy Act 2002* in NSW also reflects the same basic set of principles.

The core concepts in the OECD Guidelines, which are reflected in the IPPs, can be summarised as:

- collection limitation
- data quality
- purpose specification
- use and disclosure limitation
- security safeguards
- openness
- individual participation

It is our submission that these core concepts are sound, and do not require revisiting. However their interpretation into NSW law is worthy of review.

---

[66] The 12 IPPs are set out in sections 8-19 of the PPIP Act. Plain English explanations for members of the public and for public sector agencies have been published by Privacy NSW as Fact Sheet #1 and #2 respectively.

[67] See http://www.oecd.org/document/18/0,2340,en_2649_37409_1815186_1_1_1_37409,00.html

Flexibility of the IPPs

The PPIP Act is an instance of principle based legislation being applied in a legal system which is more familiar with applying legal rules[68]. Principle based legislation requires an approach to interpretation which treats the principles as a reference point and guide to seeking particular outcomes but recognises that they can not be imposed absolutely and that their application may need to take into account other principles. The application of legal rules requires a much closer fit between conduct and the rules governing it.

Yet the drafting of the PPIP Act does not consistently reflect the principle based approach inspiring the legislation. The difficulties this creates for interpretation extend to the arrangement and substantive provisions of the Act itself, as many of the exemptions which are necessary to the practical operation of the Act are expressed in a rule based form. Defining the scope of the information protection principles is also affected by the enforcement process under the Act, which unlike similar legislation in other jurisdictions, gives the Tribunal a primary enforcement function and accords a more limited role for the statutory privacy authority.

The drafting of a mandatory 'principle' is thus a difficult task. In effect, the IPPs contain a mix of both:

- core privacy principles, and
- the prescriptive mechanisms by which each principle is to be obtained.

For example, the core privacy principle of 'collection limitation' is described in the OECD Guidelines as:

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

In practice, under the NSW law, this core privacy principle is to be achieved by complying with IPPs 1-4. Taking just one of the IPPs as an example, IPP 2 states:

IPP 2: Section 9. Collection of personal information directly from individual

A public sector agency must, in collecting personal information, collect the information directly from the individual to whom the information relates unless:

(a) the individual has authorised collection of the information from someone else, or

(b) in the case of information relating to a person who is under the age of 16 years--- the information has been provided by a parent or guardian of the person.

That is, IPP 2 allows certain things (the collection of information about a person aged under 16 from their parent or guardian) and prohibits others (the collection of information about a person aged under 16 from other sources without their authorisation; the collection of information about a person aged 16 or older from any other source without their authorisation).

---

[68] For the distinction between principles and rules see generally G Dworkin, *Taking Rights Seriously*, Harvard University Press, Cambridge Mass 1977, Chapter 2 "The Model of Rules 1". See also E Riedel, "Standards and Sources. Farewell to the Exclusivity of the Sources Triad in International Law?" *European Journal of International Law* (1991) Vol 2(2) : 58 at pp 74,78, downloaded from http://www.ejil.org/journal/Vol2/No2/art3.html

In this sense, the 'collection limitation' *principle* is to be achieved by following a very specific *mechanism* for collection of personal information, which allows certain things and prohibits others.

It is our submission that while the core privacy principles are sound, the *mechanisms* by which those principles are expected to be achieved can sometimes be too rigid.

Privacy is a right that affects how individuals interact with organisations, and in that sense is about regulating relationships. This is a complex task to achieve - covering the full spectrum of citizen to government interactions in 12 sections.

Information privacy laws are not one-way or passive laws; they assume some level of responsibility on the citizen to participate in the protection of their privacy. They create a citizen-focussed framework, in which the citizen is expected to give or refuse consent to how their personal information will be collected, used or disclosed. The law therefore assumes that all people are equally capable of exercising their privacy rights within this framework.

Yet the law is a blunt instrument, and often cannot take account of the realities of people's lives. IPP 2 for example does not explain:

- how to obtain 'authorisation' from a person aged 16 or older to collect information from someone else, if that person has limited or no capacity to provide or refuse an authorisation
- whether or in what circumstances people aged under 16 should be dealt with directly instead of through their parent or guardian
- how to obtain 'authorisation' from a person aged under 16 to collect information from someone other than their parent or guardian

The first issue identified above - that of adults with limited or no capacity to make decisions regarding their personal information – has therefore proven particularly challenging for public sector agencies in understanding and applying their obligations under the PPIP Act.

To note that there has been difficulty in complying with the letter of law in terms of the *mechanisms* is not to suggest that the core *principles* themselves are unsound. Privacy NSW has therefore been particularly concerned to ensure that the solution to these challenges is not the creation of wholesale exemptions from the principles themselves. We would prefer to see solutions that ensure the core privacy standards are achieved, not diminished.

For example we have recently published a best practice guide: *Privacy and people with decision-making disabilities*, which attempts to provide more flexible mechanisms in which to achieve the core privacy principle at issue[69]. The guide was prepared to assist NSW public sector agencies to apply the IPPs in a manner that protects and promotes, to the greatest extent possible, the privacy of adults with a decision-making disability.

As the guide itself states:

> The PPIP Act is silent about what happens when a person cannot understand or make decisions about how their personal information is handled. This guide recommends a best-practice approach, based on principles or 'signposts' that agencies can use to inform their policies and procedures when handling personal information about people with decision-making disabilities.

[69] See http://www.lawlink.nsw.gov.au/pc.nsf/pages/bpg_disability

> This guide is not legally binding. It does not override the IPPs in the PPIP Act or diminish the entitlements of people with a decision-making disability under the Act. It just provides a best practice guide for handling personal information about individuals with a decision-making disability.

Privacy NSW would support amendments to the PPIP Act to enable this type of solution to have equal footing with the IPPs themselves.

This type of flexibility is already a feature of other privacy law in NSW, namely under the Health Records & Information Privacy Act 2002, which allows the Privacy Commissioner to make statutory guidelines which then form part of the enforceable privacy principles[70].

In pursuing this approach, IPPs 6-8 should be seen as protecting the overall interest of individuals in the protection of their privacy by giving them the opportunity to find out what information is held about them, assisting them to take action to correct this information if it is inaccurate, irrelevant, out-of-date, incomplete, or misleading, and seeking redress under the other IPPs if the presence or the context of the information indicates a likely breach. For example discovering that an agency holds specific information about an individual may point to illegal or unauthorised collection, unjustified retention, or unauthorised disclosure by another agency.

Recommendation:

- That the IPPs more clearly distinguish between the core *principle*, and the *mechanism* by which the principle is expected to be achieved.
- That the Privacy Commissioner be able to make statutory guidelines, with the approval of the Attorney General, which can allow modifications to the *mechanisms* by which privacy principles are to be achieved, but cannot modify the core *principles* themselves.

Structure of the IPPs within the Act

The IPPs are found in sections 8-19 of the PPIP Act.

Exemptions to the IPPs are scattered across the Act in:
- sub-sections of the IPPs themselves,
- definition sections (eg. section 4),
- sections that set out the application of the IPPs or the Act generally (eg. section 6, and section 20), and
- specifically labelled exemption provisions (eg. sections 23-28).

This structure has proven confusing for public sector agencies to understand and apply, and for complainants to understand and assert. Even in a simple tabulated format, the list alone (not the actual text) of current exemptions takes up four A3 pages[71].

[70] The guidelines made under the HRIP Act are about the mechanisms rather than the core principles themselves – for example, the mechanisms to be used to assess whether or not health information can be disclosed for research purposes. See HPPs 3, 4, 10 and 11.

The IPPs are already a mix of the prescriptive or proscriptive[72] core principle and the permissive 'exemption'. For example section 18 (IPP 11) creates a general prohibition on disclosure, but then provides exemptions to the general statement for circumstances outlined in sub-sections to section 18.

To alter the structure of the PPIP Act to bring all Act-based exemptions directly under the general rule would be consistent with the Federal *Privacy Act* and the NSW HRIP Act, and would make the IPPs easier to find, read, and therefore understand and apply.

Recommendation:

- That the IPPs should be amended to bring all Act-based exemptions directly under the general rule.

Detailed examination of the IPPs

This part of our submission highlights those IPPs which may not be clear in their intent and/or effect, and in some cases suggests revision. This part does not address existing exemptions to the IPPs found outside the IPPs themselves; for a discussion of Act-based exemptions see part 3.1.2 of this submission, and for a discussion of other types of exemptions see part 2.1.2 of this submission.

IPP 1 (section 8)

IPP 1 provides that personal information can only be collected for a lawful purpose, and only if it is directly related to the agency's activities and necessary for that purpose.

It is submitted that collection of particularly sensitive personal information ought be more strictly regulated. The disclosure of particularly sensitive personal information is already regulated under IPP 12 (see below). However other Australian privacy laws[73] recognise that the best means of preventing misuse of personal information is to restrict its collection in the first place, to that which is absolutely necessary.

[71] See the exemptions matrix at http://www.lawlink.nsw.gov.au/pc.nsf/files/privacyessentials_04.pdf/$FILE/privacyessentials_04.pdf

[72] The core privacy principles in the IPPs are a mix of the prescriptive and proscriptive. For example IPP 5 creates obligations on agencies to take positive steps, while IPP 11 prohibits certain conduct.

[73] See NPP 10 in the Federal Privacy Act 1988, IPP 10 in the Victorian Information Privacy Act 2000; and IPP 10 in the Northern Territory Information Act.

Recommendation:

- That IPP 1 be amended to include a specific limitation on the collection of sensitive classes of personal information.

IPP 2 (section 9)

IPP 2 is particularly restrictive, in that it prohibits any indirect collection of personal information (that is, collection other than from the individual themselves), except with the person's authorisation.

There is an accepted practice of collecting social and medical histories from clients, in order to provide appropriate services to that client. For example, a client who presents to a hospital complaining of chest pains may be asked by the treating doctor whether their parents or siblings have a history of heart disease. However for the doctor to collect such information about the client's parents or siblings, without their prior authorisation, would be contrary to IPP 2. The parents or siblings could make a complaint that their privacy had been breached.

Privacy NSW has recognised this particular inflexibility of IPP 2 in the context of the provision of human services, and in December 2003 the NSW Privacy Commissioner issued a temporary public interest direction to exempt certain agencies as a result[74].

We would support an amendment to allow a more permissive approach, so as to allow indirect collection about a person, where reasonably necessary in order to provide a service to a client (where the client is not the person whose personal information is being collected without their knowledge).

Such an amendment should however be limited to circumstances in which the collection of the person's personal information is solely for the purpose of, and reasonably relevant and reasonably necessary for, the provision of services, diagnosis, treatment or care to the client. Subsequent use and disclosure of the person's personal information by the agency should therefore be extremely limited[75].

[74] For a copy of the public interest direction see http://www.lawlink.nsw.gov.au/pc.nsf/pages/s41bsd . The Federal Privacy Act posed similar difficulties, and the Federal Privacy Commissioner issued a public interest determination under that Act to cover similar circumstances; see http://www.privacy.gov.au/act/publicinterest/index.html .

[75] For example the information could not be used in order to provide services to the person themselves, if they are also a client of the agency. Existing exemptions, such as mandatory notification of suspected child abuse, would not be affected.

Recommendation:

- That IPP 2 include an exemption in relation to the collection of personal information from an individual who is a client of the public sector agency (the client), of personal information about another individual (the person), where the collection of the person's personal information is reasonably relevant and reasonably necessary for the purpose of the agency providing services, diagnosis, treatment or care to the client.

IPP 3 (section 10)

IPP 3 requires agencies to provide people with a 'privacy notice' when collecting their personal information. It states:

> If a public sector agency collects personal information ***from an individual***, the agency must take such steps as are reasonable in the circumstances to ensure that, before the information is collected or as soon as practicable after collection, ***the individual to whom the information relates*** is made aware of … . (Emphasis added.)

For example, Government Department A collects information about Jane Citizen from Jane herself, by Jane filling out a form. Under IPP 3, Government Department A must clearly give the notification to Jane.

However the wording of IPP 3 is open to argument[76] as to the requirement on an agency to provide notice to the subject person when collecting their personal information from an indirect source, whether from another individual person or organisation (in which case IPP 2 is an issue), or by passive means. That is, the means of collection can differ, but IPP 3 does not provide clarity or flexibility to meet the different means of collection.

For example:

- what if Government Department A collects personal information about Jane from Joe Bloggs?
- what if Government Department A collects personal information about Jane from Government Department B?
- what if Government Department A collects personal information about Jane by taking her photograph without her knowledge?
- what if Government Department A collects personal information about Jane from the *White Pages*?

In fact the requirement set out further in the detail of IPP 3 itself contemplates that collection could be from another agency, despite the apparent precondition at the beginning of the provision, relating to collection *from an individual* – see section 10(f):

[76] See a case decided whilst we were in the middle of writing this submission: *HW v Director of Public Prosecutions (No 2)* [2004] NSWADT 73, which found that IPP 3 and IPP 4 did not apply to indirect collection. The ADT found that the phrase "from an individual" meant "from the individual to whom the information relates". A preliminary reading of the effect of this decision is that agencies that collect personal information by indirect means (such as via another agency, via another individual, or via passive means such as a camera) need not comply with IPPs 3 or 4.

(f) the name and address of the agency ***that is collecting*** the information and the agency ***that is to hold*** the information.

An amendment to clarify the extent of the notification obligation, to cover each possible means of collection, would be in line with other NSW privacy law[77]. It would ensure that the protection of the privacy principles in relation to notification and non-intrusiveness apply equally to those most at risk (those who are not directly providing the information about themselves) as to those least at risk (those providing the information themselves and can therefore exercise direct control over what is revealed)[78].

This is a separate issue to appropriate exemptions to the notification requirement, which include existing exemptions in relation to law enforcement and so on. In any case, the mechanism of IPP 3 only expects 'reasonable steps' to be taken to meet the core principle.

We suggest that as a matter of best privacy practice, the core principle is that Government Department A should be taking reasonable steps to ensure that Jane Citizen *receives* the appropriate notice. (What constitutes 'reasonable steps' in different circumstances is a different issue; see more below).

Recommendation:

- That IPP 3 be amended to clarify that the core principle is that the collecting agency should be taking reasonable steps to ensure that the *subject* of the personal information receives the appropriate notice, regardless of whether the agency is collecting their personal information direct from the subject, or from any other source or any other means.

What constitutes 'reasonable steps' in different circumstances has also been a difficult issue for both public sector agencies and members of the public to understand and apply.

We are often asked to advise on what might constitute 'reasonable steps' in the context of:

- different audiences with different capacities (for example, children, people of NESB, people with decision-making disabilities),
- different technologies for the collection (for example, by paper form, via online survey, by CCTV camera),
- different means of collection (for example, from the person direct, from another person, from a publicly available publication), and
- different purposes of collection of the information (for example, if it is for dealing with the subject person, or for dealing with another person).

[77] The Health Privacy Principles in the HRIP Act require a privacy notice to be given to the person who is the subject of the information, whether their information is collected directly from the person or from another source; see HPP 4(2).

[78] The recent decision of *HW v Director of Public Prosecutions (No 2)* [2004] NSWADT 73 has exposed the weakness caused by unclear drafting in IPPs 3 and 4.

However the PPIP Act cannot, in one section, attempt to address all these issues. This is a topic that could be the subject of more detailed statutory guidelines issued by the Privacy Commissioner[79].

Privacy NSW has already for example provided practical guidance to agencies on how to comply with IPP 3 in relation to people decision-making disabilities[80]. We have also recently published the Community Language Privacy Notice[81], which is a set of 23 downloadable texts, which provide a generic privacy notice, translated into 23 community languages, for incorporation into agencies' printed or online publications, forms, and so on.

IPP 4 (section 11)

IPP 4 requires agencies to take reasonable steps to ensure that information collection is relevant, not excessive, accurate, up-to-date and complete, and that the collection does not intrude unreasonably into a person's personal affairs. It states:

> If a public sector agency collects personal information ***from an individual***, the agency must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:
>
> > (a) the information collected is relevant to that purpose, is not excessive, and is accurate, up to date and complete, and
> >
> > (b) the collection of the information does not intrude to an unreasonable extent on the personal affairs of ***the individual to whom the information relates***. (Emphasis added.)

Like IPP 3, the wording of IPP 4 is ambiguous as to the requirement on an agency to ensure relevance, accuracy, etc when collecting personal information about a person from an indirect source, whether from another individual person or organisation, or by passive means (such as a video camera). That is, the means of collection can differ, but IPP 4 does not provide clarity or flexibility to meet the different means of collection[82].

---

[79] See above at part 3.1.1 as to the suggestion for the need for statutory guidelines to allow greater flexibility in the mechanism of the IPPs. In relation to the means of collection, such guidelines might include for example:

- where the information is collected from a publicly available publication : no notice required
- where the information is collected from a person acting in an agency relationship (eg. parent / child) : steps should be taken to provide notice to the person from whom the information is collected
- where the information is collected not from the subject person but from a different person (the client), for the purpose of providing services to the client (see the proposal above in relation to IPP 2) : no notice required
- where the information is collected from another public sector agency on a routine basis : the first collecting agency to provide the notice
- where the information is collected from another public sector agency on an ad-hoc basis : the last collecting agency to ensure that at least one of the two agencies has notified the person direct about both agencies' collections.

[80] See the 'Best Practice Guide' : *Privacy and people with decision-making disabilities* at http://www.lawlink.nsw.gov.au/pc.nsf/pages/bpg_disability

[81] See the 'Privacy Essentials' series : *Community language privacy notice* at http://infolink/pc.nsf/files/privacyessentials_01.pdf/$FILE/privacyessentials_01.pdf .

[82] See above in the discussion of IPP 3 for the impact of a recent decision (*HW v Director of Public Prosecutions (No 2)* [2004] NSWADT 73) on the interpretation given to the wording of IPP 4, which demonstrates the need for an amendment as a matter of priority.

The means of collection could be particularly relevant to the extent to which the conduct is judged against requirement (b). That is, indirect collection by its very nature can be intrusive into a person's personal affairs, since the subject individual does not control how much information is provided.

Recommendation:

- That IPP 4 be amended to clarify that the core principle applies to the *subject* of the personal information, regardless of whether the agency is collecting their personal information direct from the subject, or from any other source or any other means. For example, the amendment could be:

  If a public sector agency collects personal information **about** an individual, the agency must take such steps as are reasonable …

IPP 5 (section 12)

IPP 5 creates a positive obligation on agencies to take steps to minimise the risk of other privacy principles being breached, most notably inappropriate or unauthorised use or disclosure[83].

It is a reasonably flexible provision, and adopts a technology-neutral approach. While a more prescriptive approach might initially appeal in terms of clarity, it would too easily become out-of-date as technology changes. We therefore support the current flexibility of IPP 5.

In particular, section 12(b) is intended to achieve complementarity with record-keeping obligations on agencies under the State Records Act[84], and 12(c) is flexible enough to incorporate industry and government standards on security of information.

However neither IPP 5 nor the previous IPPs 1-4 adequately deals with an obligation to ensure secure *collection*. This especially important as agencies increasingly collect information through websites and emails.

Recommendation:

- That IPP 5 be amended to include an obligation to ensure secure *collection* of personal information.

[83] For cases applying these requirements to different fact situations, see *FH v Commissioner, New South Wales Department of Corrective Services* [2003] NSWADT 72, and *HW v Commissioner of Police, NSW Police and Anor* [2003] NSWADT 214.
[84] See for example a discussion of this issue in *GR v Department of Housing* [2003] NSWADT 268, paras 28-42.

A further issue is raised when government activities are contracted out. The situation under the PPIP Act when personal information is held by contractors to government agencies is complex, and there is other discussion on this topic elsewhere in this submission[85]. IPP 5 acknowledges the risks inherent when personal information is held by a contractor to an agency, rather than the agency themselves, and under section 12(d) obligates the agency as follows:

> (d) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information.

Privacy NSW has advised agencies that in order to meet the terms of IPP 5, as well as sensible risk management, they should include compliance with the IPPs as part of their contracting terms, with penalty clauses and/or indemnity for the agency if the contractor causes a breach. However greater clarity could be achieved if the requirement to bind contractors to meet the IPPs were mandatory under IPP 5, as is the case under the Federal Privacy Act[86].

Two caveats to this proposal are:

- if the current indirect system of coverage for contractors remains[87], the terminology to be used in IPP 5 should reflect this, and
- the privacy standards to be met ought be the IPPs as they apply to the agency, that as, the IPPs as modified by any exemption that applies to that agency (for example under a Privacy Code of Practice).

Recommendation:

❖ That IPP 5 be amended to include an obligation to bind contractors, by way of contract with appropriate penalty clauses, to the same privacy standards that apply to the agency.

IPP 6 (section 13)

This provision is to do with a systemic obligation owed by agencies generally to the community[88], to ensure a high degree of transparency about information handling practices, and may apply even where an agency is exempt from the obligation in IPP 3 to notify an individual at the time of collection that their personal information is being collected by that agency. We do not suggest any revision is required of IPP 6.

However we do question the need for the exemption from IPP 6 as set out in section 20(5). See the further discussion at 3.1.2 below on this issue.

---

[85] See the discussion of section 4(4) of the Act, in part 3.1.2 of this submission.
[86] Section 95B(1) of the Federal *Privacy Act 1988* states: This section requires an agency entering into a Commonwealth contract to take contractual measures to ensure that a contracted service provider for the contract does not do an act, or engage in a practice, that would breach an Information Privacy Principle if done or engaged in by the agency.
[87] See discussion of s.4(4) at part 3.1.2 of this submission.
[88] See *HW v Commissioner of Police, NSW Police and Anor* [2003] NSWADT 214, para 55-56.

IPP 7 (section 14)

IPP 7 creates a right of access to one's own personal information. It can be seen as a less formal alternative to FOI, desirable because access to one's own personal information will generally require less consideration of other interests than a request to access someone else's personal information or government policy documents.

However in practice the effect of section 20(5) makes IPP 7 less useful than it could be, owing to a lack of clarity about the breadth of its application. See the further discussion at 3.1.2 below on this issue.

There are further difficulties in the practical application of IPP 7 (and the right of correction under IPP 8) to information 'held' by agencies, but not recorded in a material form.

Recommendation:

- That IPP 7 and IPP 8 be amended to ensure their flexible application in relation to personal information held by agencies but not recorded in a material form.

IPP 8 (section 15)

IPP 8 creates a right of amendment to one's own personal information. Like IPP 7, it can be seen as a less formal alternative to FOI, desirable because amendment of one's own personal information will generally require less consideration of other interests than a request to amend someone else's personal information or government policy documents.

However in practice the effect of section 20(5) makes IPP 8 less useful than it could be, owing to a lack of clarity about the breadth of its application. See the further discussion at 3.1.2 below on this issue.

While there was some initial lack of clarity as to how IPP 8 interacts with agencies' record-keeping obligations under the State Records Act, the main difficulty will shortly be resolved by way of a minor amendment to IPP 8 which will come into effect when the HRIP Act commences on 1 September 2004[89].

There is however some confusion for both public sector agencies and members of the public as to how IPP 8 is intended to work in practice.

IPP 8 provides:

> (1) A public sector agency that holds personal information ***must*** …make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the personal information:

[89] The amendment moves from s.20(4) to IPP 8 itself (s.15(4)) a provision which states that IPP 8 clearly overrides section 21 of the State Records Act, despite section 25 of the PPIP Act which otherwise would allow the State Records Act to override IPP 8.

(a) is accurate, and

(b) … relevant, up to date, complete and not misleading.

(2) ***If a public sector agency is not prepared to amend*** … the agency ***must*** … take such steps as are reasonable to attach to the information … any statement provided by that individual of the amendment sought.

(3) ...

The issue is whether the language of sub-section (2) in IPP 8 ('*if* an agency is not prepared ...') overrides the obligation in sub-section (1) ('an agency *must* ... '). At face value, the two requirements stand in conflict. However the Administrative Decisions Tribunal has not been prepared to read down sub-section (1) so as to hold that the only amendments that can properly be made under sub-section (1) are notations made in accordance with sub-section (2)[90].

Our view is that IPP 8 requires a threshold test: first the agency must determine whether or not the personal information at issue is accurate, relevant, up to date, complete and not misleading. Then, if the answer to any of those questions is 'no', then the agency *must* amend the information under sub-section (1).

We submit that sub-section (2) therefore should only relate to the situation where the answer to all of the above threshold questions is 'yes', but where the person still insists on an amendment. For example it might be a matter of opinion not fact such as a disputed medical diagnosis, or despite the 'accuracy' of a criminal record the person wants to maintain their innocence, or the person might want recorded on their file that they believe in UFOs. Sub-section (2) allows a mechanism to deal with this situation.

It must be acknowledged that while there may be a simple yes/no answer in relation to accuracy of the information, more subjective determinations are required as to whether information is relevant, up to date, complete or not misleading. This subjectivity is accommodated within the mechanisms of IPP 8 by allowing an agency to refer to the purposes of collection or use in their determination.

Recommendation:

- That IPP 8 be amended to clarify an agency's obligations as follows:

(1) …
(2) If a public sector agency ***is not required to amend personal information under s.15(1)(a), and believes on reasonable grounds that it has complied with s.15(1)(b)***, the agency must, if so requested by the individual concerned, ….

IPP 9 (section 16)

IPP 9 requires an agency to take reasonable steps to ensure that personal information is relevant, accurate, up to date, complete and not misleading, before it is used.

[90] See *GR v Department of Housing* [2003] NSWADT 268.

We submit that IPP 9 should include both use and *disclosure* as triggers for the requirement to ensure accuracy.

The mischief IPP 9 is intended to address involves an agency taking action on the basis of information it holds about an individual, and in a way which is adverse to the interests of that individual, without taking reasonable steps to ensure the information is accurate, or in the circumstances irrelevant, incomplete, out of date or misleading. It is only possible to give effect to the intention of the section if 'use' is interpreted as the process of considering, assessing or weighing up personal information so as to make a decision or adopt a further cause of action. It is arguable that it is not possible to disclose personal information without first using it anyway (and hence triggering IPP 9), but Privacy NSW suggests that to remove any doubt this intention should be express within the provision.

That only 'reasonable steps' are required means such an amendment will not create an unreasonable burden on agencies[91].

Recommendation:

- That IPP 9 be amended to include both use and *disclosure* as triggers for the requirement to ensure accuracy.

Note:
Such an amendment would not be necessary if the concepts of 'use' and 'disclosure' were collapsed, as recommended separately below.

IPP 10 (section 17)

IPP 10 places limitations upon the *use* of personal information.

Our only concern with IPP 10 is the dichotomy created between *use* and *disclosure*, the latter being dealt with under IPPs 11 and 12. This dichotomy is largely a peculiarity of Australasian privacy legislation. Elsewhere use and disclosure are dealt with together, often under a generic expression like *processing*[92].

[91] For example the ADT has stated that the test of reasonable practicality in IPP 9 should be applied in a way that reflects the kind of use to be made of information (*GL v Director General, Department of Education & Training* [2003] NSWADT 166, paragraphs 45-46). In *GL* Deputy President Hennessy applied the test with a low threshold, reflecting the fact that the information was only used to provide a school principal with background information.

[92] See for example the UK Data Protection Act 1989 Schedule 1 Data Protection Principles, Principle 6; the Canadian Personal Information Protection and Electronic Documents Act 2000, Schedule 1 Principle 5; the European Union Directive 95/46/EC of the European Parliament of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 2(b). The original OECD Guidelines also covered both concepts within the one 'Use Limitation' principle, applying to information 'disclosed, made available or otherwise used', and the European Union Directive on data protection uses the encompassing concept of 'processing'.

The separate concepts in the PPIP Act has historical roots in the original Information Privacy Principles in the Federal *Privacy Act*, which were drafted in 1988 to regulate Australian Government public sector agencies, and which were the model for the IPPs in the PPIP Act. The distinction has sensibly been removed under the more recently drafted Australian privacy laws[93].

The difficulty created by the different IPPs for use and disclosure is that they involve different standards. In particular, 'sensitive' classes of personal information (such as information about a person's health, sexual activities, political opinions and so on) are afforded a higher degree of protection than other information with respect to disclosure (see IPP 12), but not in relation to use. Yet an inappropriate use of personal information may cause as much harm to the individual as would a disclosure.

The distinction therefore gives rise to a number of technical arguments[94] about the circumstances in which processing information in a particular way should be interpreted as a use or disclosure. These do not significantly assist the protection of privacy.

One common scenario, in terms of complaints to this Office, is the breach of confidentiality that can occur when information about a person is transferred *within* an organisation. For example, a school counsellor tells a school principal about sensitive medical issues relating to a student's parent; the school counsellor only knew the information because the student told the counsellor during a counselling session. If this is treated as a 'disclosure', then the strict test for the handling of sensitive (health) information in IPP 12 will apply. However if it is treated as a 'use', the much more lenient standards in IPP 10 will apply.

The fact that different standards apply to use versus disclosure means that there must be clarity for all parties as to what constitutes use, and what constitutes disclosure. However there are at least three possible ways in which to distinguish between 'use' and 'disclosure':

- Ask: where is the information going? In this context, internal handling of the information is 'use', while external handling is 'disclosure'.
- Ask: who has control? Similar to the above, but allows a more subtle distinction such that the transfer of information to a contractor to use in order to carry out the terms of its contract (eg. an auditor or a mail clearing-house) is a 'use', while the transfer of information to a party over which the originator has no subsequent control is a 'disclosure'.
- Ask: what is happening to the information? 'Use' in this context can mean to put to a (new) purpose, while 'disclosure' suggests a revelation to a person or organisation, with or without a specific purpose.

In a number of contexts the first interpretation makes little sense, for example where information from a confidential selection or discipline process within an agency is divulged, where an agency consists of a number of discrete semi-autonomous units, or where information held by an agency is made available to a contractor or consultant.

---

[93] See the NPPs for the private sector in the Federal Privacy Act 1988 (inserted in 2000), the IPPs in the Victorian Information Privacy Act, and the IPPs in the Northern Territory Information Act.

[94] See for example the arguments put forward in *KJ v Wentworth Area Health Service* [2004] NSWADT 84, in which the respondent agency argued for a hard and fast distinction between use and disclosure to minimise compliance requirements. The Tribunal disagreed with the respondent's submission.

The Act provides no guidance as to which of the above interpretations is to be taken. The ADT has found that 'use' in the context of IPP 10 means "to avail oneself of; apply to ones own purposes"[95].

The conduct variously described in the IPPs as collection, use, and disclosure reflects an analytical distinction between different stages in the information-processing cycle. It is our view that the distinctions should not be exaggerated to the point where they result in significant gaps in the way personal information is protected.

The approach taken by Privacy NSW in the advice given to agencies, and in submissions to the Administrative Decisions Tribunal, is that clear and unambiguous wording would be required to exclude disclosure *within* an agency from the scope of IPPs 11 and 12. In particular, where sensitive information is held by an agency, it may be wholly inappropriate that such information is accessible to persons within an agency other than those persons who must reasonably handle the information. In such circumstances 'disclosure' should be given its plain meaning – to disclose is to reveal. This reasoning is in line with other jurisdictions; for example the New Zealand Privacy Commissioner has taken the view that it is possible to breach a principle by disclosure of information to persons within the same agency[96].

In a case decided by the Tribunal whilst this submission was being written, the Tribunal generally agreed with the Privacy Commissioner's views that disclosure of information could occur *within* a public sector agency:

> While generally speaking the expression "disclosure" refers to making personal information available to people outside an agency, in the case of large public sector agencies consisting of specialised units, the exchange of personal information between units may constitute disclosure.[97]

In that case it was found that the placing of sensitive information, namely psychological counselling notes, on the patient's general medical file placed the area health service at risk of 'disclosing' the information to hospital staff in other units.

There are further difficulties for agencies knowing whether something is a 'use' or a 'disclosure' in the context of related entities. Trying to find the distinction is difficult for local councils[98], for agencies with a governing or advisory board[99], for agencies dealing with quasi-judicial bodies[100], and for large agencies with many distinct units[101].

---

[95] *FM v Vice Chancellor, Macquarie University* [2003] para 42

[96] See the Privacy Commissioner's submissions in the case of GR v Department of Housing [2003] NSWADT 268.

[97] *KJ v Wentworth Area Health Service* [2004] NSWADT 84, at para 50.

[98] For example when the general manager provides financial information about ratepayers in arrears to councillors.

[99] For example Privacy NSW and the Privacy Advisory Committee.

[100] For example the Department of Corrective Services dealing with the Serious Offenders Review Board.

[101] For example both Privacy NSW and the Legal Practitioners Admission Board are business centres of the Attorney General's Department.

A further area of confusion is with respect to contractors. Parliament clearly understood that public sector agencies may need to provide personal information to contractors[102], but it is not clear whether such conduct would constitute a use or a disclosure. Treating such activities as a disclosure may hamper legitimate activities where sensitive personal information is at issue. That may have been Parliament's intention, but it is difficult for all concerned to determine if that is the case.

Recommendation:

- That IPPs 10-12 be amended to provide greater clarity about the privacy standards for 'use' and 'disclosure', by:

  collapsing the concepts of 'use' and 'disclosure' into one principle, as per the NPPs in the Federal *Privacy Act 1988* and the IPPs in the Victorian *Information Privacy Act 2000*;

  or

  matching exactly the privacy standards, and exemptions from those standards, for 'use' and 'disclosure', as per the HPPs in the NSW *Health Records & Information Privacy Act 2002*.

IPP 11 (section 18)

IPP 11 regulates the disclosure of non-sensitive personal information, within NSW. (Disclosures of sensitive personal information, and disclosures outside NSW, are covered by IPP 12).

IPP 11 currently provides a fairly low privacy standard in some respects, yet inflexible in others.

For example it is inflexible in that it doesn't allow for disclosures to occur even when the disclosure is the very purpose for which the information was collected (ie, where the *primary* purpose of the collection was to pass it on to another party). Examples include when a local council is merely a collection agent for a State agency. A focus on regional service delivery and shared corporate services between agencies has increased the likelihood that one agency will collect information on behalf of another, with no intention to store or use the information for its own purposes.

Similarly, IPP 11 doesn't clearly allow information to be 'disclosed' to a contractor, even if it is necessary for that contractor to provide a service to the agency – for example so that a lawyer, accountant, auditor or investigator can provide legal services to the agency. The prospect of contracting out is implicit elsewhere in the Act[103], but IPP 11 appears to prevent such activities.

[102] For example IPP 5 and s.4(4) contemplate this situation.
[103] For example IPP 5 and s.4(4) contemplate this situation.

On the other hand IPP 11 is fairly lenient. It allows any disclosure so long as a notification was given to the subject under IPP 3. This is not nearly strong enough to provide adequate privacy protection from unwarranted disclosures, as it neither requires actual consent, nor does it apply any kind of operational relevance test. That is, an IPP 3 notification can be drafted so widely as to allow completely unfettered disclosure of personal information to third parties. The core privacy principle at the heart of IPP 11 is therefore easily undermined because of the lax mechanism provisions.

Recommendation:

- That IPP 11 be amended to allow greater flexibility with respect to contractors and other disclosures that are directly related to the reason for which the information was collected; and to limit the scope for unrelated disclosures without consent.

Note:
An example of how this recommendation could be achieved follows:

A public sector agency that holds personal information must not disclose the information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency, unless:

the disclosure is ***for the purpose*** for which the information was collected, and the person to whom the information relates has been made aware, in accordance with section 10, that information of that kind is usually disclosed to that other person or body, or

the disclosure is ***directly related[104] to the purpose*** for which the information was collected, and the person to whom the information relates is reasonably likely to have been aware, or has been made aware, in accordance with section 10 that information of that kind is usually disclosed to that other person or body, or

the disclosure is for an ***unrelated purpose*** but the person to whom the information relates has expressly consented to the disclosure for that purpose in the knowledge that the disclosure would not be permitted by this section otherwise, or

the agency believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.

IPP 12 (section 19)

Section 19(1) in IPP 12 provides a higher standard for disclosures of particularly sensitive personal information, which is defined as:

> information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities

[104] This 'directly related' test should include information disclosed to an organisation or individual contracted to provide services to the agency, but only where such disclosure is reasonably necessary for the service provider to provide its services.

It is our submission that the special protection of these classes of personal information is appropriate. The possible misuse of health records and health information in particular causes much concern in the community; in terms of information privacy matters, health information is the most frequent type of information at issue in informal enquiries, formal complaints, internal review applications and requests for advice received by Privacy NSW[105].

However one other class of personal information is worthy of special protection: information about a person's criminal history or criminal record. Around 6% of enquiries and complaints received by Privacy NSW relate to misuse of a person's criminal history or criminal record. The inappropriate disclosure of spent convictions is of particular concern, particularly in the employment context[106]. The potential for the internet and powerful search engines to undermine spent conviction laws, which encourage rehabilitation by allowing society to 'forgive and forget' old and minor offences, is of particular concern in relation to privacy protection[107]. There is a danger that genuine and legitimate concerns about child protection and security risks can too easily promote disproportionate responses, in which all employees are 'checked' regardless of the risk posed, and all types of criminal records are treated as evidence of a threat to safety. This class of personal information is recognised in other Australian privacy laws as deserving of special levels of protection on the same basis as other classes of sensitive personal information[108].

It is also submitted that the list of sensitive classes of personal information could be clarified with respect to 'sexual activities'. On one view this relates to information about a person's sexual preferences (heterosexuality, homosexuality, bisexuality, etc), and on another view this relates to sexual conduct (extramarital affairs, etc) including illegal conduct (sexual assault, etc).

In terms of the structure of the IPPs, the separation of section 19(1) in IPP 12 from section 18 (IPP 11) has caused confusion, and instances in which the stricter provision is overlooked. It is submitted that section 19(1) should be included as a subsection under IPP 11, as it relates more so to the general prohibition on disclosure than it does to transborder data flows.

The remainder of IPP 12 (section 19(2)-(5)) allows two possible mechanisms by which transborder data flows from agencies within NSW to individuals or organisations outside NSW can be regulated. To date neither of these mechanisms have been utilised[109] [110], and

---

[105] See our Annual Report 2002-03.

[106] Existing spent convictions laws do not appear to protect information about a person's criminal history, such as charges that were ultimately withdrawn or dismissed.

[107] For more information on this topic see a recent speech made by the Deputy Privacy Commissioner on *Privacy and records management in a digital age*, at http://www.lawlink.nsw.gov.au/pc.nsf/files/A02-027_11022004.pdf/$FILE/A02-027_11022004.pdf

[108] See NPPs 2 and 10 in the Federal Privacy Act 1988, IPP 10 in the Victorian Information Privacy Act 2000, and IPP 10 in the Northern Territory Information Act.

[109] Section 19(3) provides that the Privacy Commissioner may declare another jurisdiction's privacy law to be a 'relevant privacy law'. Having done so, section 19(2) allows disclosures to such jurisdictions without any further restriction. In practice the Privacy Commissioner is unlikely to ever have the resources to make such a determination. The European Union for example goes to great lengths to determine which other jurisdictions' privacy laws are considered adequate; this process takes years. Furthermore it appears undesirable to allow a disclosure to an outside jurisdiction that would not be allowed within NSW.

therefore the normal rules about disclosure (IPP 11 and IPP 12 in relation to sensitive personal information) apply[111]. If it considered necessary to keep a separate transborder privacy principle, the mechanisms should be amended, to clarify that a person "who is in a jurisdiction outside NSW" includes Australian Government and other instrumentalities even if they are physically located *inside* NSW's geographical boundaries.

Recommendation:

- That the provisions in IPP 12 relating to disclosures of particularly sensitive personal information be incorporated into IPP 11.
- That the provisions in IPP 12 relating to disclosures of particularly sensitive personal information be amended to clarify the scope of 'sexual activities', and to include criminal records and criminal history as an additional class of sensitive personal information.
- That the provisions in IPP 12 relating to disclosures of personal information outside NSW be amended such that they apply to any person or body who is ***subject to*** a jurisdiction ***other than*** New South Wales.

Missing privacy principle: Unique identifiers

All other Australian privacy laws include an additional privacy principle regulating the use of unique identifiers[112].

A 'unique identifier' is a number or code that is used to identify a person for the purposes of an organisation dealing with that person. It includes things like a driver's licence number, and a Tax File Number. The use of unique identifiers is the source of many privacy complaints and concerns[113]. However the pressure on agencies to deliver services efficiently, and in a 'whole of government' or 'joined up government' manner, means greater pressure on agencies to share and link personal information together.

---

[110] Section 19(4) requires that the Privacy Commissioner prepare a privacy code of practice relating to the disclosure of personal information by public sector agencies to persons or bodies outside New South Wales, and that such code be prepared by 1 July 2001. A draft code was prepared, but it was not made by the Attorney General. At least one reason for this is that legal advice was received which cast doubt on the efficacy of the code, due to the wording of section 19(2): that "person or body who is in a jurisdiction outside New South Wales" does not cover persons or bodies *subject to* a jurisdiction other than NSW even though physically located inside NSW's borders – eg. Commonwealth Government departments.

[111] The prohibition on transborder data flows in section 19(2) only comes in to effect once a privacy code has been made under section 19(4).

[112] The use of unique identifiers is included in HPP 12 in the NSW HRIP Act; in NPP 7 in the Federal Privacy Act; in IPP 7 in the Victorian Information Privacy Act; and in IPP 7 in the Northern Territory Information Act.

[113] In 2002-03 for example, the third most common category of record / information type, about which Privacy NSW received formal complaints against the NSW public sector, was 'identity records', including drivers' licences; see our Annual Report 2002-03, page 22.

The adoption of unique identifiers poses significant privacy risks for the individual cardholder, data security risks for the agency holding the information, and may hamper efforts to combat identity theft and identity fraud.

The direct privacy risks for individuals include 'function creep' – that is, secondary uses of the base information by the agency collected it, or by other unrelated government agencies through data-matching. Purpose specification and use limitation are two fundamental principles that underpin the protection of privacy and ensure the fair use of personal information by government.

A further privacy risk relates to the use of the unique identifier by third parties to link information from various sources together. For example the development of a photo identification card for non-drivers[114], as a partner to the driver's licence, would allow activities to be linked and profiled by third parties such as businesses, through use of the unique photo card / driver's licence number. (In the absence of such a card for non-drivers, use of a driver's licence number alone has not provided the necessary 'total population capture' that provides an incentive for profiling.)

A third risk is the increased risk of identity theft and fraud posed by centralised identity management system using unique identifiers. The prevention of identity theft and fraud is not only about the integrity of the issuing authority's systems or their data security. It may seem a counter-intuitive notion, but centralised identity management systems utilising unique identifiers across agencies can pose greater threats to identity theft and fraud than dispersed / multiple identification systems[115].

It is therefore our submission that a privacy principle dealing with unique identifiers should be designed to address concerns about people being reduced to 'a number in the system', and concerns about data-matching and profiling by third parties. A privacy principle dealing with unique identifiers should limit when an agency can:

- require an individual to provide a unique identifier
- adopt a unique identifier that has been assigned by another organisation
- create or assign a unique identifier
- use or disclose a unique identifier

Recommendation:

❖ That the IPPs be amended to incorporate a privacy principle relating to unique identifiers, which limits unique identifiers to single-purpose uses.

[114] See the recent proposal by the NSW Minister for Roads, in Anne Davis, "Non-drivers offered a $40 ID card", *Sydney Morning Herald*, 29 October 2003.

[115] A centralised database of linked unique identifiers is more attractive to criminals than dispersed systems. This is because the perceived 'strength' or reliability of the single document issued by a trusted authority increases uncritical reliance by third parties upon such documents as proof of identity, and often as some 'token' of the person's honesty or intentions. This makes the document more valuable to organised crime. The centralised nature of the information can also make obtaining a false or fraudulent identity more straightforward for the organised criminal. Put bluntly, the organised criminal only needs to bribe one person instead of many.

Missing privacy principle: Anonymity

All other Australian privacy laws include an additional privacy principle of anonymity[116].

Anonymity suggests that wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering into transactions with an agency. The former Federal Privacy Commissioner promoted the value of anonymity thus:

> Complete anonymity is neither possible nor desirable in human society. However, a free society generally allows individuals to make appropriate choices about when, and to what extent, they reveal themselves to others. Requiring individuals to be identifiable when it is not necessary can be a form of privacy intrusion[117].

However anonymity can serve other purposes beyond the individual's privacy protection. Allowing for anonymous health care for example can help promote better public health outcomes in areas such as sexual health. Allowing anonymous enquiries to regulators can encourage problems to be identified and solutions found in circumstances which might otherwise be hidden and therefore exacerbated. Other purposes of social value include allowing individuals and groups to avoid physical or financial harm, and enabling the accountability promoted through 'whistle-blowing'[118].

The need for a privacy principle to promote anonymity is perhaps best demonstrated not by futuristic scenarios, but by the current uses of existing technology to track the movements, preferences and behaviour of 'innocent' people across the State:

- the point-to-point speed camera that knows when you are driving down the Pacific Highway (even if you are not speeding)
- the toll-road camera that knows when you drive through the Sydney Harbour Tunnel (even though you have paid your toll)
- the caller-identification system that diminishes your ability to order a pizza delivery or a taxi fare without being tracked
- iris-recognition technology that knows when you are visiting a gaol
- the GPS technology on a mobile phone that tells a child's parents or school where the child is

Recommendation:

❖ That the IPPs be amended to incorporate a privacy principle relating to anonymity.

[116] Anonymity is included in HPP 13 in the NSW HRIP Act; in NPP 8 in the Federal Privacy Act; in IPP 8 in the Victorian Information Privacy Act; and in IPP 8 in the Northern Territory Information Act.
[117] Malcolm Crompton, Federal Privacy Commissioner, *Proof of ID Required? Getting Identity Management Right*, presentation on 30 March 2004, at the Australian IT Security Forum, available at www.privacy.gov.au/news/speeches/sp1_04.doc
[118] For a further discussion of this issue see Roger Clarke, 1999, *Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice* at www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html

3.1.2 The exemptions to the information protection principles

Sources of exemptions

There are four sources of exemptions to the PPIP Act:

- exemptions written in the PPIP Act itself
- exemptions written in a regulation made by the Attorney General under the PPIP Act
- exemptions written in a privacy code of practice, made by the Attorney General under the PPIP Act
- exemptions written in a public interest direction, made by the Privacy Commissioner under the PPIP Act

Each exemption could affect one or more of:

- the definition of 'personal information' (for example section 4(3)(j))
- whether the Act affects specific functions (for example section 6)
- whether the IPPs apply to a particular agency (for example section 27)
- one or more of the IPPs (for example section 23)
- the public register provisions (for example the Privacy Code of Practice for Local Government)

This plethora of exemption mechanisms has made the PPIP Act confusing for all those attempting to interpret and apply the law. We have only recently finalised the task of 'mapping' all known exemptions – even in a small matrix format the document is four pages long[119].

Elsewhere in this submission (see part 2.1.2) we address the three mechanisms by which exemptions may be granted under the Act. This part deals only with those exemptions granted by Parliament, that is, written into the Act itself.

Statutory interpretation of exemptions

Enforcement of the Act is primarily through individual applicants seeking internal review of conduct or a decision, with binding findings and enforceable remedies only available on subsequent application to the Administrative Decisions Tribunal. The result is an adversarial / litigation model.

[119] The matrix of exemptions only identifies whether or not a particular exemption *might* apply – it does not provide the detail of how that exemption works. The reader must still consult the original source document before relying on an exemption, such as the text of a particular section of the Act, a privacy code of practice or a public interest direction. The matrix of exemptions also sets out only those exemptions which apply at the date of its latest update; because some exemptions such as public interest directions are temporary, the matrix can easily become out-of-date. The matrix can be downloaded from our website at http://www.lawlink.nsw.gov.au/pc.nsf/pages/essentials

Our oversight role in internal review matters allows us to make submissions to agencies, but our interpretation of the Act is not binding. It is therefore up to the applicant themselves to challenge this type of legal reasoning in the Administrative Decisions Tribunal – an option that few applicants have the time or resources to pursue.

It is our observation that this model, in very general terms, results in agencies commonly settling those cases with the greatest chance of success, and defending those claims seen as unmeritorious. Defended claims involve agencies seeking to rely on exemptions in the Tribunal, even if the agency's officer, whose conduct or decision is under review, did not consciously rely on the claimed exemption at the time.

Applicants are often unrepresented in the Tribunal, while respondent agencies are well represented, and better able to make arguments about statutory interpretation. Of the 23 matters proceeding to judgment to date in the Tribunal or Appeal Panel, only five have not involved argument about the statutory interpretation of the exemptions to the definition of 'personal information'[120] or exemptions to the IPPs.

The result of this adversarial and typically one-sided litigation model is that it is in the interests of respondent agencies to argue before the Tribunal for the broadest possible interpretations of exemption provisions, against individual applicants who are often ill-equipped to argue the contrary position, and often have little interest in the implications of statutory interpretation beyond the impact on their own matter.

It would appear that Parliament sought to address this imbalance by creating a role for the Privacy Commissioner in Tribunal proceedings. The Privacy Commissioner does not support, advocate for or represent either of the parties to the dispute. We approach our role in the Tribunal as pursuing an interpretation of the PPIP Act that promotes the objects of the Act, namely to protect the privacy of individuals.

Privacy NSW has therefore taken the view that exemptions provide a necessary component of information privacy legislation, but care should be taken when interpreting them, not to effectively nullify the beneficial purposes of the legislation. We therefore support an approach in which the privacy principles are read purposively, and a restrictive approach is taken to the construction of statutory exceptions.

It is our view that the protection of privacy as a fundamental human right justifies a construction of the PPIP Act that is consistent with Parliament's intention to provide general statutory restrictions on interfering with individuals' privacy, with minimal exceptions to the general rule. This approach to the interpretation of legislation affecting privacy rights has been accepted by the High Court in *Coco v the Queen,*[121] and the Federal Court in *Taciak v Commissioner of Australian Federal Police*[122].

Our submission with respect to the statutory exemptions which follow is therefore made in the light of our experience in advising agencies about the Act on the one hand, and our experience in assisting the Tribunal with matters of statutory interpretation on the other.

---

[120] Indeed one of the difficulties, noted below, is the number of exemptions to the definition of 'personal information' (rather than being framed as exemptions to one or more of the IPPs), and thus applicants may find themselves having to argue about the scope of the Act itself in order to meet a jurisdictional hurdle well before coming to discussion about the facts or the application of the IPPs to the conduct or decision in question.

[121] (1994) 179 CLR 427

[122] (1995) 131 ALR 319

Exemptions to the definition of personal information

'Personal information' is the key to the scope of the PPIP Act. Not only are the IPPs about the handling of personal information, but also the public register provisions in Part 6 and the criminal offence provisions in Part 8 of the Act. Therefore the definition of 'personal information' is crucial.

Section 4(1) defines personal information as

> information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

Section 4(2) provides some illustrations:

> (2) Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics.

Given the implications of exempting a class of information or conduct from the definition of 'personal information'[123], it would seem particularly important that any exemptions to the definition be kept strictly to a minimum.

Yet section 4(3) then goes on to provide 12 exceptions to the above rule, such as information about a person's suitability for employment, information contained in a publicly available publication, and so on.

It is our submission that while a case could be argued for excluding most of the categories in section 4(3) from the operation of one or more of the IPPs, specific exemptions from the relevant IPPs would be preferable to the current situation, which takes these categories outside the scope of the Act altogether.

For example, information about a person collected from a publicly available publication is a category of information that might be considered reasonable and appropriate to exclude from the normal prohibition in IPP 2 on collection of personal information other than from the person themselves. However the current drafting of section 4(3) allows such information to be used or disclosed in ways which would be considered corrupt and be subject to the criminal offence provisions of the Act, were if not for the exemption.

Furthermore, many of the exemptions found in section 4(3) are for types of information that should be subject to particularly tough sanctions against corrupt disclosure, such as information about protected witnesses, information collected through telecommunications interception, and information about adoptions.

[123] If the information or conduct at issue is exempt from the definition of 'personal information', not only will there be no enforceable remedy for a complainant in terms of a breach of their privacy, but they cannot even seek review in the Tribunal of their complaint. Furthermore there will be no offence of corruptly disclosing that information.

Section 4(3)(b) – publicly available publication

Section 4(3)(b) exempts from the definition of 'personal information'

> information about an individual that is contained in a publicly available publication.

'Publicly available publication' is not defined in section 3 of the Act, other than to say that

> "publicly available publication" does not include any publication or document declared by the regulations not to be a publicly available document for the purposes of this Act.

The scope and intention of this provision is unclear, and because of its nature (as an exemption to the definition of personal information per se) its breadth places much of people's personal information at risk of misuse without penalty.

For example this provision has been used to justify disclosure of a complainant's identity (name and address) to a third party, on the basis that their name and address is in the White Pages telephone directory. (In terms of complaints against public sector agencies that proceeded to internal review, 22% of all cases in 2002-03 involved alleged misuse of personal contact details such as name, address and home phone number.)

Section 4(3)(b) has also been used by an agency to deflect an argument that unsubstantiated allegations should not have been used in the department's decision-making about a person, simply because such allegations had been aired in a newspaper.

When the potential scope of this exemption is considered and taken to its logical conclusion[124], the object of the Act itself – *an Act to provide for the protection of personal information and for the protection of the privacy of individuals generally* – is effectively undermined.

Combined with the exemption for disclosures to an agency's minister or the Premier under section 28(3) of the PPIP Act, section 4(3)(b) also allows 'information laundering' to occur[125].

However the utility of the exemption must also be examined from a practical point of view. In order for an agency to be able to rely on this exemption, it must undertake a forensic exercise of tracing back the origins or pedigree of each piece of information, rather than consider the information as a class, or in the context of the collection, use or disclosure now at issue. This means that the name of address of clients of an agency could be treated differently, depending on whether or not each appears in a published telephone directory.

---

[124] Even taking the view that 'publicly available publication' only includes such mass publications as newspapers and the White Pages telephone directory, this could take many people's name, date of birth and parents' and siblings' names (which appear in birth notices), home address and home telephone number out of reach of the Act. The Appeal Panel of the Administrative Decisions Tribunal found in *Commissioner of Police, New South Wales Police v EG; EG v Commissioner of Police, New South Wales Police (GD)* [2004] NSWADTAP 10 that "meaning is gleaned from both the content and the context in which information or an opinion appears" [para 59] and therefore for example "a name and address in a telephone directory conveys different information to the same name and address held in the file of a child protection agency" [para 61]. Nonetheless the Appeal Panel stated that the interpretation of section 4(3)(b) cannot be confined to "information which is both contained in and sourced from a publicly available publication" [para 58].

[125] This point is dealt with in more detail below, in relation to section 28(3).

The absence of any definition of 'publicly available publication' has also been the source of confusion and disagreement about the interpretation of the PPIP Act. What is a 'publication'[126]? How widely must it be distributed or read for it to be considered 'publicly available'? How are publicly available publications different to public registers?

Despite the necessity of the information's inclusion in a 'publication', some affected parties have asserted interpretations of the phrase which include any document which is made publicly available (such as a court record)[127], information which is stated in some public forum (such as a criminal conviction read out in open court)[128], or information that could be made available to a member of the public upon application (such as information applied for under the FOI Act or section 12 of the Local Government Act, or a public register)[129].

It has been Privacy NSW's advice to agencies that section 4(3)(b) does *not* provide a 'public domain' exemption of the type that might apply in relation to an action for breach of confidence, rather than breach of privacy. This view has been supported to some extent by case law[130]. Nonetheless the lack of clarity surrounding section 4(3)(b) seems to have added to the common misunderstanding in which privacy is treated like confidentiality.

The collection, use and disclosure of information about a person from publicly available sources or from the 'public domain' can still have considerable privacy impacts[131]. For example the discredited techniques of the former Special Branch of the NSW Police relied greatly on the creation of dossiers of material collected from publicly available sources such as press clippings.

Most of us make distinctions between what we share with our partners or close friends, and what we share with a neighbour over the fence; or what we would tell our doctor compared to what we might tell our employer. Privacy is about respecting these choices; allowing each person some control over who knows what about them. In this sense, privacy is about our ability to define who we are, our very identity, and how we are perceived by others.

If we take seriously the proposition that the IPPs are about protecting informational privacy by putting the control of information about a person back into that person's hands, it must be accepted that context is everything.

As American academic Jeffrey Rosen noted in his book *The Unwanted Gaze*[132],

> Privacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge.

---

[126] The Macquarie Dictionary defines a 'publication' as *that which is published as a book or the like*, and 'publish' as *to issue or cause to be issued in copies made by printing, for sale or distribution to the public, as a book, periodical etc*.
[127] See the arguments in *Wy Kanak v Department of Local Government* [2002] NSWADT 208.
[128] See the arguments in *FM v Vice-Chancellor, Macquarie University* [2003] NSWADT 78.
[129] See the arguments in *Wy Kanak v Department of Local Government* [2002] NSWADT 208.
[130] For example the ADT has found there is no express or implied exclusion for information or opinions that may be obtained by members of the public through mere observation; see *FM v Vice Chancellor, Macquarie University* [2003] NSWADT 78, para 50.
[131] Profiling, in which conclusions are drawn about people from different sources of data rather than asking the person direct, highlights the possibility of accurate information being misinterpreted. A simple example is this: what would you think of someone who often appears at neo-Nazi rallies? You might jump to the conclusion that that person is a follower of neo-Nazism. But they may in fact be a journalist covering the rallies, or a student of political science writing their PhD on the topic.
[132] Jeffrey Rosen, The Unwanted Gaze, Random House, New York 2000.

The risk of inaccurate information, or accurate information being misinterpreted or taken out of context, has only increased since the days of paper files. The power of the internet search engine should prompt a re-examination of exemptions relating to the collection, use and disclosure of information about a person from publicly available sources[133]. Some questions for this 'Google Age' are: When does shaming end? How long should people remain in the 'digital stocks'?[134]

It is submitted that the appropriate manner in which to deal with publicly available publications is therefore to create specific exemptions as necessary in relation to the IPPs dealing with collection, rather than the current exemption from the definition of 'personal information' itself.

Such a scheme could for example allow an agency to collect personal information from a publicly available publication (such as when looking up an address in the White Pages), but would not allow the agency to in turn disclose the person's name and address to a third party in circumstances that would otherwise breach the IPPs or corrupt disclosure provisions.

As currently drafted, IPP 2 creates the main barrier to the collection of personal information from a publicly available publication. It is submitted that the other information protection principles are flexible enough to not pose unduly restrictive requirements on agencies, so long as their collection of personal information from a publicly available publication is relevant and for a lawful purpose (IPP 1), notification is provided if it is reasonable to do so (IPP 3), and the collection is not excessive, overly intrusive and so on (IPP 4)[135]. The Federal Privacy Commissioner's interpretation of the Federal Privacy Act's requirements point the way in terms of allowing a sensible and context-driven approach to this issue[136].

Recommendation:

- That the section 4(3)(b) exemption from the definition of personal information (information about an individual that is contained in a publicly available publication) be deleted.
- That an exemption to IPP 2 be created for the collection of personal information from a 'publicly available publication'.

[133] For an article about the power of one search engine, Google, to find supposedly 'private' information see Yuki Noguchi, "Watch out, they've got you by the Googles", *Washington Post*, reproduced in the *Sydney Morning Herald*, 14 February 2004, page 27.
[134] These questions have been drawn from a panel discussion led by the Victorian Privacy Commissioner, Paul Chadwick, at the International Conference of Data Protection and Privacy Commissioners, Sydney, September 2003 : "Open justice, forgiveness, compassion, context and proportionality".
[135] If a person demonstrates their homosexuality by participating in a gay pride march, or demonstrates their trade union membership by participating in a rally outside Parliament, and they are photographed at the event and the photograph published in a daily newspaper, should that information be applied in an unrelated context, such as to impact on their relationship with government as a client of a government agency? It is submitted that for an agency to collect such sensitive information, it should be subject to these tests in IPPs 1, 3 and 4.
[136] See Office of the Federal Privacy Commissioner, 2003, *Information Sheet 17 – Privacy and personal information that is publicly available*, available from http://www.privacy.gov.au/publications/index.html#I

❖ That 'publicly available publication' be more clearly defined.

Section 4(3)(c)-(h) – miscellaneous law enforcement categories

Section 4(3)(c)-(h) exempts from the definition of 'personal information' various classes of information that have primarily to do with law enforcement functions of police and similar agencies, namely information:

- about a witness in witness protection
- arising out of a warrant for interception of telecommunications
- contained in a protected disclosure or
- arising out of a controlled operation
- arising out of a Royal Commissioner or similar
- arising out of a complaint about a police officer

It is submitted that, for the reasons noted above about the breadth of exemptions to the definition of 'personal information', that these matters be dealt with as specific exemptions to relevant IPPs, if they are indeed necessary.

It may however be the case that existing exemptions to the IPPs for law enforcement agencies (see section 27), for various law enforcement functions (see sections 23 and 24), and in cases where non-compliance with the IPPs is authorised or contemplated by other legislation (see section 25), already deal with whatever problems in relation to law enforcement were anticipated when section 4(3) was drafted.

The language used in section 4(3) has also made the exemptions extremely difficult to define. In particular, the phrase "arising from" requires a forensic exercise of tracing back the origins or pedigree of a piece of information, rather than consider the information in the context of the collection, use or disclosure now at issue[137]. It is submitted that this particular form of words has enabled a broadening of the scope of the exemption beyond that which was presumably desired by the legislature.

Recommendation:

❖ That the section 4(3)(c)-(h) exemptions from the definition of personal information be reviewed in consultation with affected agencies, and deleted if found to be unnecessary.

❖ That any remaining exemptions in section 4(3)(c)-(h) be worded more specifically to define the scope of the exemption.

❖ That any remaining exemptions in section 4(3)(c)-(h) be re-cast as exemptions to specific IPPs.

[137] See for example *GA and Ors v Department of Education and Training and NSW Police* [2004] NSWADT 2.

Section 4(3)(i) – exempt FOI documents

It would appear that this exemption is aimed at preventing first party access requests under the PPIP Act from becoming a 'backdoor' way of obtaining Cabinet and Executive Council documents that are exempt from access under the FOI Act.

Given the existing exemption under section 20(5) which imports any restrictions from the FOI Act into consideration under the PPIP Act (see more below), and the general exemption under section 25 which allows non-compliance with the IPPs when authorised or contemplated under another Act (see more below), this further exemption from the definition of 'personal information' for Cabinet and Executive Council documents appears unnecessary.

Again the language of the exemption ('information about an individual that is contained in a document …') is likely to be much broader in scope than was intended to achieve the purpose of preventing access to those specific documents, such that any personal information which is attached to a Cabinet Minute henceforth loses all privacy protection under the PPIP Act.

Recommendation:

- That the section 4(3)(i) exemption from the definition of personal information be reviewed in consultation with the Cabinet Office, and deleted if found to be unnecessary.
- That if the exemption is found to be necessary, that it be re-cast as an exemption to specific IPPs.

Section 4(3)(j) – suitability for employment

Section 4(3)(j) exempts from the definition of 'personal information'

> information or an opinion about an individual's suitability for appointment or employment as a public sector official.

This provision was the result of an amendment included during Legislative Council debates on the then PPIP Bill, and appeared to be aimed at allowing 'free and frank' referee discussions.

However as noted above, the impact of establishing this as an exemption to the definition of 'personal information' is that it takes almost all information about public sector employees out of the scope of the Act - including the 'corrupt disclosure' criminal provisions.

We understood the exemption was supposed to be about the selection process, to allow the transfer of an employee's service record between departments, free and frank reference checks, and criminal record / integrity checks where appropriate. However the very first case brought to the Administrative Decisions Tribunal under the PPIP Act confirmed that section

4(3)(j) as drafted does not achieve its purpose, having gone well beyond just the personal information issues involved in the selection process[138].

One complaint that proceeded to internal review under the Act demonstrates the illogical consequences of this provision. The particular matter involved a disclosure of personal information during a selection process; a member of the selection committee told an unrelated party of the identity of one or more of the applicants[139]. The only information disclosed was the name and telephone number of a job applicant. There was no information *about* their suitability per se, and therefore the conduct was not affected by the exemption under section 4(3)(j). The conduct was found to breach the IPPs, the council's code of conduct, the ICAC Act and possibly also the corrupt disclosure provisions in the PPIP Act; the council provided an apology and compensation to the job applicant as a result.

However the paradox is that had even *more* information been disclosed, such as a copy of the applicant's CV or written application which could be described as about the applicant's suitability for the job, it would have been exempt from the definition of personal information under section 4(3)(j), and therefore neither the IPPs prohibiting disclosure nor the corrupt disclosure offence provisions would have applied.

The employment context is one in which many and varied privacy issues arise, given the personal information likely to be held about employees – details of their bank accounts and tax file number, records of sick leave, personal contact details, applications for employment, transfer or promotion, disciplinary information, criminal record or service checks, reference checks, health checks and so on. Not surprisingly, employees as a class commonly appear as complainants or internal review applicants[140]. However the impact of section 4(3)(j) has effectively been to deny privacy protection to employees of government agencies for much of their personal information[141].

It is submitted that, for the reasons noted above about the breadth of exemptions to the definition of 'personal information', that these matters should instead be dealt with as specific exemptions to relevant IPPs, if they are indeed necessary[142].

---

[138] In *Y v Director General, Department of Education & Training* [2001] NSWADT 149, President O'Connor interpreted section 4(3)(j) thus: "The information in issue must be able to be shown to be information 'about … suitability.' It must contain within it language which indicates to an objective observer that the information canvasses the aptitude and competence of the employee with respect to their current or prospective employment (and can embrace such matters as co-operativeness, ability to work effectively as part of a team and interpersonal skills). If this approach is adopted, then it would be an unusual case where the exclusion would apply outside what I have described as the routine personnel context (that of recruitment, promotion, discipline and involuntary retirement)" [para 36].

[139] The details of this internal review were included as a case study in our 2002-03 Annual Report, see pages 33-35, available at http://www.lawlink.nsw.gov.au/pc.nsf/pages/annrep

[140] In 2002-03, 18% of complainants against NSW public sector agencies were employees of the agency complained about, and 15% of internal review applicants were employees of the agency complained about; see the Privacy NSW 2002-03 Annual Report.

[141] Other decisions on this point include *BQ v Commissioner of Police* [2002] NSWADT 64, and *GL v Director General Department of Education and Training* [2003] NSWADT 166.

[142] In most cases 'free and frank' referee discussions could take place in compliance with the IPPs because the applicant has nominated the referee and consents to the discussion taking place.

It may however be the case that existing exemptions, such as in cases where non-compliance with the IPPs is authorised or contemplated by other legislation (see section 25), already deal with whatever problems in relation to recruitment were anticipated when section 4(3) was drafted[143].

Recommendation:

- That the section 4(3)(j) exemption from the definition of personal information be deleted.
- That the need for any exemptions in relation to recruitment processes be the subject of further review and consultation.
- That if any exemptions in relation to recruitment processes are found to be necessary, that they be re-cast as an exemption to specific IPPs.

Exemptions for specific functions

Section 6 - judicial functions

Section 6 provides:

> (1) Nothing in this Act affects the manner in which a court or tribunal, or the manner in which the holder of an office relating to a court or tribunal, exercises the court's, or the tribunal's, judicial functions.
> …
> (3) In this section, "judicial functions" of a court or tribunal means such of the functions of the court or tribunal as relate to the hearing or determination of proceedings before it, and includes …

This exemption is drafted in such a way that non-judicial functions of courts and tribunals will be affected by the PPIP Act. It is the dividing line between judicial and 'other' functions that would benefit from further clarification for both interpretation of the PPIP Act and related legislation dealing with public accountability for information management (such as the FOI Act and the State Records Act). To date judicial interpretation of the phrase 'judicial functions' has shed little light on the scope of the provision as it applies to personal information[144].

It is our submission that 'judicial functions' would include the hearing and determining of proceedings and all orders pertaining thereto, whereas the administration and publication of court lists, registry decisions in relation to application forms and processes, registry decisions about access to and publication from court files should be defined as non-judicial

[143] For example, the new Public Sector Employment and Management Act 2002 (or the guidelines issued under that Act) may now provide guidance and clarity on questions such as what can and cannot be included in a person's service record, when it can be transferred, when criminal record or integrity checks can be conducted and what that process should involve, and what information can and cannot be sought from a referee.

[144] See for example a consideration of the exemption under the FOI Act in N v Director General, Attorney General's Department [2002] NSWADTAP 41.

functions[145]. The NSW Ombudsman has also argued that there should be greater scrutiny of administrative decisions made by courts and tribunals, such as the publication of the list of reserved judgments[146].

Complaints to Privacy NSW about the handling of personal information by courts and tribunals have included the inclusion of a child's name in a published court list, the disclosure of a plaintiff's contact details to the respondent, a lack of notification about standard court processes (including the manner in which each party's papers will be provided to the other), the release of subpoenaed documents to third parties, media access to court files, and the supply of court decisions to legal publishers such that 'spent' convictions are published on the internet[147]. The unrepresented litigant or witness appears to be particularly vulnerable in this respect.

While possible solutions to many of these privacy concerns include anonymising judgments or court lists are policy decisions for courts themselves rather than the executive government, this may be an area which would benefit from some further, comprehensive review, such as by the Law Reform Commission[148].

Recommendation:

- That the section 6 exemption for judicial functions be more clearly defined.
- That further consideration be given to a review of policy and practice with respect to anonymisation of court records.

Exemptions to the IPPs for specific agencies

Section 27 – law enforcement agencies

Section 27 provides (emphasis added):

> (1) Despite any other provision of this Act, the Independent Commission Against Corruption, the Police Service, the Police Integrity Commission, the Inspector of the Police Integrity Commission, the staff of the Inspector of the Police Integrity Commission and the New South Wales Crime Commission ***are not required to comply with the information protection principles***.

[145] See for example the arguments posed as to whether or not information collected in a way that would be contrary to IPP 2, in order to be supplied to a court, was in response to an order or a request of the court, and whether the carrying out of judicial orders (or requests) by a party can rely on the exemption in section 6, in *GV v Office of the Director of Public Prosecutions* [2003] NSWADT 177.
[146] See the 2000-01 Annual Report of the NSW Ombudsman, page 107.
[147] See for example "Some say it's criminal that others can see their court records", a New York Times article reproduced in the *Sydney Morning Herald*, 6 September 2002.
[148] For further discussion on this point see the paper "Justice: now open to whom?", delivered by former Privacy Commissioner Chris Puplick, in his address to judges' conferences in May 2002. Versions of this paper have also appeared in the *Law Society Journal*, June 2002, Vol 40 (5) 51 and *The Judicial Review*, Vol 6(1) 95. The full paper is available on the Privacy NSW website at http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_publications#14

> (2) ***However, the information protection principles do apply*** to the Independent Commission Against Corruption, the Police Service, the Police Integrity Commission, the Inspector of the Police Integrity Commission, the staff of the Inspector of the Police Integrity Commission and the New South Wales Crime Commission ***in connection with the exercise of their administrative and educative functions***.

In the second reading speech on the then PPIP Bill, the then Attorney General, the Hon Jeff Shaw QC, explained this provision thus:

> "The purpose of the legislation is not to protect secrecy in dealings or to protect the Government from accountability for its actions, and accordingly there are generous exemptions in the bill for such investigative agencies as the Independent Commission Against Corruption, the Police Integrity Commission and the New South Wales Crime Commission, which have to comply with the information protection principles in connection with the exercise of their administrative and educative functions. A similar exemption is provided for the Police Service"[149].

We understand therefore that the purpose of section 27 is to ensure accountability of the Government, by ensuring that 'privacy' cannot be used as a 'secrecy' shield, behind which government agencies may hide from proper scrutiny by other 'watchdog' bodies. Specifically, section 27 aims to protect these agencies from any barriers that the information protection principles might otherwise pose to their operational and investigative activities.

It is our submission that this intention of section 27 is not being met. The legitimate functioning of watchdog bodies and the police could be safeguarded by other measures, while reducing the negative side effects of the current situation.

The first significant difficulty with section 27(2) is that it is a reverse test. That is, the effect of the exemption is that the IPPs only apply to what fits into the phrase 'administrative and educative functions'[150]. This not only exempts police and similar agencies' operational functions (which was presumably the intention of Parliament), but any other type of conduct that is not 'administrative' or 'educative'.

For example, conduct that represents a gross misuse of police operational information cannot be classified as 'administrative' or 'educative', and is therefore not regulated – yet it is exactly the type of conduct that should be regulated. The case of HW v Police[151] clearly illustrates this point.

In that case a police officer assisting the DPP prepared an invalid subpoena and presented it to the NSW Medical Board and HW's employer, an area health service. The Medical Board and the area health service provided information about HW to the police officer, including details of HW's personal medical history. The police officer handed the information directly to the prosecution and defence teams in court, instead of returning it to the court in a sealed envelope. As a result of this improper process, sensitive information about HW became known to members of the prosecution and defence teams, and also allegedly to HW's father

---

[149] Corrected Copy NSW Legislative Council Hansard, Article No.44 of 17 September 1998, pages 7599-7602.

[150] For example the 'educative' functions of NSW Police have been described by the ADT as the work done 'in connection with community and school education programs, as well as its internal education and training programs'; see *HW v Commissioner of Police, NSW Police Service and Anor* [2003] para 31.

[151] *HW v Commissioner of Police, New South Wales Police Service and Anor* [2003] NSWADT 214

who sat in court when the information was exchanged, in circumstances where it might otherwise never have become known.

The Tribunal accepted that the conduct of the police officer could not be categorised as 'educative' or 'administrative'. Therefore, even though the conduct was prima facie an unlawful collection of personal information, the police were not bound to comply with the IPPs.

The Administrative Decisions Tribunal stated:

> The events identified by this application for review do not reflect well on the agencies concerned…
>
> Hopefully those actions have contributed in the future to greater rigour in the process of collecting sensitive information by subpoena and ensuring that strict protocols are observed in keeping subpoenaed material secure and presenting it direct to the court or tribunal.
>
> As to the application for review as it relates to the Police Service, it must, for the reasons given, be dismissed. The Police Service enjoys a substantial immunity from the application of the IPPs.
>
> … The DPP does not enjoy as substantial an immunity from the application of the IPPs, and that is the basic reason for the seemingly odd result that the Police Service has escaped any adverse finding and the DPP remains at risk of one.[152]

At least if the reverse test was used (for example, that the IPPs do not apply to conduct in pursuit of bona fides investigation and / or operational functions) then a gross misuse of operational information would not be seen as 'in pursuit of bona fides operational functions', and hence would be regulated by the IPPs.

The second difficulty is lack of clarity about what is or is not included in the scope of the exemption. That is, even if the test is reversed as recommended, 'operational functions' would require some concise definition. Examples of conduct which has been the subject of complaints to Privacy NSW or internal review applications to NSW Police have included the administration of criminal history information (including the accuracy of COPS database entries, the accuracy of criminal records, access to and disclosure from criminal records), disclosures to the media, the sale of information to insurance companies, the activities of a police officer in supporting a prosecution, and internal recruitment practices[153]. In each case there has been ambiguity or disagreement as to whether or not the conduct in question could or should be categorised as educative / administrative or 'other / operational'[154].

The confusion surrounding this area has prevented closer scrutiny by the Privacy Commissioner or the public of whether the administration of criminal history information, for example, is aiding or remedying identity theft and identity fraud, and / or frustrating the intention of the 'spent conviction' aspects of the Criminal Records Act[155].

---

[152] *HW v Commissioner of Police, New South Wales Police Service and Anor* [2003] NSWADT 214, paragraphs 65-68.

[153] Most of the complaints received against NSW Police are from their own employees.

[154] The case law to date on this issue includes *HW v Commissioner of Police, NSW Police and Anor* [2003] NSWADT 214, and *GA & Ors v Department of Education & Training and NSW Police* [2004] NSWADT 2. A similar exemption in the FOI Act has been found not to directly assist interpretation of section 27; see *GA & Ors v Department of Education & Training and NSW Police* para 32.

[155] It is our understanding that when a person makes an FOI request for a copy of their own criminal record or statement that they have no criminal record (such as may be required by their prospective or

In particular it is our submission that the maintenance of criminal records and criminal histories should be seen as an administrative function of NSW Police, such that first party access should be allowed under IPP 7 (instead of people having to make FOI applications to receive a copy of their own criminal record), and accuracy made enforceable under IPP 8 and IPP 9, except where the existing law enforcement exemptions apply (including under the FOI Act).

The third difficulty with section 27 is that it is cast too broadly, as it provides a 'blanket' exemption from the IPPs for all the covered activities. It is our submission that section 27 delivers for a few select agencies the very shield that it was intended to prevent – a shield of secrecy to prevent scrutiny of government conduct. For example, why shouldn't the listed investigative and law enforcement agencies be obliged to limit their collections of personal information to that which is reasonably necessary for their functions, or to take reasonable steps to ensure that the information on which they base their actions is accurate? The danger of the blanket exemption in allowing misconduct to escape scrutiny or remedy is well illustrated by the case of HW v Police, mentioned above.

Investigative and law enforcement activities are already subject to some specific exemptions in sections 23 and 24, and general exemptions under section 25, which, with some considered review and redrafting, should be able to protect legitimate investigative and law enforcement activities from whatever detriment is anticipated from compliance with fair information practices.

A more focussed exemption for law enforcement functions of law enforcement agencies would be consistent with other Australasian privacy law[156].

Recommendation:

- That the section 27 exemption be reviewed as to its necessity to prevent detriment to the conduct of legitimate law enforcement and investigative activities, and if found to be not necessary, deleted.
- That the section 27 exemption, if retained as necessary, be redefined such that it only exempts the legitimate law enforcement and investigative activities of the named agencies from specific IPPs.

Section 28(1) – complaint-handling agencies

Section 28(1) provides (emphasis added):

> (1) The Ombudsman's Office, Health Care Complaints Commission, Anti-Discrimination Board and Guardianship Board are not required to comply with section 19.

---

current employer), the resulting report does not excise old matters which the applicant may legitimately consider 'spent' and thus not necessary to disclose to their employer.

[156] See for example section 13 of the Victorian Information Privacy Act, which focuses on law enforcement functions. As far as we can determine, the Federal Privacy Act does not include any exemptions specific to the federal police.

Section 19(1) covers sensitive information : “ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities”; while section 19(2)-(5) covers inter-jurisdictional transfers.

This exemption is too broad – it provides a *carte blanche*. Why should these agencies be allowed to disclose particularly sensitive personal information about any person without any limits, and/or disclose any personal information outside NSW without any limits?

Health information will be taken out of the scope of the PPIP Act shortly, when the HRIP Act commences. Of the other categories of ‘sensitive’ personal information, it is not clear that any of these agencies would even normally deal with information about union membership, sexual activities, political opinions, or religious or philosophical beliefs (with the possible exception being the Anti-Discrimination Board with respect to discrimination complaints about sexuality or race). In any case there is no reason to allow these agencies to disclose such information with impunity.

The more relaxed information sharing arrangements allowed for complaints handling agencies, introduced in 2002, likely obviate the need for this provision even where such disclosures might be reasonably necessary for the purposes of these agencies’ investigative and/or complaint handling functions.

It is submitted that this provision should be deleted as unnecessary, or at least amended to limit its scope and allow review of claims made under this exemption. An objective test (that would allow review by the ADT) could for example be ‘where the agency is reasonably satisfied that non-compliance would prejudice their investigative and/or complaints resolution functions’.

Recommendation:

- That the section 28(1) exemption be reviewed as to its necessity to prevent detriment to the conduct of legitimate investigative and/or complaint-handling activities, and if found to be not necessary, deleted.
- That the 28(1) exemption, if retained as necessary, be redefined such as to limit its scope and include an objective test so as to allow a review of conduct under the exemption.

Exemptions to the IPPs generally

Section 4(4) – when is information ‘held’ by an agency

Section 4(4) provides:

> (4) For the purposes of this Act, personal information is "held" by a public sector agency if:
>
> (a) the agency is in possession or control of the information, or
>
> (b) the information is in the possession or control of a person employed or engaged by the agency in the course of such employment or engagement, or

(c) the information is contained in a State record in respect of which the agency is responsible under the State Records Act 1998.

IPPs 5-12 use language to indicate that they apply to information that is 'held' by a public sector agency[157]. The purpose of section 4(4) is therefore to define the scope of the application of the IPPs. Yet each of the IPPs that govern conduct after the point of 'collection' in the information processing life-cycle effectively apply to information held by an agency. This provision could more explicitly explain this concept (that is, that IPPs 5-12 apply to information 'held' by an agency) before defining what 'held' means.

Recommendation:

- That section 4(4) be more explicitly expressed in terms of the significance of IPPs 5-12 to information that is 'held' .

'Held' is a state that can exist independent of 'collection'[158]. That is, the obligation to store, use and disclose information, and provide access to that information, in accordance with fair information handling principles arise whenever an agency 'holds' information, irrespective of way in which the information was collected.

There has been some case law on the phrase 'possession or control' in section 4(4)(a), supporting our view that there is no requirement for any proprietary rights to be established before information or an opinion can be 'held' by an agency[159]. Nor is 'held' information limited to that captured in formal record systems – a distinction that makes privacy law, with its focus on 'information' instead of 'documents' or 'records' – distinct from freedom of information and records management laws[160].

However it is our submission that section 4(4)(b) is the more difficult part of this provision to interpret. Section 4(4)(b) has the effect of making public sector agencies liable for the actions of their contractors, in terms of compliance with the IPPs. This is entirely appropriate, and consistent with other Australian privacy laws; government agencies should not be able to 'contract out' of its accountability arrangements.

[157] Each of these IPPs uses the word 'held' or 'holds'.

[158] Elsewhere the Act provides that information is not 'collected' if it is unsolicited (see section 4(5)). The Appeal Panel of the ADT has clearly found that even if information was not 'collected' (for example because it was unsolicited), once the information is in the possession and control of the agency, it is 'held', and the remaining IPPs apply to that information; see *Vice-Chancellor, Macquarie University v FM (GD)* [2003] NSWADTAP 43, para 87. Furthermore an understanding of the manner in which information is generated also demonstrates that information may be generated within an agency, for example through a process of creation, observation, assessment, analysis or observation, such as occurs in schools or hospitals.

[159] See for example *Vice-Chancellor, Macquarie University v FM (GD)* [2003] NSWADTAP 43. The fact that the PPIP Act takes as its subject matter information rather than records provides an indication that it was not intended to be limited to information of a proprietary nature. Indeed if a proprietary interest were attached this would impair the remedies available.

[160] Again see *Macquarie University v FM NSW*.

However the significance of this provision is somewhat lost within a definition of what information is 'held' by an agency. Furthermore, as noted above, information that is 'held' may not have been 'collected'. Yet it is our submission that the collection of personal information by a contractor, on behalf of a public sector agency, should also be covered by the PPIP Act.

The test for responsibility of an agency is whether the contractor is 'a person employed or engaged by the agency', and if their handling of the personal information in question was in their 'possession or control', 'in the course of such employment or engagement'.

Interpretation of this provision has proven difficult for public sector agencies, contracted service providers, NGOs funded by State or local government agencies, members of the public and clients of those services.

By way of background, the Federal *Privacy Act 1988*, in its private sector coverage, explicitly excludes the activities of organisations that are performed under or pursuant to a contract with a State or local government agency. The Federal Act does not regulate 'contracted service providers to State agencies' on the assumption that the States will deal with their handling of personal information under State law and/or contractual conditions[161].

However the wording of section 4(4)(b) in the PPIP Act does not match the wording of the Federal Privacy Act. It is not clear whether it includes services provided direct to an agency paying for them[162], and/or services provided to the agency's clients on behalf of the agency funding the contractor (that is, 'contracting out' the provision of a core government service)[163], and/or untied funding arrangements[164].

There is a risk that some private sector organisations may effectively be caught by both Acts, with their differing privacy standards. However of even more concern is the prospect that some organisations' activities will fall into an unregulated 'gap' between the State and Federal Acts.

For example there is currently some debate between the Australasian privacy commissioners and affected parties as to who, if anyone, has jurisdiction over private sector organisations which build, own and operate toll-roads. Toll-road operators collect vast amounts of personal information from people who use electronic tags in lieu of cash, and can effectively track their movements[165]. At the moment anonymity of movement can be guaranteed by simply using cash. However the move to cashless toll-roads in the near future in NSW has caused particular concern amongst privacy advocates[166].

---

[161] See the definition of 'contracted service provider' in section 6 of the Federal Privacy Act 1988, which includes "an organisation that is or was a party to the government contract and that is or was responsible for the provision of services to … a State or Territory authority under the government contract …"

[162] For example, if DOCS pays PWC to do some management consulting.

[163] For example, if DOCS pays an NGO to deliver a domestic violence service in Western Sydney.

[164] For example, if DOCS funds a community centre to do whatever it wants.

[165] Tag users must supply their name, address and bank account details to the toll-road operators. Details of each car movement through a tollway are recorded by the toll-road operator for billing purposes. Where there is a 'false negative' reading (that is, a genuine tag-holder drives through but the tag is accidentally not read) the car number plate is photographed, and details sent to the RTA for enforcement or correction.

[166] It is currently proposed that casual users of cashless road-tolls will need to purchase in advance single or multi-trip 'vouchers', and supply to the operator at the time of purchase at least the vehicle registration number. More personal information will be required if paying for the voucher other than by

A recent case which settled in the ADT further illustrates the difficulty. The case was brought against an area health service which cited St Vincent's Hospital as the proper respondent. The conduct at issue was a disclosure of sensitive health information by the hospital - a patient's psychiatric information was posted on the internet by accident. The hospital is an affiliated health service under the Health Services Act 1997 and operates a public hospital under section 15 of that Act. The hospital argued it was not a public sector agency as defined in the PPIP Act, because it was not a statutory body representing the crown and its accounts were not audited under the Public Finance and Audit Act. The health service argued that it was not responsible for the hospital's actions as the hospital, although funded by it, was not 'employed or engaged by' the area health service to deliver services. The hospital also indicated that, as a 'contracted service provider' to the State government it was not covered by the Federal Privacy Act.

In effect therefore, the hospital argued that no privacy law applied to it even though the applicant was a public hospital patient. As the matter settled, the ADT did not need to make a ruling on the issue; however that these arguments occur at all illustrates the difficulty when the language of the State and Federal Acts do not exactly match up.

It is interesting to note that by contrast the same hospital is considered a 'public authority' for the purposes of the FOI Act[167].

Even once it is accepted that a particular agency is going to be held accountable for the actions of its contractor, it is our experience that the contractor is often unclear as to what compliance with the IPPs means in a practical sense. Smaller NGOs in the welfare sector for example may be ill-equipped to not only understand the IPPs, but find and interpret the various exemptions that might apply.

Also as noted in relation to IPP 10-12 above, there is a lack of clarity as to whether the provision of personal information from an agency to a contractor, such that the agency is still considered to have some 'control' over the information, constitutes a 'use' or a 'disclosure'.

Privacy NSW has advised agencies that in terms of sensible risk management with respect to their responsibilities under section 4(4)(b), they should include compliance with the IPPs as part of their contracting terms, with penalty clauses and/or indemnity for the agency if the contractor causes a breach. However greater clarity could be achieved if the requirement to bind contractors to meet the IPPs were mandatory, as is the case under the Federal Privacy Act[168].

---

cash over the counter (eg. credit card details). Cashless toll-roads are proposed to work by (i) regular users having the toll deducted from their debit account as they pass through, with the reading coming off a mounted tag, and (ii) casual users driving through without a mounted tag, their number plate photographed, and that number plate matched against a list of vehicles for which casual use vouchers have been purchased. Cost has been the primary argument of operators as to why casual users cannot purchase disposable or re-chargeable mountable tags, with cash, for single or small-volume usage (in the way that one may purchase a stored value telephone card).

[167] See *KR v St Vincent's Hospital* [2004] NSWADT 85.

[168] Section 95B(1) of the Federal *Privacy Act 1988* states: This section requires an agency entering into a Commonwealth contract to take contractual measures to ensure that a contracted service provider for the contract does not do an act, or engage in a practice, that would breach an Information Privacy Principle if done or engaged in by the agency.

Recommendation:

- That a separate provision explain the accountability arrangements for contracted service providers to public sector agencies.
- That the accountability arrangements for contracted service providers include information *collected* by the contractor, as well as information *held* by the contractor, on behalf of the public sector agency.
- That the accountability arrangements for contracted service providers use the same language as that in the Federal Privacy Act, to ensure there are neither gaps nor overlaps in jurisdiction.
- That the accountability arrangements for contracted service providers clarify whether the provision of information from an agency to its contractor constitutes a 'use' or a 'disclosure' (unless the distinction between 'use' and 'disclosure' is removed, as is recommended elsewhere in this submission).
- That the accountability arrangements for contracted service providers require the agency to include in the terms of the contract reasonably explicit instruction as to prescribed conduct that will meet (or proscribed conduct that will breach) the IPPs as they apply to that agency and that activity as if it were being conducted by the agency itself.

Section 4(5) – when is information 'collected' by an agency

Section 4(5) provides:

> (5) For the purposes of this Act, personal information is not "collected" by a public sector agency if the receipt of the information by the agency is unsolicited.

IPPs 1-4 govern the process by which information is 'collected'[169]. The purpose of section 4(5) is therefore to define the scope of the application of IPPs 1-4, and thereby provide an exemption to IPPs 1-4 for information that is 'unsolicited'[170].

This provision could more explicitly explain this concept (that is, that IPPs 1-4 apply to information 'collected' by an agency) before defining what 'collected' means (or does not mean). The difficulty with the current wording is that its scope is not clear. For example IPPs 8, 10 and 11 also mention the word 'collected', and the Administrative Decisions Tribunal has found that the application of those IPPs to unsolicited information is therefore brought into question[171].

[169] Each of IPPs 1-4 uses the word 'collection' or 'collecting'.
[170] This interpretation is shared by Privacy NSW and the Appeal Panel of the Administrative Decisions Tribunal, see *Vice-Chancellor, Macquarie University v FM (GD)* [2003] NSWADTAP 43, para 86: "As we conceive of the term 'unsolicited' it refers to information that an agency finds itself receiving (primary meaning, *Macquarie Dictionary*, 'not asked for'). A public sector agency is not bound by the Collection principles in that situation as it had no opportunity to define or set the parameters under which it was received."
[171] See *KD v Registrar, NSW Medical Board* [2004] NSWADT 5; note however this decision is at odds with the Appeal Panel's decision in Macquarie v FM.

There are difficulties in characterising the process of collecting 'unsolicited' information. 'Unsolicited' means 'not asked for' - information that an agency finds itself receiving[172].

However public sector agencies and members of the public have found it difficult to apply this concept in practice. Examples of conduct which turn on the definition of 'unsolicited' include:

- a local council writes to neighbours affected by a development application, inviting them to make submissions or objections
- an agency announces a review or inquiry and calls for public submissions
- a complaints-handling agency receives a complaint about a matter within their jurisdiction
- a council receives a written complaint from a resident about their neighbour's noisy dog
- an agency receives correspondence from a member of the public about a matter within their minister's portfolio or that agency's responsibilities
- a local council receives a petition from residents about the quality of street-lighting in their area
- an agency sets up a public 'suggestion box' in its foyer or on its website
- an agency mounts a CCTV camera in its foyer for security purposes, but also collects (or 'captures') incidental information about people walking in and out of their building or meeting in the foyer

All of these examples involve an agency ultimately receiving information of a general type that they would reasonably expect to receive (although they may not expect the precise contents), and on which they might reasonably be expected to act or respond. Some of these examples involve some degree of solicitation of a response from a targeted or a broad audience. However none of these examples involve what might be termed 'active' collection in the sense of the agency asking for specific information from a specific person in a formal way – the archetypal staff member with a clipboard, asking a person to fill out a form.

By contrast examples of what could genuinely be described as 'not asked for' would include:

- a complaints-handling agency receives a complaint about a matter that is clearly *not* within their jurisdiction
- an agency receives an anonymous letter criticising a staff member because he is homosexual
- a local council receives a faxed complaint about the actions of the Pope

It is submitted that the Act could better clarify what constitutes 'unsolicited' information for the purposes of exemption from the collection principles. It would be dangerous to adopt a self-serving or circular definition in which the collection principles only apply to collections that are formal, direct, targeted or specific, for this would leave unregulated the broad 'fishing net' approach to the collection of personal information that the Act is supposed to prevent.

A further issue is to what extent unsolicited information *should* be exempt from the collection principles.

---

[172] *Vice-Chancellor, Macquarie University v FM* [2003] NSWADTAP 43, para 86

The policy rationale behind an exemption from the collection principles for unsolicited information is succinctly put by the ADT:

> A public sector agency is not bound by the Collection principles in that situation as it had no opportunity to define or set the parameters under which it was received.[173]

This is particularly an issue for agencies in terms of setting the parameters for collection under IPP 1 (collection must be for a lawful purpose, reasonably necessary, etc), IPP 2 (collection must be directly from the individual), and IPP 4 (collection must be relevant, not excessive, accurate, etc).

However it is submitted that IPP 3 might be applied even to unsolicited information. IPP 3 requires only 'reasonable steps' to be taken to notify the person of various matters, including how the information will be used and to whom it will be disclosed. This flexibility could accommodate a distinction in treatment between material that is solicited in a broad sense but collected passively (such that the recipient cannot control the scope of the precise content that might be received), compared with material that is genuinely 'not asked for'.

Recommendation:

- That section 4(5) be more explicitly expressed in terms of it providing exemptions to the collection principles for information that is unsolicited.
- That the term 'unsolicited' be clarified or defined.
- That consideration be given to limiting the exemption for unsolicited information to IPPs 1, 2 and 4.

As noted above, once information is held – regardless of whether or not it was 'unsolicited' – it becomes subject to IPPs 5-12. However a further difficulty with respect to unsolicited information is that some of those other IPPs state their core principle with reference to the 'purpose of collection' for guidance. Therefore in relation to IPPs 8, 10 and 11, where the handling of the personal information is determined according to the 'purpose of collection', agencies need some way of inferring a 'primary' purpose into information whose purpose of collection was not clear, because it was unsolicited.

One possible solution is to examine why the information was *sent* to the agency. That is, we suggest that the law should look to the prima facie intention of the sender, in providing such information to the agency, in order to define the 'primary purpose' for which the information was intended. In some cases this will be a straight-forward task, especially where the agency solicited a broad category of information for a defined purpose (such as objections to a development application or submissions to a public inquiry), if not soliciting the precise content.

[173] V*ice-Chancellor, Macquarie University v FM (GD)* [2003] NSWADTAP 43, para 86

For example, a petition to a council asking for new street lights is clearly intended to be used for the purpose of facilitating council decision-making and prioritising of resources in relation to its street-lighting program. To use it for direct marketing would not be part of the senders' view of why they sent their information to the council.

In some cases the agency might say the unsolicited information is useless to them for any purpose (for example, the fax to the council complaining about the Pope), but they continue to hold such information because of State Records obligations. In such a case we would suggest that the only 'purpose' against which to reference IPPs 5-12 is the purpose of records maintenance obligations under the State Records Act. Therefore any other use will *prima facie* be beyond its 'purpose of collection'.

Recommendation:

- That the definition of 'unsolicited' information incorporate a mechanism by which the 'purpose of collection' may be determined for such information, so as to apply IPPs 8, 10 and 11.

Section 20(3) – information collected before commencement

This common-sense provision exempts from the collection principles (IPPs 1-4) information collected before commencement of this part of the PPIP Act. Our only suggestion in relation to this exemption is already incorporated above at 3.1.1, namely that all exemptions be replicated as part of, or directly below, the IPPs to which they relate, as is the case in the HRIP Act.

Section 20(5) – incorporation of FOI provisions

Section 20(5) effectively provides that if access could be refused under the FOI Act then it may also be refused for an application made under IPP 6 (information about personal information held by the agency), IPP 7 (access to one's own personal information) or IPP 8 (correction of one's own personal information), as if the 'conditions and limitations' of the FOI Act had been directly imported into the PPIP Act[174]. No doubt this provision is intended so as to prevent the PPIP Act being used as a 'backdoor' way for a person to gain access to a document to which they would not be entitled under the FOI Act.

However the wording of this provision – namely the broad phrase 'conditions and limitations' – provides little guidance on how exactly the access and correction provisions of the FOI Act relate to or are imported into the PPIP Act. For example, does it have the effect of importing:

- the requirement to lodge an FOI request in writing?
- the requirement to pay a set application fee and/or processing fees?
- the list of exempt documents in Schedule 1 to the FOI Act?

[174] Section 20(5) provides: Without limiting the generality of section 5, the provisions of the *Freedom of Information Act 1989* that impose conditions or limitations (however expressed) with respect to any matter referred to in section 13, 14 or 15 are not affected by this Act, and those provisions continue to apply in relation to any such matter as if those provisions were part of this Act.

- the list of exempt bodies in Schedule 2 to the FOI Act?
- the consultation requirements in Part 3 of the FOI Act?

The benefits of a less formal approach to simple requests for access to (or amendment of) one's own personal information are lost if the request must in effect become an FOI application.

Furthermore it is not clear how the major limitation on the FOI Act – that it only applies to 'documents' – affects the much broader definition of 'information' under the PPIP Act. For IPP 8 in particular, it is not clear how the amendment provisions of the FOI Act, which do not make provision for the deletion of information[175], affect the requirement to delete personal information where it is appropriate under IPP 8 (section 15(1)).

The application of provisions of the FOI Act to IPP 6 is even more unclear. IPP 6 is not an obligation to provide documents, or even the information in question; it is an obligation to inform the person in general terms of the nature of personal information held about them, the main purposes for which it is used, and the fact that they can seek access under IPP 7. It is difficult to see how any of the provisions of the FOI Act need apply to such an obligation; the mechanical provisions for processing FOI applications make little sense in this context, and given that the obligation in IPP 6 is only to take 'such steps as are, in the circumstances, reasonable', then the types of particularly sensitive documents that an agency does not even wish to acknowledge exist (for example, that the police have a surveillance report on a criminal suspect) can simply be argued as not reasonable in the circumstances.

These difficulties in the interpretation and application of IPPs 7 and 8 have affected both public sector agencies and members of the public seeking to exercise their rights of access. Privacy NSW drew attention to these difficulties when the then HRIP Bill was being considered by Parliament in 2002[176].

Recommendation:

- ❖ That the exemption in section 20(5) be deleted.
- ❖ That IPPs 7 and 8 be amended to specify exactly which provisions of the FOI Act are to be considered as imported into the mechanisms to be followed under IPPs 7 and 8 respectively.

Section 23 - Exemptions relating to law enforcement and related matters

Section 23 provides (emphasis added):

> (1) A law enforcement agency is not required to comply with ***section 9*** if compliance by the agency would ***prejudice the agency's law enforcement functions***.

[175] See sections 39, 40 and 43 of the FOI Act.
[176] See our June 2002 Position Paper on the HRIP Bill at http://www.lawlink.nsw.gov.au/pc.nsf/pages/hripcomment

(2) A public sector agency (whether or not a law enforcement agency) is not required to comply with ***section 9*** if the information concerned is collected ***in connection with proceedings*** (whether or not actually commenced) before any court or tribunal.

(3) A public sector agency (whether or not a law enforcement agency) is not required to comply with ***section 10*** if the information concerned is collected ***for law enforcement purposes***. However, this subsection does not remove any protection provided by any other law in relation to the rights of accused persons or persons suspected of having committed an offence.

(4) A public sector agency (whether or not a law enforcement agency) is not required to comply with section ***17*** if the use of the information concerned for a purpose other than the purpose for which it was collected ***is reasonably necessary for law enforcement purposes or for the protection of the public revenue***.

(5) A public sector agency (whether or not a law enforcement agency) is not required to comply with ***section 18*** if the disclosure of the information concerned:

(a) is made ***in connection with proceedings for an offence or for law enforcement purposes*** (including the exercising of functions under or in connection with the Confiscation of Proceeds of Crime Act 1989 or the Criminal Assets Recovery Act 1990), or

(b) is to a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ***ascertaining the whereabouts of an individual*** who has been reported to a police officer as a missing person, or

(c) is authorised or required by subpoena or by search warrant or other statutory instrument, or

(d) is reasonably necessary:

(i) for the ***protection of the public revenue***, or

(ii) in order to ***investigate an offence*** where there are reasonable grounds to believe that an offence may have been committed.

(6) Nothing in subsection (5) requires a public sector agency to disclose personal information to another person or body if the agency is entitled to refuse to disclose the information in the absence of a subpoena, warrant or other lawful requirement.

(7) A public sector agency (whether or not a law enforcement agency) is not required to comply with ***section 19*** if the disclosure of the information concerned is reasonably necessary for the ***purposes of law enforcement*** in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed.

This exemption covers five different IPPs, both law enforcement agencies and all agencies, and uses nine different tests.

The absence of express definitions for many of the phrases and tests used has left ambiguity as to the extent of these exemptions.

For example, respondents to a complaint may seek to argue that the expression ‘law enforcement’ under section 23(3), (4) or (5)(a) includes the enforcement of any law of the Commonwealth or of a State or Territory, although under section 23(7) the expression ‘law enforcement’ only relates to criminal offences.

It is our submission that the expression ‘law enforcement’ should not be interpreted as applying to every context where an agency is seeking to give effect to its legal powers and responsibilities. To do so would render large parts of the PPIP Act meaningless, as most of

the activities of public sector agencies could be characterised in these terms. The exemptions in the section are primarily directed toward expediting the investigation of matters that involve breaches of the criminal law and the preparation of cases before courts or tribunals. There is for example a line of authority in the Administrative Decisions Tribunal's FOI jurisdiction which supports confining 'law enforcement' in this way[177].

Another phrase requiring definition is 'for the protection of the public revenue'. This phrase has caused much confusion for those trying to interpret and follow the Act. For example, is this exemption aimed at the pursuit of monies owing to the State such as unpaid fines, and/or to prevent fraud against consolidated revenue, and/or to prevent waste or misuse of public money?

It should be noted that the HRIP Act has incorporated a simpler 'law enforcement' exemption into the health privacy principles; see for example HPP 11(1)(j), which provides:

> (j) the disclosure of the information for the secondary purpose is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed

A separate provision in relation to finding a missing person has also been incorporated into the HRIP Act[178].

Recommendation:

- That the exemptions in section 23 be comprehensively reviewed to clarify their objectives, and their necessity to prevent detriment to the conduct of legitimate law enforcement activities.
- That the exemptions in section 23, if found to be not necessary, deleted.
- That the exemptions in section 23, if retained as necessary, be clarified to a greater degree of specificity, and wherever possible replicate the equivalent provisions in the HRIP Act.

Section 24 – Exemptions relating to investigative agencies

Section 24 provides (emphasis added):

> (1) An investigative agency is not required to comply with ***section 9 or 10*** if compliance with those sections might ***detrimentally affect (or prevent the***

[177] See *Watkins v Chief Executive, Roads and Traffic Authority* [2000] NSWADT 11, paragraphs 39-42; *BY v Director General, Attorney General's Department (No. 2)* [2003] NSWADT 37, paragraphs 43-53; and *McDonald v Commissioner of Police, NSW Police Service* [2003] NSWADT 111, paragraphs 32-36.

[178] See for example HPP 11(1)(h) which provides: "the disclosure of the information for the secondary purpose is to a law enforcement agency … for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person".

proper exercise of) the agency's complaint handling functions or any of its investigative functions.

(2) An investigative agency is not required to comply with ***section 17*** if the use of the information concerned for a purpose other than the purpose for which it was collected is reasonably necessary in order to ***enable the agency to exercise*** its complaint handling functions or any of its investigative functions.

(3) An investigative agency is not required to comply with ***section 18*** if the information concerned is disclosed ***to another investigative agency***.

(4) The exemptions provided by subsections (1)–(3) extend to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter ***that could be referred or made to an investigative agency***, or that has been referred from or made by an investigative agency.

(5) The exemptions provided by subsections (1)–(3) extend to ***the Department of Local Government***, or any officer of that Department, who is investigating or otherwise handling (formally or informally) a complaint or other matter even though it is or may be the subject of a right of appeal conferred by or under an Act.

(6) ***The Ombudsman's Office*** is not required to comply with ***section 9 or 10***.

(7) An investigative agency is not required to comply with ***section 12 (a)***.

This exemption covers five different IPPs, investigative agencies (defined), two additional named agencies and all agencies, and uses five different tests.

The lack of consistency between each test has created ambiguity as to the extent of these exemptions. The necessity of the provisions should also be reviewed.

For example section 24(3) in particular is now redundant for some investigative agencies, as the issue of referrals of complaints between investigative agencies is now dealt with under the complaint referral and information-sharing provisions of the Ombudsman Act[179]. For the remainder, (the ICAC and the Police Integrity Commission), we would suggest that this exemption be amended so as to narrow its scope along the same lines as the complaint referral and information-sharing provisions of the Ombudsman Act; namely that disclosures between investigative agencies should be limited to situations in which a complaint has been referred for action or joint investigation, and the complainant consents to the referral of the complaint itself.

In relation to section 24(6), it should be noted that the Ombudsman's Office is recognised in the definitions to the Act as one of a number of investigative agencies to which section 24(1) applies, creating an exemption to IPPs 2 and 3 in certain circumstances. However that office alone then receives an additional, unqualified exemption to IPPs 2 and 3 in section 24(6).

On the other hand it can be argued that these exemptions are deficient, in that they do not contemplate regular 'investigations' conducted by and within public sector agencies that are not primarily considered 'investigative agencies'. Examples include investigations of staff for alleged misconduct or other disciplinary matters, or investigations of clients or other parties

[179] A copy of the arrangements, signed by Privacy NSW, the NSW Ombudsman, the Office of the Legal Services Commissioner, the Health Care Complaints Commissioner and the Anti-Discrimination Board is available from our website at: http://www.lawlink.nsw.gov.au/pc.nsf/pages/omb_arrange

to determine whether a breach of a condition or licence has occurred (such as a breach of a tenancy agreement, development consent, pollution laws, and so on). Agencies may need to brief external experts, legal counsel and so on in order to conduct legitimate investigations.

This deficiency was recognised early in the Act's life by Privacy NSW, and a draft code to cover this scenario was prepared for consultation. Although the code remains now in only draft form, a series of public interest directions has been granted by the Privacy Commissioner to provide exemptions until this matter is resolved[180]. It is submitted that consideration be given to the incorporation of a more comprehensive exemption for investigations conducted by or within general public sector agencies, so as to obviate the need for future public interest directions or code provisions[181].

The HRIP Act has already incorporated exemptions to specific health privacy principles for investigative agencies[182], and others for general agencies conducting investigations of their staff or persons registered by the agency[183].

Recommendation:

- That the exemptions in section 24 be comprehensively reviewed to clarify their objectives, and their necessity to prevent detriment to the conduct of legitimate investigative activities.
- That the exemptions in section 24, if found to be not necessary, deleted.
- That the exemptions in section 24, if retained as necessary, be clarified to a greater degree of specificity, and wherever possible replicate the equivalent provisions in the HRIP Act.
- That consideration be given to the incorporation of a more comprehensive exemption for investigations conducted by or within general public sector agencies, wherever possible replicating the equivalent provisions in the HRIP Act.

Section 25 - Exemptions where non-compliance is lawfully authorised or required

Section 25 provides:

> A public sector agency is not required to comply with section 9, 10, 13, 14, 15, 17, 18 or 19 if:
>
> (a) the agency is lawfully authorised or required not to comply with the principle concerned, or
>
> (b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).

[180] The current direction is available from our website at: http://www.lawlink.nsw.gov.au/pc.nsf/pages/s41invest

[181] It should be noted that the HRIP Act has incorporated some, if not all, of these types of exemptions into the health privacy principles; see for example HPP 11(1)(i), (j) and (k).

[182] See for example HPP 11(1)(k).

[183] See for example HPP 11(1)(i).

In the second reading speech on the then PPIP Bill, the then Attorney General, the Hon Jeff Shaw QC, explained this provision thus:

> "It should be stressed that the data (sic) protection principles are generally subject to any specific provision in any law relating to the use or disclosure of information."[184]

However the ultimate wording of section 25 relates not only to use or disclosure of personal information, but also the collection, access and amendment provisions, and instead of 'specific provisions' the required nexus to another authorising source can be more tenuous. Section 25 thus provides an exceptionally broad exemption.

In practice we have found it is unclear to agencies and members of the public whether what must be contemplated by the other law is the action (for example, a disclosure of personal information) or the action to deliberately not comply with the IPPs (for example, disclosure that would otherwise be prohibited under IPP 11).

Furthermore the reference in section 25(b) to 'other law' is unclear in its scope. For example, 'other law' might be contemplated to include:

- regulations made under an Act
- ministerial orders made under an Act or regulation
- statutory instruments such as a Local Environmental Plan made under planning law
- quasi-statutory instruments such as a Development Control Plan made under planning law
- a council's code of meeting practice made under the Local Government Act
- a common law 'duty of care'

It is submitted that any interpretations beyond the first point (namely, regulations) has the effect of delegating to agencies and ministers other than the Attorney General the ability to override the privacy protections established by Parliament.

The 'common law' interpretation is being argued in a case presently before the ADT, in relation to the disclosure of health information about a student by a school teacher to an external body; that is, it is argued that a common law 'duty of care' overrides the specific statutory prohibition in IPP 12 (section 19) on the disclosure of health information except with consent or where necessary to prevent or lessen a serious and imminent threat.

A further category – of judicial orders or directions, subpoenas, warrants or other lawful instruments – may also be contemplated under this provision. Yet they are also dealt with (in terms of disclosure) in the section 23(5)(c) exemption.

Even if found to be restricted to Acts and regulations, the current drafting of section 25(b) effectively allows agencies to rely on even the hint of non-compliance under another Act or regulation to justify their non-compliance with almost all of the privacy principles. Thus section 25 has the effect of subordinating a privacy law intended to confer general rights and have general application, to laws limited to specific situations in a way which undermines public expectations and produces wide ranging uncertainty.

---

[184] Corrected Copy NSW Legislative Council Hansard, Article No.44 of 17 September 1998, pages 7599-7602.

For example we have seen internal review matters in which an agency has justified a disclosure of personal information (such as disclosing a complainant's identity to the respondent to their complaint) on the basis that *if* a person had applied for the document under FOI they *might* have got it, and therefore the disclosure (that would otherwise have breached IPP 11) was permitted, necessarily implied or reasonably contemplated under the FOI Act[185]. Such an approach not only avoids Parliament's intentions in relation to the PPIP Act, but circumvents the privacy safeguards built into the FOI Act in terms of consultation when the document in question contains information about a person's personal affairs[186].

It is submitted that this exemption should be narrowed to a provision similar to that in section 6 of the Victorian *Information Privacy Act*, which gives priority to other legislation only in cases of express inconsistency. It is also submitted that the exemption should require agencies to ensure some kind of reasonable necessity to their actions in order to justify non-compliance[187].

Recommendation:

- That section 25 be amended to only provide an exemption in relation to circumstances in which another Act or regulation creates an express inconsistency, and it is reasonably necessary for the agency to carry out the activity or conduct under the other Act or regulation.
- That there be a separate provision relating to conduct that may be required in order to comply with judicial orders or directions, subpoenas, warrants or other lawful instruments.

[185] Our oversight role in internal review matters allows us to make submissions to agencies, but our interpretation of the Act is not binding. It is therefore up to the applicant themselves to challenge this type of legal reasoning in the Administrative Decisions Tribunal – an option that few applicants have the time or resources to pursue.

[186] It is not disputed that if an FOI application had actually been made, and the proper processes under the FOI Act been followed, the disclosure might have been permitted under the FOI Act (and hence section 25 of the PPIP Act would prevent such conduct from being seen as a breach of the IPPs). The point is that it might *not* have been required – see for example a number of FOI cases in which a decision by an agency to not disclose a complainant's identity to the respondent to the complaint has been upheld in the ADT: BY v Director General, Attorney General's Department [2003] NSWADT 37; Optima Developments Pty Ltd v General Manager, Wyong Shire Council [2002] NSWADT 99; Ingram v General Manager, Sutherland Shire Council [2000] NSWADT 69; and Gilling v General Manager, Hawkesbury City Council [1999] NSWADT 43.

[187] To take the same example of an FOI application authorising a disclosure of personal information, our recommended approach to revising section 25 would allow information to be disclosed contrary to IPPs 11 or 12 if (i) the non-compliance with the privacy principle in question is reasonably necessary to comply with an FOI application, and (ii) the agency has followed the provisions of the FOI Act with respect to procedural matters and the 'personal affairs' test.

Section 26 - Other exemptions where non-compliance would benefit the individual concerned

Section 26 provides:

> (1) A public sector agency is not required to comply with section 9 or 10 if compliance by the agency would, in the circumstances, prejudice the interests of the individual to whom the information relates.
>
> (2) A public sector agency is not required to comply with section 10, 18 or 19 if the individual to whom the information relates has expressly consented to the agency not complying with the principle concerned.

Section 26(1) is very broad and appears to allow agencies to take a paternalistic approach to determining what is in the interests of a person. It is not clear what type of situations are contemplated by this provision, and to date there has been no case law on this point. It may be that this provision as aimed at people with decision-making disabilities, but in such a case we would prefer to see solutions that ensure that privacy standards are achieved, not diminished[188].

Section 26(2) is by contrast narrowly drawn. In relation to the exemptions to IPPs 11 and 12 in relation to disclosure, the provision is clear. The requirement for consent to disclosure be 'express' indicates a more onerous standard that 'consent' under IPP 10 for 'use', which could arguably be either express or implied.

The Appeal Panel of the Administrative Decisions Tribunal has found that this express consent provision should be strictly applied in order to protect the right to freedom from interference with privacy:

> In our view the requirement of express consent must be the subject of administrative action by the agency disclosing the information. It must have gone to the individual concerned and obtained an express consent that is precise as to the kind and, possibly, the exact contents of the information to which the consent relates.[189]

The earlier Tribunal case suggested furthermore that what is being consented to is not only the conduct (eg. the disclosure), but the non-compliance with the IPP (ie. the disclosure in the knowledge that if they did not consent it could not occur)[190].

While this concept makes sense in relation to IPP 11 and 12, it seems of little value in relation to IPP 3. Our understanding of section 26(2) is that, in order for an agency not to have to give a person a 'privacy notice' under IPP 3, they must seek the person's express consent to not being given a privacy notice. In a practical sense, it seems easier for the agency to meet IPP 3 itself than this exemption to it.

---

[188] As noted above in part 3.1.1 of this submission, we have recently published a best practice guide: *Privacy and people with decision-making disabilities*, which attempts to provide more flexible mechanisms in which to achieve the core privacy principle at issue.

[189] *Vice-Chancellor, Macquarie University v FM (GD)* [2003] NSWADTAP 43 para 97

[190] *FM v Vice Chancellor, Macquarie University* [2003] NSWADT 78 para 76

Recommendation:

- That section 26(1) be deleted.
- That section 26(2) be amended to only relate to IPPs 11 and 12.

Section 28(2) – health information disclosed for continued care

This provision will become obsolete once the HRIP Act commences, as 'health information' will be taken out of coverage of the PPIP Act.

Section 28(3) – disclosures to Minister, Premier or their agencies

Section 28(3) provides:

> (3) Nothing in section 17, 18 or 19 prevents or restricts the disclosure of information:
>
> (a) by a public sector agency to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or
>
> (b) by a public sector agency to any public sector agency under the administration of the Premier if the disclosure is for the purposes of informing the Premier about any matter.

Members of Parliament are exempt from the PPIP Act, and so once personal information is in the hands of a minister or the Premier, its use or disclosure is not subject to the scrutiny of privacy law. This situation is not in question in this submission, although it is worth noting that by contrast, the Federal Privacy Act covers ministers within the definition of 'agency'.

Nor is it under question that ministers and agencies within their portfolio must be able to freely discuss matters of importance for decision-making at both ministerial and departmental level.

However a reasonable person might assume that one of the objectives of privacy law is to prevent personal information, held in trust by government agencies, from being made available to a wider class of people not subject to that privacy law (such as ministers or MPs) except where necessary, so as to limit the possibility of such information being collected, used or disclosed in an inappropriate manner.

Yet section 28(3)(b) of the PPIP Act allows any disclosure of any personal information by any public sector agency to the Premier for any reason whatsoever. There is no justification for the breadth of this provision.

The impact of section 28(3)(b) is that privacy law does not stand in the way of the Premier of NSW obtaining the medical records of the Leader of the Opposition or those of his family members, or the criminal history of a powerful media figure, or alcohol counselling notes about a senior public servant[191].

[191] The excision of 'health information' from the PPIP Act when the HRIP Act commences will not alter this situation, because the same exemption is replicated in the new HRIP Act.

Combined with the exemption to the definition of 'personal information' in section 4(3)(b) in relation to information contained in a publicly available publication, section 28(3) also allows 'information laundering' to occur.

Information laundering undermines the objectives of the Act, even while complying with the letter of the law. For example, if a public sector agency wishes to use or disclose personal information in a way that would otherwise be prohibited under the IPPs, it can do so – whether accurate or not, whether 'fact' or just opinion, whether relevant and necessary to its functions or merely salacious 'gossip'. The agency merely has to disclose the information to its minister or the Premier under section 28(3)(b); the minister or Premier then discloses that information to the media; and the media reproduces the information in a publicly available publication. At that point the information is no longer protected by the PPIP Act, and all subsequent collection, use or disclosure by public sector agencies is unregulated.

It is submitted that the exemption in section 28(3) should be narrowed in scope such as to allow proper briefings from public sector agencies to their respective ministers to continue, and possibly even expanded to clarify an agency's obligations when handling ministerial correspondence on behalf of their minister[192], while also protecting the privacy of personal information held by those agencies.

Recommendation:

- That the exemption in section 28(3) be amended such that it only applies to disclosures by agencies direct to their responsible minister (or the staff of that minister), where such disclosures are reasonably necessary for the minister to perform the ministerial functions relating to that portfolio or agency.

3.1.3 The public register provisions

What is a public register?

Section 3 provides:

> public register means a register of personal information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee)

Like the exemption for 'publicly available publication' (see part 3.1.2 of this submission), the definition of public register has been the source of confusion and disagreement about the interpretation of the PPIP Act.

[192] Ministerial staff are often the conduit between an agency and its minister. Ministerial staff are considered to be employees of the Premier's Department, and therefore under the PPIP Act the Premier's Department is considered to be the agency which 'holds' any information in their possession. Thus exchanges of information from say the Department of Housing to the Minister for Housing will typically go via the Premier's Department in law, even if the concept is a fairly artificial one. This is one area which could benefit from legislative amendment.

In particular, the phrase 'or is made' is not qualified in terms of whether the practice of making the register publicly available must have, could have, or could only have, occurred prior to commencement of the PPIP Act. It is also unclear as to whether or not the decision to make a register publicly available is itself subject to the IPPs in relation to disclosure of personal information.

This definition has therefore resulted in much confusion about what is or is not a 'public register', especially in relation to local government. For example, prior to commencement of the PPIP Act, some councils incorporated information about property ownership, collected in order to levy rates, into a 'rates book' or 'rates roll' available for inspection at the counter. This was not required by law[193]. In some cases the rates roll was routinely sold to real estate agents, valuers, and other parties interested in its use for direct marketing purposes.

Therefore some councils were able to classify their general property ownership records as a 'public register', while others could not[194]. This situation has led to non-uniform application of the PPIP Act across the State, causing complaints from local councils, property owners, professional property valuers, real estate agents, neighbours of absentee landlords, ratepayers' associations, and developers.

Despite the necessity of the information's inclusion in a 'register', some affected parties have asserted interpretations of the phrase which include any information that could be made available to a member of the public upon application (such as information applied for under the FOI Act or section 12 of the Local Government Act).

Recommendation:

- That the definition of 'public register' be amended so as to only apply to registers required by law to be made open to public inspection, and identified in their authorising legislation as a 'public register'.

Disclosure from a public register

Section 57 provides:

> (1) The public sector agency responsible for keeping a public register must not disclose any personal information kept in the register unless the agency is satisfied that it is to be used for a purpose relating to the purpose of the register or the Act under which the register is kept.
>
> (2) In order to enable the responsible agency to comply with subsection (1), the agency may require any person who applies to inspect personal information contained in the public register to give particulars, in the form of a statutory declaration, as to the intended use of any information obtained from the inspection.

[193] Section 12(1) of the Local Government Act lists a number of documents which must be made available for inspection or copying, but rates information and property ownership records are not included in that list. Section 603 of the Local Government Act sets out a mechanism by which rates information may be made available about an individual property, for a fee.

[194] For a further explanation of the complexities and implications of this provision, see the Department of Local Government Circular to Councils 2000-75 "Is council's rates record a 'public register'?", available at: http://www.dlg.nsw.gov.au/dlg/dlghome/Documents/Circulars/00-75.pdf.

Typically, individuals have little choice over whether or not their personal information will be held on a public register, unless they meet the test for suppression (see below). For example, it is compulsory to enrol to vote, and enrolled voters are put on the electoral roll; if one wants to build a new house, one must obtain a development consent, and development consents are listed in a register of consents. Various professional and trade bodies require registration before one is able to practice (lawyers, medical practitioners, builders, and so on), and the membership records are often required to be made open for public inspection. Councillors must declare their pecuniary interests on forms that become a public register.

The reason that a register is made open for public inspection is usually one of accountability:

- accountability of an organisation's decision-making or activities (eg. development consents can be compared for consistent decision-making; to ensure the conduct of fair elections), or
- accountability of the individual (eg. to ensure a person purporting to be a solicitor really is a solicitor; to check that a councillor has excused themselves from voting on a matter which presents a pecuniary interest).

Yet as rich sources of personal information, public registers can facilitate the abuse of people's privacy. The aim of privacy law is therefore to balance the accountability of both government agencies and individuals with the protection of privacy.

No doubt the purpose of section 57 is therefore to prevent access to personal information held on a public register for purposes other than that for which it was intended, for example on a mass basis for direct marketing.

However its efficacy has been limited, as the key test relies on the agency knowing the 'purpose of the register or the Act under which the register is kept'. It is surprising that many public registers are established under legislation which does not actually state what the purpose of the register is, and attempting to draw an alternative purpose for a specific register from the wider legislation can be either futile or defeating of the intention of the PPIP Act[195].

The temptation to use new technologies to improve public access to information held by government has impacted greatly on this area, and the legal protection of personal information on public registers has not kept up. For example agencies may wish to improve access to a public register, such that an interested member of the public need not have to visit their offices during working hours to inspect the register. Loading the entire register onto the internet therefore has a certain appeal to agencies.

However once on the internet, the risks to the personal information contained in public registers is great. In the name of accountability and transparency, personal information is published to the world at large, with no control over its secondary use.

[195] For example how should one succinctly describe the purpose of the Local Government Act, with its more than 700 provisions, in order to define the purpose of one of the registers created under that Act, such as the pecuniary interests register?

There used to be certain natural barriers that protected people's privacy by default – the barriers of time, distance and cost. In the days of paper files, the sheer effort of collecting and tracking detailed personal information about the average person was simply not worth the effort, unless one had a specific purpose in mind (such as the purpose for which the public register was established). Hence privacy was, for the most part, protected by default.

Now in this 'Google Age', unprecedented amounts of information are available to the public, anywhere across the globe, to search through almost instantly.

With the advent of the internet and its powerful search engines, the home address of a locum GP, or the name of the owner of a particular property, can be collected, used and disclosed by the person's neighbour, boss, bank manager or ex-boyfriend, or complete strangers with no connection at all to that person. This can be a risk not only in terms of privacy, but in terms of security of the person from theft, violence, or identity theft and fraud.

At the same time, the current public register provisions can be seen as too strict, as there is no exemption if the person consents to their information being used or published more broadly. This has led to some fairly ridiculous situations which defy common sense.

We therefore believe that the PPIP Act should prevent against public registers being published in such a way as to facilitate secondary uses of people's personal information without their consent.

It is suggested that the Act could instead deal with disclosures from 'public registers' under IPPs 11 and 12 with an additional exemption, such that disclosure from a public register is allowed if the disclosure is reasonably necessary for the agency to comply with the legislation establishing the public register and its uses. It is anticipated that the 'reasonably necessary' test would enable public inspection at office premises, but would generally prohibit widespread publication on the internet in the absence of specific legislative authority to publish the information at large.

It should be noted that the current tests for disclosure of personal information under the IPPs are not considered sufficient to ensure an adequate level of protection[196]. However if the IPPs and section 25 are amended as recommended above (see parts 3.1.1 and 3.1.2 of this submission), it may be possible to achieve adequate protection for the personal information held on public registers by simply deleting section 57, and relying on IPPs 11 and 12, read with the exemption under section 25 if necessary.

However any disclosure from a public register should still be subject to an overriding ability of the person to seek suppression of their information (see below).

Recommendation:

- That section 57 be deleted.
- That an additional exemption to IPPs 11 and 12 be created, allowing disclosure from a public register if the disclosure is reasonably necessary for the agency to comply with the legislation establishing the public register and its uses, *and* the information is not suppressed.

[196] See the criticism of section 18(1)(b) and recommendations for amendment to IPP 11, above at part 3.1.1 of this submission.

Suppression of information on a public register

Section 58 provides:

> (1) A person about whom personal information is contained (or proposed to be contained) in a public register may request the public sector agency responsible for keeping the register to have the information:
>
> (a) removed from, or not placed on, the register as publicly available, and
>
> (b) not disclosed to the public.
>
> (2) If the public sector agency is satisfied that the safety or well-being of any person would be affected by not suppressing the personal information as requested, the agency must suppress the information in accordance with the request unless the agency is of the opinion that the public interest in maintaining public access to the information outweighs any individual interest in suppressing the information.
>
> (3) Any information that is removed from, or not placed on, a public register under this section may be kept on the register for other purposes.

The current test for suppression in section 58(2) is incoherent, as it tries to address two types of harm that could be dealt with separately. If there is a serious risk of harm to an individual, an agency would face considerable difficulty applying the 'reasonable balance' test. Furthermore this test, by virtue of section 59 (below), overrides tests for the suppression of personal information from public registers which had their own legislative tests for suppression (such as the electoral roll and registers held by local councils).

We suggest that the test for suppression in section 58 ought to be a two tiered one, so that it allows people to easily opt out when there is no strong public interest in their information being made available, but which uses the a more serious 'risk' test to suppress information in any case.

Recommendation:

- That the test for suppression of personal information from a public register favour an 'opt out' approach where there is no public interest reason to the contrary, but which also protects those at more serious risk of harm.

Note:
An example of how this recommendation could be achieved follows:

(2) The public sector agency must suppress the personal information in accordance with a request made under s.58(1), unless

the agency is of the reasonable opinion that the public interest in maintaining public access to the information outweighs any individual interest in suppressing the information, and

the request is not one to which (2A) applies.

(2A) If the public sector agency is reasonably satisfied that the safety or well being of any person would be ***placed at risk*** by not suppressing the personal information as requested, the agency must suppress the information in accordance with the request.

(3) ...

(4) An agency need not comply with (2)-(2A) if the legislation establishing the public register has an alternative method for suppressing personal information from public inspection or disclosure.

Inter-relationship with other legislation

Section 59 provides:

> The provisions of this Part prevail to the extent of any inconsistency with the requirements of the law under which the public register concerned is established.

Section 59, combined with section 57, paradoxically imposes a more stringent test on disclosing personal information from public registers than the IPPs impose on any other source of personal information. There are no exemptions for consent to disclosure, nor can specific legislation override these provisions.

As a result, the public register provisions have been the subject of many exemptions granted by the Attorney General under privacy codes of practice and by way of regulations made under the Act. In recognition of the difficulties faced by agencies in the application of the public register provisions, the Privacy Commissioner has supported some of those exemptions.

Recommendation:

- That section 59 be deleted.

3.1.4 Special case: data-matching

As noted at the beginning of part 3.1 of this submission, we have reviewed the privacy standards set for state and local government under the Act, namely:

- the information protection principles in Part 2 of the Act, and
- the public register provisions in Part 6 of the Act.

Our review of the IPPs included identifying two additional privacy principles which we have recommended for inclusion – the use of unique identifiers and anonymity (see part 3.1.1 above).

However there is one further area of activity which does not fit neatly into either the information protection principles or the public register provisions of the Act : data-matching.

The IPPs governing collection, use and disclosure of personal information do not fully canvass the issues and privacy impacts raised by data-matching projects across or between agencies. Their application has led to ad-hoc requests to the Privacy Commissioner for exemptions by way of public interest directions or codes, when it would be preferable to set generic but binding guidelines. Such an approach would be similar to that in other

Australasian privacy laws[197]. For example guidelines and rules have been developed and incorporated into law as part of the New Zealand Privacy Act, which seek to identify those circumstances where information matching is most clearly justified in the public interest notwithstanding some detriment to individual privacy.

For example in September 2003 a request was made to the Privacy Commissioner for a public interest direction, to enable the Registry of Births, Deaths and Marriages to participate in a data-matching and data-cleansing exercise of unprecedented size with various Commonwealth agencies, coordinated by Centrelink. The exercise was to take place within a matter of weeks. The timeframe was such that Privacy NSW was unable to conduct any consultation or considered review of the likely privacy impacts or implications of the exercise.

Other recent examples of requests for large-scale data-matching include a proposal for the RTA to supply all drivers' odometer readings to the Office of Fair Trading (so that the Office of Fair Trading can find any tampering with odometers in motor vehicles), and for the Department of Lands to supply all property ownership information on all land owners in NSW to Centrelink (so that Centrelink can check social security recipients for any undeclared assets). Each of these proposals involves mass collections of information about people who are under no suspicion whatsoever, for purposes unrelated to the original purpose of collection, and in circumstances where people are compelled by law to provide their personal information to the government agency in the first place.

Recommendation:

- That a new provision be created to deal with data-matching, requiring compliance with guidelines to be issued by the Privacy Commissioner, and/or the approval of the Privacy Commissioner to the terms of the exercise, prior to commencement.

3.2 Enforcement of the privacy standards

This part of our submission reviews the mechanisms by which the privacy standards set out for state and local government by Parliament are or can be enforced. The mechanisms include:

- enforcement by and for individual complainants, and
- how systemic issues are or could be addressed.

This submission examines:

- whether the mechanisms are appropriate and effective, and
- whether the processes for all parties are clear and fair.

[197] See section 12 in the Australian Federal Privacy Act, and guidelines issued under the New Zealand Privacy Act. The Victorian Information Privacy Act uses IPP 7 to restrict data-matching in a defacto way.

Introduction to enforcement mechanisms

The PPIP Act aims to protect 'personal information'. Enforcement of the privacy standards set out in the Act for information privacy (the IPPs and the public register provisions) is primarily through administrative review. Individual applicants may seek internal review of conduct or a decision, with binding findings and enforceable remedies available on subsequent application to the Administrative Decisions Tribunal for a fresh review. The result is an adversarial / litigation model.

On the other hand, the PPIP Act also aims to protect 'the privacy of individuals generally'. This is primarily achieved by a complaints-handling and conciliation role for the Privacy Commissioner, not limited to information privacy matters subject to the privacy standards set out in the Act. This role – encompassing the resolution of complaints as varied as bodily privacy, territorial privacy and the privacy of communications – was inherited by the Privacy Commissioner upon abolition of the Privacy Committee, which existed from 1975 to 1999.

The Privacy Commissioner has some ability to address systemic issues by way of inquiries and investigations into 'privacy related matters', in which he or she may exercise Royal Commission powers, and by way of advice, assistance and education.

The role of enforcement mechanisms in achieving the objects of the Act

We will outline below some of the deficiencies in these two models (complaint conciliation, and administrative review) for enforcement of privacy standards.

Neither of these two models is particularly adept at bringing about systemic change in the way in which government agencies are expected to handle personal information in particular, or protect privacy in general. Yet the objects of the PPIP Act are to bring about just such a transformation.

However before considering reform or alternative models, it is worth pausing to consider who each model of enforcement serves. The five main stakeholder groups and their likely interests might be summarised as:

Individuals with privacy complaints

- want a fast / simple / cheap resolution of their complaint
- often only seeking acknowledgement of wrong-doing and an apology[198]
- may want their 'day in court' for a sense of closure
- may desire systemic change ('I don't want this to happen to anybody else')
- uninterested in statutory interpretation except as directly affects their complaint

[198] Interestingly almost no complainants or internal review applicants are seeking compensation. To date only two internal review matters have resulted in compensation, and no Tribunal matters have involved an order for compensation.

Individual agencies responding to privacy complaints

- want clarity in the law
- may want a fast / simple / cheap resolution of the complaint
- yet willing to litigate in order to resist complaints seen as unmeritorious
- may resist systemic change

Specialist privacy practitioners (advocates, academics, lawyers)

- interested in case law as a means of aiding interpretation of the Act[199]
- not directly interested in individual complaints or their resolution
- may want to bring about systemic change

Privacy NSW

- want to ensure the robustness of privacy laws
- interested in case law as a means of aiding interpretation of the Act
- want to bring about systemic change
- yet also supposed to conciliate cases wherever possible

The Government

- want a fast / simple / cheap way in which to resolve privacy complaints made against government, to maintain trust in government
- concerned about costs of litigating complaints
- not directly interested in individual complaints or their resolution

It should be acknowledged that these interests often sit in tension. For example, a case before the Tribunal may have some prospects of settlement through mediation if the complainant's case is strong and the facts are not in dispute. The respondent is likely to favour an out-of-court settlement, Privacy NSW and privacy advocates would be likely to prefer an open judgment, and the complainant must decide between the path of least resistance in settling, and the satisfaction but uncertainty of their 'day in court'. This illustrates the difficulty in using an adversarial model to enforce laws that by their very nature are aimed at systemic change.

The PPIP Act seems to be trying to have a bet each way: a specialist, free complaints conciliation service (Privacy NSW), and a mechanism by which complainants can obtain an enforceable remedy and/or large volumes of case law can be generated (external review by the Tribunal) while also acknowledging and trying to address the power imbalance faced by complainant litigants (independent role for the Privacy Commissioner in the Tribunal). Yet it is possible that in trying to please everybody, the processes in the PPIP Act serve nobody.

[199] See for example the editorial in the latest edition of the *Privacy Law and Policy Reporter* (Volume 10(10), 2004), in which the PPIP Act is praised for its ability to generate large volumes of cases before the ADT, while the Federal Privacy Act is criticised for the manner in which complaints are conciliated behind closed doors, with no case law from the Federal Court.

This submission does not offer any radical solutions to this dilemma, nor do we suggest whose interests ought be given precedence. Perhaps it is better to focus upon how (we trust) all parties see the ideal situation: no privacy complaints, because all members of the public share the same expectations of privacy and accept a sensible balance with other interests, the law reflects those shared public expectations perfectly, all agencies understand the law perfectly, and all agencies comply with the law perfectly. In that sense, the ultimate aim of Privacy NSW is to do itself out of a (complaints-handling) job.

However in our very imperfect reality, a mechanism by which to enforce the law and resolve complaints is needed. Nonetheless it is worth remembering the utopia just described, particularly when thinking about the mechanisms by which privacy can be protected by means other than complaints-handling, such as education, advice and assistance.

Indeed in the second reading speech on the then PPIP Bill, the then Attorney General, the Hon Jeff Shaw QC, noted that:

> "The Privacy Commissioner's complaints-handling role will have a conciliation and education focus"[200].

3.2.1 Complaints to the Privacy Commissioner

Explanation of the complaints model

Section 45(1) provides:

> A complaint may be made to (or by) the Privacy Commissioner about the alleged violation of, or interference with, the privacy of an individual.

'Privacy' is not defined. However it is clear from the context of section 45(2) that it is intended to be broader in scope than a breach of the IPPs by a public sector agency[201]. This is fairly unique amongst Privacy Commissioners; more commonly complaint-handling relates only to information privacy in terms of the privacy principles established by statute, and against respondents bound by those principles.

Sections 45 to 51 set out the Privacy Commissioner's complaint-handling powers, including a requirement under section 49 to 'endeavour to resolve the complaint by conciliation'. The Commissioner may make findings or recommendations in a report to the relevant parties under section 50. Earlier provisions such as section 38 deal with more general inquiry and investigation powers, including providing the Privacy Commissioner with the powers, authorities, protections and immunities of a Royal Commission. Under section 65 the Privacy Commissioner may make a special report to Parliament on 'any matter arising in connection with the discharge of his or her functions'.

[200] Corrected Copy NSW Legislative Council Hansard, Article No.44 of 17 September 1998, pages 7599-7602.
[201] Section 45(2) provides that the subject-matter of a complaint *may* relate to conduct to which the alternative process of administrative review applies.

The complaints model in practice

Who is the complainant?

Section 45(1) of the PPIP Act provides:

(1) A complaint may be made to (or by) the Privacy Commissioner about the alleged violation of, or interference with, the privacy of an individual.

Despite the language of 'the privacy of *an* individual', Privacy NSW has received legal advice to suggest that section 45(1) prevents the Privacy Commissioner from receiving complaints about the privacy of a person other than the complainant themselves[202]. This would suggest that 'whistleblower' type complaints could not be accepted. This creates a significant accountability gap in terms of the enforcement of privacy standards, particularly as the individuals whose privacy has been affected by conduct may be the last to know, and may find it very difficult to determine the source of an unauthorised collection, use or disclosure. The link between privacy breaches and corrupt conduct is clear[203], and it is submitted that the trigger mechanisms by which alleged corrupt conduct may be exposed to scrutiny, such as third party or anonymous whistleblower complaints, ought likewise be allowed in relation to privacy complaints.

It would also appear that interested party, representative or 'class action' type complaints cannot be accepted because of the wording of section 45(1). This has impacts in terms of the efficiency and effectiveness of complaints-handling, as well as the ability to deal with systemic problems in an appropriate way.

The success of the representative model of complaints-handling has been recently demonstrated in the Federal Privacy Commissioners jurisdiction, with numerous complaints about tenancy 'blacklists' being resolved through a representative action[204]. This allowed resources of both the Privacy Commissioner and the respondent organisations to be dedicated to a single investigative and conciliation process, instead of dealing with multiple individual claims. Furthermore remedies were able to address both the individual complainants and the 'class' of all other individuals affected or potentially affected by the practices at issue.

Should this recommendation be adopted, some means of managing subsequent claims by other aggrieved parties will be required.

However we believe there is nothing in the Act to deny the normal entitlement of any person who is aggrieved by a public sector agency to bring a complaint via an agent, whether the relationship is that of lawyer on behalf of client, parent on behalf of child, or another form of agency.

---

[202] For more on this point see the Privacy Commissioner's *Special Report to NSW Parliament under section 65 of the Privacy & Personal Information Protection Act 1998, Complaint by Student A and his father against Hon John Aquilina MP, Mr Walt Secord, Mr Patrick Low*, 7 May 2002, available on the Privacy NSW website.
[203] See the ICAC's 1992 report, *Report into the Unauthorised Release of Government Information*.
[204] See http://privacy.gov.au/act/casenotes/index.html#comdet

Recommendation:

- That section 45(1) be amended to allow both whistleblower complaints and representative complaints to be made to the Privacy Commissioner.

Note:
An example of how this recommendation could be achieved follows:

A complaint may be made **by any person (the complainant)** to the Privacy Commissioner about the alleged violation of, or interference with, the privacy of **the complainant or the privacy of any other individual or group of individuals**.

- Alternatively, that Part 4 Division 3 of the PPIP Act be amended to clarify that the Privacy Commissioner's powers under Part 4 Division 2 of the PPIP Act do apply to complaints which do not meet the test in section 45(1), namely that the person whose privacy has allegedly been violated or interfered with is the complainant.

What is a breach of privacy?

The ability to make findings as to a 'violation of, or interference with' the complainant's privacy necessitates some process of dispassionate analysis of conduct as compared against coherent standards. This is not a simple task when the complaint subject-matter is 'privacy', which is notoriously difficult a concept to define[205]. Information privacy is relatively clear, but other forms of privacy (such as bodily, territorial, physical or communications privacy) are more complex and contentious.

In the absence of any guidance from the PPIP Act, the Privacy Commissioner has determined that Privacy NSW will use 'relevant standards' to determine whether or not a 'violation or interference with' a person's privacy has occurred. This process is set out in our Complaints Protocol, available on our website.

With respect to a complaint about information privacy against a public sector agency respondent, the Commissioner uses the IPPs and the public register provisions as the 'relevant standards'.

With respect to a complaint about information privacy against any other respondent, or other types of privacy concerns (physical, bodily, territorial, and so on), the Privacy Commissioner uses different standards. Depending on the nature of the complaint, those standards might be general fair information processing standards[206], specific laws or widely accepted

[205] See for example discussions in the Australian Law Reform Commission, *Privacy*, Report No 22, 1983, and the Victorian Law Reform Commission Occasional Paper, *Defining Privacy*, 2002. Many definitions are quite circular. For example a landmark case in Queensland recently found that there existed a common law tort of invasion of privacy. The necessary elements to found a cause of action were described as a willed action by the defendant which "intrudes upon the privacy or seclusion of the plaintiff" in a manner that would be considered highly offensive to a reasonable person of ordinary sensibilities, and which causes the plaintiff harm; see *Grosse v Purvis* [2003] QDC 151, at para 444.
[206] The Privacy Commissioner has formally adopted the Data Protection Principles (DPPs) for this purpose. The DPPs were first established by the former Privacy Committee in 1991.

guidelines or policies governing the specific conduct[207], or broader tests that go more to the nature of the harm suffered to determine whether or not there was a violation of or interference with privacy.

For example the Prosser tests, developed by American academic William Prosser, treat the following as breaches of privacy:

- the intrusion upon a person's seclusion or solitude or personal affairs
- public disclosure about embarrassing facts about a person
- publicity which places the person in a false light in the public eye
- appropriation of a person's name or likeness

How should complaints proceed?

It appears that while 'complaints' lodged under Division 3 may also be the subject of 'investigation' or 'inquiry' under Division 2[208], a 'privacy-related matter' being investigated under Division 2 cannot be 'conciliated' under Division 3 unless there is also a complaint lodged under Division 3.

Thus the requirement to resolve a complaint by conciliation (section 49) sits uncomfortably with the ability to conduct an investigation (section 38), and make findings and recommendations by way of a formal report (section 50).

As a matter of practice, Privacy NSW almost never conducts traditional face-to-face conciliation proceedings. This decision has been taken purely because of resourcing constraints. Therefore most investigation and conciliation occurs by correspondence, and the 'conciliation' aspect mostly relates to negotiations about recommendations once the investigation phase is complete.

In practice the process followed is usually:

- determine whether the allegation can be accepted as a 'complaint' under section 45
- conduct preliminary assessment under section 46
- conduct investigation under section 39, including requesting information under section 37
- come to findings as to the conduct that occurred
- analyse the conduct against the relevant standards
- come to findings as to whether or not the complainant's privacy was 'violated or interfered with'
- issue a report to both parties under section 50, setting out findings and recommendations
- follow up with respondent as to whether or not recommendations are to be followed

[207] For example complaints about the checking of a handbag at a supermarket are compared against the adopted industry bag-checking code; complaints about overt video surveillance are assessed with reference to the non-binding code issued by the then Department of Industrial Relations and the then Privacy Committee.
[208] See section 38(1).

At any point in this process, if the respondent makes concessions (such as recognising that the conduct caused some harm to the complainant and thus offering an apology or other remedy, or accepting that the conduct raises a systemic issue and undertaking to change practices accordingly), the complaint is usually considered resolved, and the matter is finalised at that point.

Furthermore while section 50 mentions 'findings', it is not clear what we can make a 'finding' about. The practice to date is that the Commissioner makes a finding as to whether or not a 'violation or interference with' a person's privacy has occurred, as determined against relevant standards (see above).

Between sections 45(2) and 50 it is implicit that the Privacy Commissioner can make a finding about whether or not an IPP has been breached by a public sector agency, thus creating a situation in which the Privacy Commissioner holds a quasi-judicial role (albeit an unenforceable one), parallel to the Tribunal. However it would be beneficial to have a provision which clearly states that the Privacy Commissioner can reach findings as to breaches of IPPs or other applicable standards, in determining whether or not there has been a 'violation of, or interference with' a person's privacy.

Some further clarity regarding the Privacy Commissioner's power to decline complaints may also be of benefit. Specific power in relation to certain grounds exists in section 46 to decide not to 'deal with' a complaint, and the power to 'decline' a complaint is mentioned in section 48. However it is only implicit from the terms of section 45 that complaints not meeting certain criteria may also be declined. These include that no allegation in relation to privacy is raised, or that the complaint is not lodged within time.

Nevertheless if a complaint is declined because it does not meet section 45(1) (for example because the complainant is alleging a violation of someone else's privacy rather than their own), it would appear that it may still be dealt with by 'an inquiry or investigation into any general issues or matters raised in connection with the complaint'[209]. This would allow the Privacy Commissioner to exercise his or her Royal Commission powers and the power to require any person or public sector agency to answer the Commissioner's request for information, documents, etc, under Part 4 Division 2 of the PPIP Act, even if the complaint does not satisfy the test in section 45(1).

Unfortunately section 51 does not include, as a matter which may still be investigated or the subject of an inquiry under Part 4 Division 2 of the PPIP Act, a complaint that has been withdrawn by the complainant. This is of concern if, for example, the Privacy Commissioner suspects the complaint was withdrawn under undue pressure from the respondent. Furthermore, if a complaint raises systemic issues potentially affecting a class of individuals (rather than just the complainant), the withdrawal of the complaint prevents any resolution of those systemic issues.

A good safeguard against corrupt conduct is to allow investigation of a matter even in circumstances where:

- the complaint has been withdrawn
- the complainant is anonymous and/or uncontactable

[209] See section 51.

Recommendation:

- That the process to be followed in investigating and/or conciliating complaints be set out in the Act in a more precise manner.
- That section 50 be amended to clarify whether a report can be issued as part of conciliation and/or even if the complaint has been conciliated.
- That section 50 be amended to clarify about what the Privacy Commissioner can make findings, and how such findings are to be reached.
- That the inter-relationship between the Privacy Commissioner's powers of investigation and inquiry under Part 4 Division 2, and the handling of complaints under Part 4 Division 3, be clarified.
- That sections 45, 46 and 48 be amended to clarify the grounds on which the Privacy Commissioner may decline to deal with a complaint.
- That section 51 be amended to allow investigation of a matter even in circumstances where the complaint has been withdrawn, or the complainant is anonymous and/or uncontactable.

What if there is no complaint to start with?

Any 'privacy related matters' may already be the subject of an 'investigation' or 'inquiry' under Part 4 Division 2 of the PPIP Act, whether or not there has been a formal complaint lodged under section 45[210]. However it would appear that investigations or inquiries not launched as a result of a 'complaint' lodged under section 45 will preclude 'conciliation' under section 49, and/or the issuing of a report under section 50. Conciliation of or reporting on a matter may be an appropriate way to proceed where the Privacy Commissioner believes he or she may negotiate an outcome on behalf of a class of unidentified affected individuals. It is suggested that an 'own motion' complaint power would be appropriate in these circumstances.

Such an 'own motion' complaint power would be appropriate in cases where the Privacy Commissioner becomes aware (such as from a media report, an anonymous 'tip-off' or another source) that certain conduct may be in breach of the IPPs (or the HPPs in the HRIP Act, once that Act commences). It is submitted that this 'own motion' power would be suitably limited to instances where the initiating material suggests a serious infringement and/or a systemic issue, rather than the minor, one-off, human error type of conduct. It is also suggested that this power be limited to suspected breaches of the legislated information privacy standards in the PPIP Act and HRIP Act (once that Act commences), rather than the wider category of all 'privacy' matters.

It is therefore submitted that provisions allowing investigation and conciliation of these cases should be included in the Act.

[210] See section 36(2)(l).

Recommendation:

- That section 51 be amended to allow a clear 'own motion' complaint power, in cases of an alleged breach of one or more IPPs or HPPs which have had or would have an apparent systemic and/or serious impact.

Overlap with administrative review mechanism

The PPIP Act quite deliberately allows the Privacy Commissioner to accept, as complaints under section 45, matters which could also be the subject of the administrative review mechanism provided under Part 5 of the Act[211].

In the second reading speech on the then PPIP Bill, the then Attorney General, the Hon Jeff Shaw QC, explained this provision thus:

> "… in cases in which the complaint relates to a breach of a data (sic) protection principle, relevant code, or breaches of the public register provisions, the complainant ***can choose*** to have the commissioner conciliate the matter ***or alternatively*** to seek an internal review by the agency with a right of review by the Administrative Decisions Tribunal" (emphasis added)[212].

The PPIP Act does not actually require complainants to make a binding choice - in theory complainants could try both avenues. (They must be advised of the existence of both avenues by the Privacy Commissioner[213].) However as a matter of practice, the inflexible six month time limit imposed on lodging an internal review request is usually such that the complainant has little ability to gain the benefit of an investigation by the Privacy Commissioner before seeking an internal review.

This has significant disadvantages for a complainant whose complaint might require significant forensic investigation to determine whether or how the alleged conduct occurred, before proceeding to the administrative review which could deliver an enforceable remedy. On the other hand, we at Privacy NSW have recognised that there is a certain degree of unfairness to respondent agencies if a complainant is allowed 'two bites at the cherry'. Furthermore it is difficult to resolve the conflict posed between the Privacy Commissioner's role as investigator and conciliator and the Privacy Commissioner's role in oversighting and participating in the alternative administrative review mechanism.

In practice therefore, we do ask complainants to make a choice up-front about which method they prefer, and we explain the remedies available under each method and what our role will be.

[211] See section 45(2).
[212] Corrected Copy NSW Legislative Council Hansard, Article No.44 of 17 September 1998, pages 7599-7602.
[213] See section 46(2).

Difficulties for complainants

For those complainants complaining about a breach of information privacy by a public sector agency, it is our experience that complainants find the choice between the two avenues (described above) quite confusing. Even after careful explanation and the provision of literature to explain the choice they must make, many complainants maintain an expectation that the Privacy Commissioner can make binding determinations, award compensation, and so on. Some attempt to take both options, leading to confusion for respondent agencies as well. The complexity and counter-intuitive nature of the legislative arrangements, language and cultural barriers all conspire to make the situation anything but straightforward.

Those complainants who do choose investigation and conciliation by the Privacy Commissioner instead of internal review are ultimately penalised because of the inability to obtain an enforceable remedy even if a clear breach is found. More discussion on this point, and a proposed resolution, is found below at part 3.2.4 of this submission.

A different problem is the potential for victimisation. Unlike similar legislation[214], the PPIP Act does not have a provision which protects a complainant from victimisation because he or she has made or may make a complaint. It is our experience from the handling of complaints under the PPIP Act that situations have arisen where complainants are unwilling to proceed because may lose a contract or work, or fear they will lose services from a government agency, and so on.

However a related problem – the lack of protection from liability for anything done in good faith when making a complaint to or providing information to the Privacy Commissioner – will be resolved when the HRIP Act commences[215].

Recommendation:

- That the PPIP Act be amended to provide a 'protected disclosure' level of protection against victimisation for complainants.

3.2.2 Internal review

Explanation of the internal review model

An internal review is an internal investigation that a public sector agency is required to conduct upon receiving a valid application. Individuals (applicants) may seek an internal review by an agency where they believe there has been a contravention of the relevant privacy standards set for the agency under the Act.

[214] See section 50 of the Anti-Discrimination Act 1977 (NSW).
[215] When the HRIP Act commences, a cognate amendment to the PPIP Act will insert a new section 66A, providing protection from civil liability for complainants, witnesses and respondents when providing information to the Privacy Commissioner, and protection from defamation liability for agencies when providing access to personal information under IPP 7.

The Act establishes for the Privacy Commissioner an oversight role in the conduct of internal reviews. Privacy NSW must be notified by agencies of the receipt of internal review applications, and the Privacy Commissioner may make submissions to agencies on the matters being reviewed or the process of the review. However our submissions are not binding.

If the applicant is not satisfied with the outcome of the internal review, or the agency takes longer than 60 days to complete the review, the applicant can apply to the Administrative Decisions Tribunal for a further review; for more about this process see part 3.2.3, below.

The internal review model in practice

Who can seek a review?

Section 53(1) provides:

> A person (the applicant) who is aggrieved by the conduct of a public sector agency is … entitled to a review of that conduct.

The Act does not define a 'person aggrieved'. However it is our view that a 'person aggrieved' is a wider concept than 'a person whose personal information is at issue'. In particular, the Act protects the personal information of a person who is dead less than 30 years[216]. Logically this suggests that Parliament intended to protect the interests of survivors, and thus a 'person aggrieved' need not be subject of the personal information.

There has been no case that squarely faces the issue of whether a representative complaint can be made by an individual who can claim such a special interest. In one case the Tribunal held that a review of conduct of an agency did not include a review of possible future conduct[217]. This could be seen to restrict standing to individuals who were directly affected by a particular action. The Tribunal has also found that an applicant was an 'aggrieved' person because he had been specifically and adversely financially affected by the alleged breach of the Act, which involved personal information about his adult son[218].

However a broader question, yet to be the subject of argument in the Tribunal, is whether a person may be 'aggrieved' by conduct which does not involve the personal information of themselves or their immediate family.

Privacy NSW has taken the view based on case law dealing with legal standing that to be a person aggrieved an applicant must demonstrate a special interest as an individual or member of a class of individuals that is more than a merely emotional or intellectual interest[219]. In the context of some of the IPPs, this test arguably applies to any NSW resident whose personal information is held by a subject agency and who has concerns about how the agency deals with it.

---

[216] See section 4(3)(a).
[217] *Wy Kanak v Director General, Department of Local Government* [2002] NSWADT 208
[218] *KO & Anor v Commissioner of Police, NSW Police* [2004] NSWADT 3 para 18.
[219] See *Australian Conservation Foundation Inc. v. The Commonwealth* (1980) 146 CLR 493, *Onus v. Alcoa of Australia Ltd* (1981) 149 CLR 27.

In the absence of any other enforceable remedies it can be argued that the PPIP Act should support representative requests for internal review as, absent a case for damages, there are few incentives for individuals to seek satisfactory remedies for systemic failures to comply with the Act. Given the beneficial intent of the legislation, and the principles-based approach to improving fair information practices in the public sector, it is submitted that a liberal interpretation should be taken of this provision.

It is nonetheless suggested that section 53(1) be amended to clearly support such claims.

Recommendation:

- ❖ That section 53(1) be amended to define 'aggrieved person' as any NSW resident whose personal information is (or might be) held by a subject agency and who has concerns about how the agency deals with it.

What is reviewable?

Applicants may seek an internal review by an agency where they believe there has been:

- a contravention of an IPP,
- a contravention of a privacy code of practice made under the Act, or
- a disclosure of personal information kept in a public register[220].

It is submitted that this provision is deficient in several respects.

First, the section is confusing in its mention of codes of practice, which are documents which serve only to modify the application of the IPPs or the public register provisions, rather than 'codify' an entirely new set of standards. Codes do not of themselves 'cover the field', and they are inherently permissive, rather than restrictive, documents. Codes are thus on a par with public interest directions, regulations, and exemptions to the IPPs found in the Act itself. It is suggested that codes only need mention in the sense of providing a 'defence' to an alleged breach of the IPPs or the public register provisions.

Second, the 'disclosure' of 'personal information kept in a public register' should refer to unauthorised disclosure, or disclosure that contravenes the public register provisions, rather than all disclosures per se. However the failure to suppress personal information on a public register (when required to suppress under section 58) should logically be included as conduct for which review could be sought.

It is submitted that an application for internal review should simply allege:

- non-compliance with an IPP, or
- non-compliance with the public register provisions.

[220] See section 52(1).

However it should also be clarified that in answering the allegation, whether in conducting the internal review or when subject to external review by the Tribunal, the agency in question can rely on an exemption or modification (whether in the Act, regulations, a code or a public interest direction) to the particular provision, as applicable.

Recommendation:

- That section 52 be simplified in describing the conduct to which Part 5 of the Act applies:
  non-compliance with an IPP, or
  non-compliance with the public register provisions.
- That the Act more clearly state that in answering the allegation, a respondent agency can rely on an exemption or modification (whether in the Act, regulations, a code or a public interest direction) to the particular provision, as applicable.

There is a further need for clarification of the scope of the word 'conduct' in sections 52 and 53. Although the conduct at issue must be in the past or present[221], the applicant should not need to prove actual past or present misuse of their personal information in order to prove a contravention of an IPP. An applicant, as a member of a class of people whose personal information could be adversely affected in the future, could be seeking review of conduct allegedly in contravention of IPP 5. IPP 5 requires positive steps to secure personal information against loss, unauthorised access, use, modification, disclosure, or other misuse.

In this sense the 'conduct' may be a specific event (such as conduct or a decision), an omission (the absence of conduct or a decision), or a general policy, practice, procedure or state of affairs (such as a practice of leaving sensitive personal information in public space), which does not comply with an IPP. This is a much broader scope of activity than 'decisions', which are more amenable to administrative review (such as a decision to refuse the release of a document under the FOI Act).

Recommendation:

- That the scope of 'conduct' which may be reviewed under Part 5 be defined for greater clarity.

There is also what appears to be a typographical error in section 53(1), which provides:

> A person (the applicant) who is aggrieved by the conduct of a public sector agency is, ***subject to section 51(1),*** entitled to a review of that conduct (emphasis added).

[221] The Tribunal found in Wy Kanak v Department of Local Government [2002] NSWADT 208 para 17 that future or possible conduct could not be the subject of a review.

There is no section 51(1), and section 51 is in a different division of the Act entirely. It would appear the reference should instead by to section 52(1), which sets out the conduct which may be the subject of an application for internal review.

Recommendation:

- That section 53(1) be amended to refer back to section 52(1) instead of 51(1).

How must a request be framed?

Sections 53 and 54 define the scope of an application for internal review - it must be in writing and relate to conduct or alleged conduct that breaches the Act. However the Act does not require that the applicant specify that the application is one for internal review under the PPIP Act, or which information protection principles, code provisions or Part 6 provisions that the conduct of the agency has breached.

This was an issue in the very first matter decided in the Tribunal, which found it is not essential that there be express reference in correspondence with agencies to the statute under which the application is made, especially where the context suggests that a statutory right is being invoked. However where the applicant is represented by an informed agent, such as a union or solicitor,

> "it is reasonable for an agency ordinarily to expect to find direct reference to any statutory right that is being invoked"[222].

This can make it difficult for respondent agencies to recognise that they have an application for internal review, thus increasing the likelihood that the application will be ignored, or not dealt with in accordance with the requirements of Part 5. This can disadvantage both complainants (who may not be properly informed of their right to seek further review by the Tribunal) and respondents (who may find themselves in the Tribunal after 60 days without understanding why).

On the other hand, we are concerned that individuals with limited knowledge of the law could be disadvantaged by overly rigorous requirements for a particular form of words, or to complete a particular prescribed form. A complaint about conduct which is alleged to have breached the person's privacy is a more reactive position than, say, a proactive request to access information under the FOI Act. For these reasons, we would urge caution before changing the current law in this respect.

As a practical measure we have developed a (non-compulsory) privacy complaint / internal review application form. We have encouraged applicants to use the form to make their intentions clear to the respondent agency, but this only works in relation to complainants who approach Privacy NSW first. We have also encouraged agencies to make the form available to people seeking to lodge complaints with their agency, but the requisite level of staff

[222] *Y v Director General, Department of Education & Training* [2001] para 16

knowledge of these processes can be difficult to achieve for large, dispersed agencies such as those in the human services areas, which attract the highest number of applications[223].

Difficulties with the review process for agencies

As just mentioned, the co-ordination effort required of large, dispersed organisations can pose difficulties for the proper functioning of internal reviews. Often complainants try to resolve their problems locally in such agencies (such as directly with the school principal, with the hospital executive staff, or with a local police command), but the local recipients do not recognise that the 'complaint' should in fact be treated as an application for internal review, and treated in a particular way.

As one way of dealing with this common scenario, some agencies have adopted a practice of requiring local offices to forward anything that looks like a privacy complaint to the centrally-based privacy contact officer (PCO) for handling. The PCO manages all co-ordination and liaison with the Privacy Commissioner, but may delegate the actual investigation task out to the local area again.

We have found this to be a reasonably successful model. However its wider adoption requires a more formally recognised and public role for the PCO in each agency.

Recommendation:

- That each public sector agency be required to nominate one officer as its Privacy Contact Officer (PCO), with the PCO's contact details made publicly available and kept up-to-date with the Privacy Commissioner.
- That the role of PCO include the co-ordination of management of internal reviews within the agency, including primary liaison point with the Privacy Commissioner.

By contrast small agencies often find it difficult to comply with the requirement of section 53(4), that

> the application must be dealt with by an individual within the public sector agency …
>
> (a) was not substantially involved in any matter relating to the conduct the subject of the application, and
>
> (b) who is an employee or officer of an agency, and
>
> (c) who is otherwise suitably qualified to deal with the matters raised by the application.

[223] In 2002-03, 44% of all internal reviews lodged under the PPIP Act were against State government human services agencies. The next largest sector – transport (primarily the RTA) – faces a similar organisational structure.

Small agencies, such as local councils and quasi-government boards or committees, often find it difficult to find a suitably qualified employee who is also independent of the conduct or decision under review. Furthermore even large agencies can find this requirement difficult if the conduct or decision at issue implicates the CEO, other senior managers, or all persons senior enough to be considered 'suitably qualified'[224].

While the Act provides one possible solution – having the Privacy Commissioner conduct the review[225] - in practice we found the conflict of interest issues arising too great to accept any such requests. (The Privacy Commissioner is supposed to oversight the conduct of internal reviews, and then also exercise standing in the Tribunal if the matter is subject to further review.) Indeed we suggest that this provision be deleted.

It is submitted that the conduct of an internal review could be out-sourced to an appropriate organisation or individual, such as an auditor, consulting firm, or legal firm, capable of conducting the necessary forensic investigation and then analysing the conduct as against the relevant privacy standards.

Recommendation:

- That section 53 be amended to allow the conduct of an internal review to be contracted out to an appropriate organisation or individual, such as an auditor, consulting firm, or legal firm.
- That section 53(3)-(5) be deleted.

A further difficulty encountered by agencies when conducting an internal review is the absence of any powers or protection for the person conducting the review, or protection for witnesses. The reviewing officer cannot compel witnesses to appear or give sworn evidence, and the absence of protection against defamation or other liability for witnesses can make some witnesses even less likely to co-operate with the process[226]. This becomes more acute when the witnesses are not employees of the agency. However this problem may be partly resolved if formal recognition is given in the Act to the role of the PCO – see the recommendation above.

The relative roles of the PCO and the CEO could also be clarified. It is submitted that the person conducting the review should be responsible for making findings and recommending a course of action for the agency to take as a result. There should then be a requirement upon the agency CEO to receive the report and determine whether or not to act upon the recommendations – but no ability to overturn the findings of the PCO.

[224] A case study in our 2002-03 Annual Report highlighted the problems faced by one council when an employee was required to review the conduct of their superiors – in that case a selection panel comprising the Mayor, other councillors, senior staff and members of the public – 'if they expect to continue working in an organisation'; see pages 33-35.
[225] See section 54(3).
[226] For an example see the case study in our 2002-03 Annual Report, at page 35.

Like the new section 66A will provide for complainants, witnesses and respondents when providing information to the Privacy Commissioner, protection from civil liability and protection from defamation liability should be provided for applicants, witnesses and respondent agencies when providing information in good faith to the person conducting an internal review. The officer conducting the internal review should likewise be protected.

Recommendation:

- That it be further reviewed whether a PCO (or their delegate), when conducting an internal review, should have the power to compel witnesses to appear and give evidence.
- That the Act be amended to provide protection from liability for applicants, witnesses and respondent agencies when providing information in good faith to the person conducting an internal review.
- That the Act be amended to provide protection from liability for the person conducting an internal review when conducting the internal review in good faith.

Difficulties with the review process for Privacy NSW

It is submitted that the internal review process as set out in the Act could be greatly improved, to the benefit of both applicants and respondent agencies.

Much of Privacy NSW's role in oversighting internal reviews has been to guide agencies in their handling of the internal review. Our input tends to avoid any second guessing of the agency's investigation and findings in terms of the facts or evidence concerning whether the alleged conduct occurred. However we have made submissions to ensure the correct procedure is followed (such as ensuring the applicant is notified of their right to have the matter further reviewed by the Tribunal), and/or to promote best practice (where the Act is silent)[227].

The mention of 'best practice' here is important. When you see the number of applications filed in the Tribunal that are subsequently withdrawn or settled during or after initial planning meetings[228], it suggests that many complainants are simply seeking more information or greater clarity about the manner in which their personal information was handled, and whether or not it was lawfully authorised. It is our view that a 'best practice' internal review report will clearly explain what conduct occurred, outline the IPPs that apply to the conduct, and then compare the conduct as against those IPPs.

Thus in order to make compliance with the procedural aspects of Part 5 of the Act easier for agencies, and to promote best practice in order to facilitate a speedier resolution of matters, we developed a checklist for agencies to follow. Anecdotal evidence suggests that there has been an improvement in the quality of internal review processes since launching the checklist in April 2003. This can be tested once a comparison with 2003-04 results is available.

[227] For further details and analysis of this role see our 2002-03 Annual Report, at pages 29-30.
[228] Tribunal President O'Connor DCJ recently suggested to the author that the figure was around 60%, which rings true from our very preliminary assessment.

Thus while initially we saw many poor quality reviews conducted, in general agencies have risen to the challenge. In the last year or so, most internal review reports seen by Privacy NSW are considered and well-argued responses to the application.

Nonetheless the entire process could be further improved through legislative clarity and guidance. For example the precise role of the Privacy Commissioner in oversighting internal reviews is unclear from the Act.

We don't make submissions on the facts, the evidence, the process by which evidence was collected, or on what an appropriate remedy of other course of action might be. However where we do make submissions - as noted above we have approached our role as being one of providing guidance on process and, where necessary, statutory interpretation – those submissions may be disregarded by the agency.

Nonetheless the Act provides that the Privacy Commissioner must be notified of the findings of the review and of the action proposed to be taken. Why is this necessary, if the only clear role for the Privacy Commissioner is to make submissions before the review is concluded?[229]

There is no power for the Privacy Commissioner to overturn or review the results of an internal review. Nor does it appear that the Privacy Commissioner has any ability to intervene if the correct procedure is not being followed. Indeed there is no remedy available to an applicant if critical aspects of the internal review procedure are not being met, such as the independence of the reviewing officer, the requirement to complete the review as soon as practicable, or the requirement to notify the applicant of their right to approach the Tribunal.

This may be because every internal review applicant can indeed approach the Tribunal, and because their primary concern is to have reviewed the conduct at issue, rather than the conduct of the internal review. In terms of agencies following poor process, any 'repeat offenders' could be the subject of an adverse mention in Privacy NSW's annual report, and perhaps this is all that Parliament intended. Nonetheless it would be beneficial to more clearly set out the role of the Privacy Commissioner in terms of the oversighting of internal reviews.

Recommendation:

- That the role of the Privacy Commissioner in oversighting internal reviews be clarified.

Difficulties with the review process for applicants

The most immediate difficulty facing many applicants is the inflexibility of the time limits for applying for internal review. Section 53 provides:

> 53(3) An application for such a review must:
> ...
> (d) be lodged at an office of the public sector agency within 6 months (or such later date as the agency may allow) from the time the applicant first became aware of the conduct the subject of the application, and ...

[229] See section 53(5)(b) and section 54(2).

Agencies have an absolute, non-reviewable discretion as to whether or not to accept applications later than 6 months[230]. As noted above, in large and dispersed agencies, applicants may seek to resolve their complaints locally at first (such as directly with the school principal, with the hospital executive staff, or with a local police command), but the local recipients do not recognise that the 'complaint' should in fact be treated as an application for internal review, and treated in a particular way. By the time the matter is escalated to 'head office' and the complainant is advised (by either head office or Privacy NSW) to lodge a request for an internal review, the 6 month time limit has passed.

We suggest an extended and more flexible time period should be allowed for applicants to lodge their internal review request. One suggestion would be to follow the model recommended by the NSW Law Reform Commission for anti-discrimination complaints: a standard one year in which to lodge without question, a further 2 years if the applicant is found to have a good reason for the delay (a reviewable decision), and lodgement after 3 years only allowed in exceptional circumstances, with the Tribunal's agreement.

Another common difficulty for applicants is the failure of internal review, in many cases, to provide the independent investigation of the facts that they are seeking, so as to receive an explanation as to how or why something happened. Applicants often express to Privacy NSW their lack of faith in the notion of an internal review, seeing it as an opportunity for an agency to conduct a 'whitewash'. While of course ultimately the applicant may seek a further review in the Tribunal, the Tribunal is also not designed as the place in which 'the facts will come out', since the Tribunal does not have an investigatory function.

Thus applicants face a choice between forensic investigation (by the Privacy Commissioner) or an enforceable remedy (by the Tribunal). Again because of the time limitations on lodging an internal review, applicants cannot draw on the benefit of an independent investigation of the facts or application of the law to those facts by pursuing a complaint with the Privacy Commissioner before then deciding whether or not to seek an internal review.

A different problem is the potential for victimisation. Unlike similar legislation[231], the PPIP Act does not have a provision which protects a complainant from victimisation because he or she has sought internal or external review under the PPIP Act. It is our experience that situations have arisen where complainants are unwilling to proceed because may lose a contract or work, or fear they will lose services from a government agency, and so on.

As a result applicants who have the least trust in an agency, or who have the most to lose or fear, tend not to utilise the internal review option, preferring instead a Privacy Commissioner investigation. The most common types of matters which proceed in this way seem to be those in which the applicant is an employee of the agency, who fears repercussions if they seek an internal review. This is a disturbing trend, which should likely be addressed through protection from retribution for applicants, such that an internal review application is treated as a 'protected disclosure'.

Furthermore applicants often have little understanding of the complexities of case law, or the ability to challenge any statutory interpretation offered by the respondent agency. As noted above, the role of the Privacy Commissioner in second guessing the respondent's statutory interpretation is quite unclear. It is therefore up to the applicant themselves to challenge the

[230] See Y v DET [2001] NSWADT 149, para 73.
[231] See section 50 of the Anti-Discrimination Act 1977 (NSW).

respondent's legal reasoning in the Administrative Decisions Tribunal – an option that few applicants have the time or resources to pursue.

Although less common since we produced the internal review checklist for agencies mentioned above, we did initially find many agencies not complying with the requirement in section 53(8) to notify applicants of their right to approach the Administrative Decisions Tribunal for further review. Those which did so often did not mention time limits or contact details for the Tribunal, and in some cases provided misinformation (such as the name of a different tribunal altogether).

Recommendation:

- That the time limits in which to lodge an internal review application be amended to be longer and more flexible.

- That the lodging of an internal review application be protected as a 'protected disclosure', so the applicant will not face retribution for their request for an internal review.

- That the procedures for internal review be amended to require public sector agencies to notify applicants immediately upon receipt of their application:
  that they have received their application and will be treating it as an internal review under the PPIP Act;
  the contact details for the officer conducting the review;
  that the applicant may make submissions to the officer conducting the review;
  that the applicant can approach the Administrative Decisions Tribunal for further review after X date (if the review is not finalised by then); and
  the contact details for the Administrative Decisions Tribunal.

- That the procedures for internal review be amended to require public sector agencies to notify applicants immediately upon finalisation of their application:
  that the applicant can approach the Administrative Decisions Tribunal for further review before X date; and
  the contact details for the Administrative Decisions Tribunal.

3.2.3 External review by the ADT

Explanation of the external review model

Following an internal review, an applicant may seek a further review of the agency's conduct by the Administrative Decisions Tribunal under section 55 of the PPIP Act. The purpose of this review is not to review the manner in which the agency conducted its internal review, but to go back and review the original conduct or decision complained about.

The Tribunal has a range of powers available to it, which may be utilised regardless of the outcome of the review. However in practice those powers are generally only used to provide a remedy, once the review has determined that a breach of an IPP or the public register provisions has occurred.

Under section 55(7), the Privacy Commissioner has the right to appear and be heard in any proceedings brought under the PPIP Act. This includes matters which proceed to the Appeal Panel of the Tribunal[232].

The external review model in practice

The inherent imbalance

It is our observation that this model, in very general terms, results in agencies commonly settling those cases with the greatest chance of success, and defending those claims seen as unmeritorious. Defended claims involve agencies seeking to rely on exemptions in the Tribunal, even if the agency's officer, whose conduct or decision is under review, did not consciously rely on the claimed exemption at the time.

Applicants are often unrepresented in the Tribunal, while respondent agencies are well represented, and better able to make arguments about statutory interpretation. Of the 23 matters proceeding to judgment to date in the Tribunal or Appeal Panel, only five have not involved argument about the statutory interpretation of the exemptions to the definition of 'personal information'[233] or exemptions to the IPPs.

The result of this adversarial and typically one-sided litigation model is that it is in the interests of respondent agencies to argue before the Tribunal for the broadest possible interpretations of exemption provisions, against individual applicants who are often ill-equipped to argue the contrary position, and often have little interest in the implications of statutory interpretation beyond the impact on their own matter.

It would appear that Parliament sought to address this imbalance by creating a role for the Privacy Commissioner in Tribunal proceedings. The Privacy Commissioner does not support, advocate for or represent either of the parties to the dispute. We approach our role in the Tribunal as pursuing an interpretation of the PPIP Act that promotes the objects of the Act, namely to protect the privacy of individuals.

Unclear timeframes

The Tribunal has found that there are no time limits for lodging privacy applications with the Tribunal[234]. This is because not only does the PPIP Act itself not set any time limits, but section 52(4) of the PPIP Act excises section 53 of the Administrative Decisions Tribunal Act 1997, which imposes time limits under that Act.

The absence of any time limits is an unreasonable impost on public sector agencies, and Privacy NSW has previously stated its support for an amendment to set time limits in this regard. The President of the Tribunal, Judge Kevin O'Connor, has suggested to the author a period of 60 days might be considered reasonable for both parties. This is a proposal with which we would agree.

---

[232] See *Vice-Chancellor, Macquarie University v FM (GD)* [2003] NSWADTAP 43, paras 36, 41.
[233] Indeed one of the difficulties, noted above, is the number of exemptions to the definition of 'personal information' (rather than being framed as exemptions to one or more of the IPPs), and thus applicants may find themselves having to argue about the scope of the Act itself in order to meet a jurisdictional hurdle well before coming to discussion about the facts or the application of the IPPs to the conduct or decision in question.
[234] *Fitzpatrick v Chief Executive Officer, Ambulance Service of NSW* [2003] paras 16-19

We submit that such time limits should only start to run after the internal review report has been provided to the applicant. If the Privacy Commissioner is also expected to provide comment on the draft findings of the internal review (see recommendations above), any statutory timeframes should also accommodate such action.

Recommendation:

- That section 55 be amended to set appropriate time limits in which to lodge an application for external review in the Tribunal.

Effect of other statutes

Section 55 of the PPIP Act has been examined in the NSW Court of Appeal, in the context of whether or not the Tribunal may review the conduct of the NSW Ombudsman[235].

Section 35A of the Ombudsman Act provides a protection against liability for the Ombudsman, by requiring a person who seeks to commence 'civil proceedings' against the Ombudsman to first seek the leave of the Supreme Court, which must be satisfied that there is substantial ground to find 'bad faith' on behalf of the Ombudsman or other officer before leave may be granted[236].

Overturning an earlier Tribunal findings, the Court of Appeal found that review proceedings in the ADT under the PPIP Act are 'civil proceedings', rather than administrative review. Thus before a privacy complaint may proceed to the Administrative Decisions Tribunal, the applicant must first satisfy the Supreme Court that there is substantial ground to find 'bad faith' on behalf of the Ombudsman or other officer.

This case turned upon some unique issues, such as whether or not there is such a thing as the Office of the Ombudsman (in terms of being a 'public sector agency' subject to review under the PPIP Act). Nonetheless this case raises the issue of whether it was Parliament's intention that legislative provisions common to a number of agencies and statutory office holders, aimed at protecting office holders and their staff from any personal liability for their actions done in good faith, should exclude external review by the ADT of the conduct of the relevant agency as vicariously liable for the conduct of office holders and their staff.

[235] *The Ombudsman v Koopman & Anor* [2003] NSWCA 277 – Mason P, Meagher JA, Santow JA.
[236] Section 35A of the Ombudsman Act 1974 states: (1) The Ombudsman shall not, nor shall an officer of the Ombudsman, be liable, whether on the ground of want of jurisdiction or on any other ground, to any civil or criminal proceedings in respect of any act, matter or thing done or omitted to be done for the purpose of executing this or any other Act unless the act, matter or thing was done, or omitted to be done, in bad faith. (2) Civil or criminal proceedings in respect of any act or omission referred to in subsection (1) shall not be brought against the Ombudsman or an officer of the Ombudsman without the leave of the Supreme Court.
(3) The Supreme Court shall not grant leave under subsection (2) unless it is satisfied that there is substantial ground for the contention that the person to be proceeded against has acted, or omitted to act, in bad faith.

Similar provisions protecting against personal liability exist in statute for the Registrar of Births, Deaths and Marriages, the Board of Vocational Education and Training, the Commissioner for Children and Young People, the Community Relations Commission, the Director of Public Prosecutions, and the Privacy Commissioner[237].

Recommendation:

- That section 55 be amended to provide that review by the Tribunal does not constitute 'civil proceedings' for the purpose of the Ombudsman Act and other statutes which limit the personal liability of statutory and other office holders.

The Privacy Commissioner's role in the Tribunal

The Privacy Commissioner has automatic standing to appear, but is not a party to any proceedings in the Tribunal. This protects the office from any costs orders. In practice the Privacy Commissioner exercises his or her right of appearance through one of the legal officers on staff, as inadequate resources are available to brief counsel.

The lack of clarity in the Act about the Privacy Commissioner's role in the Tribunal results in many parties to litigation believing that the Privacy Commissioner intends to assist or advocate on behalf of the applicant. We are concerned that this perception may make public sector agencies less willing to seek Privacy NSW's advice in other contexts. This is disturbing, as we see our advice and assistance role as very important in ensuring privacy is protected – prevention being better than the cure.

We are currently working on some written material to better explain our role in the Tribunal, which we hope will address these common misconceptions. Nonetheless some further legislative clarity would be of benefit.

One particular area which could benefit from further clarity is the Privacy Commissioner's role when matters are referred by the Tribunal to mediation or settlement discussions. We have taken the view that the Privacy Commissioner has no role in such discussions, because the Commissioner's role is to assist the Tribunal in terms of statutory interpretation, rather than resolution of the complaint. As noted above at 3.2, these interests often sit in tension. For example, while the parties may favour an out-of-court settlement, Privacy NSW and privacy advocates would be likely to prefer an open judgment because of their interest in systemic change.

However we believe this situation can be distinguished from the situation where the Tribunal approaches the Privacy Commissioner to assist in finding a remedy to a systemic problem highlighted by the individual complainant's case. Subject to adequate resourcing of the office, Privacy NSW could participate in determining an appropriate systemic remedy – for

[237] See section 61 of the Births, Deaths and Marriages Registration Act 1995, section 11 of the Board of Vocational Education and Training Act 1994, section 48 of the Commission for Children and Young People Act 1998, section 21 of the Community Relations Commission and Principles of Multiculturalism Act 2000, section 25 of the Director of Public Prosecutions Act 1986, and section 66 of the Privacy and Personal Information Protection Act 1998.

example the Tribunal could conceivably order an agency to consult with the Privacy Commissioner when amending its practices to ensure future compliance.

The Tribunal has found that the Privacy Commissioner's right to appear and be heard in proceedings brought under the PPIP Act includes matters which proceed to the Appeal Panel of the Tribunal[238]. However formalisation of this position in statute would be of benefit to all parties.

A further issue is raised when cases proceed on appeal beyond the Appeal Panel of the Tribunal, to the Court of Appeal. The cost of appearing, and the possibility of having costs awarded against the office, prevents the Privacy Commissioner from seeking to join as a party. Nonetheless such matters may raise important matters of statutory interpretation which will affect the robustness of privacy protection in NSW.

One possible solution would be a formalised role for the Attorney General to appear as amicus in all jurisdictions beyond the Administrative Decisions Tribunal, in which matters of statutory interpretation of the PPIP Act are raised.

Recommendation:

- That section 55 be amended to clarify the role of the Privacy Commissioner in relation to assisting the Administrative Decisions Tribunal with matters of statutory interpretation.
- That section 55 be amended to clarify the role of the Privacy Commissioner in relation to the development of remedies to systemic problems.
- That section 55 be amended to clarify the role of the Privacy Commissioner in relation to matters in the Appeal Panel of the Administrative Decisions Tribunal, and the role of the Privacy Commissioner and/or Attorney General in further appeals beyond the Tribunal.

What type of review is it?

Is the Tribunal conducting a review of a reviewable decision or making an original decision?

Arguments in support of the view that the Tribunal is conducting a review of a reviewable decision include:

- Section 52(4) of the PPIP Act ousts the internal review provisions of the ADT Act. This suggests that an application under the PPIP Act is intended to be an application for a review of a reviewable decision.
- Section 55(3) of PPIP Act ensures that merit review outcomes are also available in addition to damages, injunctions and other civil remedies.
- The absence of a provision in the PPIP Act which allows the Tribunal to award costs suggests that the legislature intended that an application under the PPIP Act is an application for a review of a reviewable decision. Otherwise the Tribunal would have no costs power in relation to such applications.

[238] See *Vice-Chancellor, Macquarie University v FM (GD)* [2003] NSWADTAP 43, paras 36, 41.

Arguments in support of the view that the Tribunal is making an original decision include:

- Section 56 expressly provides that a decision made by the Tribunal under this Part may be appealed to an Appeal Panel. There would be no need for such a provision if an application under the PPIP Act was an application for a review of a reviewable decision.
- The remedies available under s55(2) of the PPIP Act include damages and injunctions. These kinds of remedies are not typically available in merits review proceedings.
- The subject matter of the application is conduct rather than the exercise of discretion to make a particular decision. Discrete decisions of an administrator, rather than conduct in which they are alleged to have engaged, are generally the subject of merits review proceedings.

Tribunal Deputy President Hennessey has concluded that applications made under section 55 of the PPIP Act are applications for a review of a reviewable decision. She noted that the use of the word 'review', albeit in relation to conduct, suggests that the Tribunal is conducting a merits review of that conduct[239].

Clearly this situation requires greater legislative clarity. We submit that Part 5 requires substantial redrafting, but that the emphasis should remain on an enquiry model (in which the complainant puts certain conduct before the Tribunal, and the respondent agency must then have a discussion primarily with the Tribunal about whether or not the agency complied with the IPPs) rather than a civil litigation model (in which the plaintiff bears the onus of proving both the conduct and that conduct's non-compliance with the IPPs).

Recommendation:

❖ That section 55 be amended to clarify what type of review is contemplated under the PPIP Act, including matters such as appropriate remedies, costs, and time limits.

The availability of systemic remedies

The *FM* case suggests the Tribunal will be reluctant to impose a systemic remedy upon an agency unless there is particular evidence of a systemic problem. Yet neither applicants nor the Privacy Commissioner are likely to be in a position to provide evidence of systemic problems.

This illustrates the difficulty of using an adversarial model to enforce laws that by their very nature are aimed at systemic change.

We submit that the Tribunal should be encouraged, through proper legislative indication, to deal with systemic problems outside of remedies for the individual complainant. For example in relation to a review of conduct involving data security, the Tribunal could make finding that the agency could use to support a business case for change of practices, such as more funding for a new computer system.

[239] *Fitzpatrick v Chief Executive Officer, Ambulance Service of NSW* [2003] NSWADT 132, para 12

Recommendation:

- That section 55 be amended to provide powers for the Tribunal to enquire into matters of a systemic nature, and order remedies appropriately.

3.2.4 Proposed alternative model

To remedy some of the difficulties outlined above in parts 3.2.1 – 3.2.3 of this submission, we propose a model in which complaints investigated by the Privacy Commissioner may then be reviewed by the Administrative Decisions Tribunal, as an alternative to the existing path of internal review then review by the Tribunal. This proposal is only in relation to complaints which could otherwise be dealt with by internal review – that is, a complaint about the handling of personal by a public sector agency.

That is, we recommend that complainants may choose *either* internal review or an investigation by the Privacy Commissioner, but regardless of their choice they can seek a review by the ADT in order to obtain an enforceable remedy.

If this suggestion were adopted, one possibility is that the Privacy Commissioner could assist to narrow issues and make a prima facie determination before any matter reaches the Tribunal. This would be similar to the role envisaged for the Privacy Commissioner under the Health Records & Information Privacy Act 2002 in relation to complaints against private sector respondents[240].

Recommendation:

- That the ability to seek review by the Administrative Decisions Tribunal be expanded to include matters which could be the subject of internal review, but for which the complainant instead sought an investigation by the Privacy Commissioner.

A by-product of the litigation-based model of enforcement is that when matters come to internal review or before the Tribunal, agencies often seek to justify, after the event, conduct which contravened an IPP, by using a technical legal argument about an exemption that the person who did the conduct or made the decision did not even know about.

[240] Under section 48 of the HRIP Act, a complainant may only lodge their request for review in the Tribunal after the Privacy Commissioner has issued a report to both parties under section 47. The Privacy Commissioner can only issue such a report this after first deciding to investigate the matter under section 45(1)(b), rather than attempting to resolve the matter by conciliation or otherwise.

One possible way to attempt to address this situation is to amend the Act such that when an agency is seeking to rely on an exemption to justify its non-compliance with an IPP or public register provision, the agency must be able to demonstrate to the Tribunal that it knew of and relied on that exemption at the time of the decision or conduct.

Recommendation:

- That Part 5 be amended to place an onus on agencies claiming an exemption to justify any non-compliance with an IPP (or public register provision) to demonstrate that the person whose decision or conduct is at issue knew of and relied on that exemption at the time of their decision or conduct.

3.3 Miscellaneous provisions

3.3.1 Definitions

Definition of 'personal information'

Section 4(1) defines 'personal information' as:

> (1) In this Act, "personal information" means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.
>
> (2) Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics.

Although these provisions appear reasonably clear to us, it is our experience that agencies and members of the public alike struggle with the concepts presented here[241].

It is also suggested that it would be beneficial to more explicitly state that photographs and video footage fit within the compass of this Act. (They are of course still be subject to the proviso in s.4(1), that a person's identity is apparent or can reasonably be ascertained from the image.)

Recommendation:

- That section 4 be amended to clarify that information or an opinion need not be recorded *or* form part of a database.
- That section 4 be amended to clarify that captured images could be personal information.

[241] For example an ambiguity was exposed as to the meaning of the words within the parentheses in Macquarie University v FM [2003] NSWADTAP 43; see discussion from para 52 onwards.

Note:
An example of how this recommendation could be achieved follows:

(1) In this Act, "personal information" means information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

(1A) Paragraph (1) applies

(i) whether or not the information or opinion is recorded in a material form, and

(ii) whether or not the information or opinion forms part of a database.

(2) Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics, and images captured in still or moving form.

Definition of 'public sector agency'

'Public sector agency' is defined in section 3 of the PPIP Act. It is a long definition with many sub-parts which we won't quote in its entirety here.

Part of the difficulty with the definition is its very complexity. Examples of organisations for which the application of the definition has not been straight-forward, or has been subject to some debate, includes the Legislative Council, Aboriginal Land Councils[242], the office of the NSW Ombudsman, community visitors, advisory committees attached to agencies, and public hospitals run by affiliated health services[243].

While it is clear that a local council is a public sector agency, and it is also clear that local councillors are public sector officials, there is some uncertainty as to whether the actions of an individual local councillor constitute the actions of the council of which he or she is a member. Unlike an employee of the council, the General Manager has little control over the actions of an individual councillor. That is, there is a question as to whether the council as a corporate body is the agency against which a remedy lies for the actions of an individual councillor.

This is a question not so much for the definition of 'public sector agency' but for a provision such as section 20 which sets out how the IPPs apply to public sector agencies. Nonetheless it is illustrative of the difficulties faced when basing accountability legislation such as the PPIP Act on a certain model of government (a State government department headed by the Director General who employs all the staff therein and can control the actions of those staff), which does not easily translate to other models of government (such as the relationship between a local council and its elected councillors), individual statutory office holders (such as community visitors), and quasi-government bodies which may have members not considered public servants (such as advisory committees or land councils).

It may be that for some of these quasi-government bodies it may be preferable that they not be considered a 'public sector agency' in terms of the actions of the individuals, on the basis

[242] Section 248 of the Aboriginal Land Rights Act provides that each Aboriginal Land Council is taken to be a 'public authority' for the purposes of the ICAC Act, FOI Act and the Ombudsman Act.
[243] St Vincent's hospital has argued that it is not a public sector agency as defined in the PPIP Act, because it was not a statutory body representing the crown and its accounts were not audited under the Public Finance and Audit Act.

that individually their members will still be considered 'public sector officials', and thus at least bound by the offence provisions of the PPIP Act in terms of corrupt disclosure. It may also be appropriate to consider that when acting collectively (such as councillors or committee members voting on a certain course of conduct) they ought comply with the IPPs.

Another difficulty with the definition of public sector agency is in relation to the grey areas between the 'public' and 'private' sector. For example some organisations may be caught by the PPIP Act definition, but also considered a private sector organisation under the Federal Privacy Act, and thus regulated twice[244].

Paragraph (g) in the definition enables organisations that provide data services to an agency to be prescribed 'in'; to date this provision has not been used. There seems little point in doing so, as the agency contracting to the service provider will be vicariously liable for its contractors' actions[245], and/or the private sector service provider will be regulated by the more recent Federal Privacy Act.

State-owned corporations are clearly exempt from the definition of public sector agency. We understand this was a policy decision taken so as to avoid duplication when the Federal Privacy Act was amended to incorporate private sector coverage – a plan being discussed in 1998 when the PPIP Bill was being drafted, but not finalised by Federal Parliament until December 2000, and not implemented until December 2001. However in its ultimate form, the Federal Privacy Act exempts State authorities and instrumentalities[246], and thus state-owned corporations have fallen through a gap in privacy regulation.

Contrary to what might be expected, at least one state-owned corporation does not like this unregulated state of affairs. Sydney Water decided some years ago to 'voluntarily comply' with the IPPs, as a matter of customer respect and trust. We understand that compliance with the IPPs has been incorporated into its customer charter, as overseen by IPART. Nonetheless this means no remedy can lie against Sydney Water in the ADT for a breach of the IPPs.

A further reason that Sydney Water and other state-owned corporations have expressed the desire to be included as a 'public sector agency' under the PPIP Act is to be able to take advantage of the exemptions currently in force relating to the transfer of personal information between agencies. That is, other agencies are now prohibited from disclosing personal information to Sydney Water, but in circumstances that would be the reverse if they were recognised as a public sector agency.

It is submitted that state-owned corporations ought be explicitly included under the PPIP Act. In many respects the PPIP Act provides more privacy protective standards than the NPPs in the Federal Privacy Act (which apply to private sector organisations, not federal government agencies), and the breadth of the employee records exemption in the Federal Act is a good reason to not promote regulation under that Act as an alternative. That is, to achieve a parity in privacy protection for employees of state-owned corporations as against other public sector employees, coverage under the PPIP Act is to be preferred.

[244] We understand that it is for this reason the NSW Law Society and the Bar Association have been exempted from the provisions of the PPIP Act entirely, by way of regulation.
[245] See section 4(4) of the PPIP Act.
[246] See section 6C of the Federal Privacy Act 1988, which defines 'organisations'.

We therefore suggest that the Act be amended to insert a mechanism by which organisations may be prescribed in or out of the definition of 'public sector agency', and/or an agency may be considered part of another agency for some or all purposes under the Act. In this way for example, the conduct of individual community visitors could be subject to review through another agency.

Recommendation:

- That the definition of 'public sector agency' be clarified in terms of its application to quasi-government bodies.
- That the definition of 'public sector agency' be extended to include state-owned corporations.

3.3.2 Application of the IPPs and exemptions to the IPPs

Division 3 of Part 2 of the PPIP Act is headed 'Specific exemptions from principles'. At the beginning of that division, section 22 provides:

> Nothing in this Division authorises a public sector agency to do any thing that it is otherwise prohibited from doing.

It is a fairly common misapprehension that the IPPs can act to 'authorise' conduct that is explicitly prohibited under another statute. For example, it is common for agencies to have a 'secrecy' provision in relation to sensitive information they handle. The IPPs relating to disclosure may in fact be more 'permissive' than such specific prohibitions[247].

Furthermore we have had experience of agencies believing that a public interest direction from the Privacy Commissioner will not only authorise conduct that would breach the IPPs, but can authorise the conduct *per se*, in such a way as to override other secrecy or confidentiality obligations imposed not under the PPIP Act. While it is clear to us that we do not have such authority, a more explicit provision would be of assistance to other parties in understanding the application of this statute, and the role of the Privacy Commissioner, in relation to their operations. It would also assist in minimising the extent to which agencies can claim that their operations are affected 'because of the Privacy Act'[248].

[247] See the discussion above at Part 3.1.1 of this submission in relation to section 18(1)(b) in particular.

[248] 'BOTPA' was coined by the former New Zealand Privacy Commissioner Bruce Slane, and is the term now commonly used by Australasian Privacy Commissioners to describe situations in which an organisation mistakenly claims it is prevented from doing something 'Because Of The Privacy Act'. Sometimes this is the result of a misreading of the PPIP Act or not finding or recognising an applicable exemption. On other occasions the real reason that the conduct is not occurring might be other specific legislative prohibition, organisational policy or corporate culture, lack of resources, contractual confidentiality reasons, political expediency, or a desire to avoid embarrassment. Some examples from NSW appear in our 2002-03 annual report.

It is therefore recommended that this provision be moved to the beginning of Part 2 of the Act, and expanded so as to cover the IPPs and *all* exemptions to the IPPs (not only the exemptions to the IPPs set out in sections 23 to 28 of the Act).

That is, clarify that the information protection principles do not override any other legislative prohibition against any particular conduct, except where explicitly stated. (The only occasion on which the IPPs override another statute is in relation to the amendment of a record under IPP 8, which overrides the State Records Act[249].)

Furthermore clarify that any exemptions to the IPPs (whether in the Act, a regulation, code or public interest direction) only modify the application of the IPPs; they do not authorise any conduct that would be prohibited under any other law, contract or obligation.

Recommendation:

- That section 22 be amended to clarify that the IPPs do not authorise any conduct that would be prohibited under any other law, contract or obligation, except where explicitly stated in the PPIP Act.
- That section 22 be amended to clarify that any exemptions to the IPPs (whether in the Act, a regulation, code or public interest direction) only modify the application of the IPPs; they do not authorise any conduct that would be prohibited under any other law, contract or obligation.

3.3.3 Exemptions mechanisms (codes and directions)

Privacy codes of practice

Sections 29 to 32 of the PPIP Act establish the mechanism by which privacy codes of practice may be made by the Attorney General after consultation with the Privacy Commissioner. For the reasons provided in part 2.1.2 of this submission, it is recommended that these provisions be deleted entirely.

Recommendation:

- That sections 29 to 32 be deleted.
- That if the above recommendation is not accepted, that Privacy NSW be approached for further advice on more specific clarifying amendments to these provisions.

[249] See section 20(4) of the PPIP Act currently, which is to be deleted but re-enacted as section 15(4) upon commencement of the HRIP Act shortly.

Public interest determinations

Section 41 establishes the mechanism by which public interest determinations may be made by the Privacy Commissioner after consultation with the Attorney General. For the reasons provided in part 2.1.2 of this submission, it is recommended that these provisions be amended as set out in that part of this submission.

Recommendation:

- That section 41 be amended as set out in part 2.1.2 of this submission.

3.3.4 Agency accountability and reporting requirements

Privacy management plans

Section 33(2) provides:

> (2) The privacy management plan of a public sector agency must include provisions relating to the following:
>
> …
>
> (d) such other matters as are considered relevant by the agency in relation to privacy and the protection of personal information held by the agency.

To date Privacy Management Plans have not been particularly useful tools in terms of a member of the public seeking to establish exactly how the IPPs or public register provisions apply to a particular agency, what exemptions might apply, how their common practices comply with the IPPs (as modified by any exemptions), or how complaints or internal reviews are likely to be handled within that agency.

There is also a requirement in section 33(5) that any plan must be sent to the Privacy Commissioner. This adds very little in terms of accountability (we have never had the resources to review draft or final plans, and rarely consult plans when investigating complaints), and creates for us a practical problem in terms of storage[250].

It is recommended that public accountability could be achieved in a less paper-wasting manner, by means of the following:

- a requirement on agencies to place their plan on their website (if they have a website) and to make the plan available for inspection at any time
- a requirement on agencies to provide the Privacy Commissioner with a copy upon the Commissioner's request

[250] We have well over 400 plans lodged to date, many of them very large documents, with little ability to destroy our copies under our disposal authority until such time as they have been superceded – a state which we find difficult to determine.

- if an agency keeps any 'public registers', that agency's plan must list each register, state clearly what the purpose of a register is, and state clearly what the 'purposes relating to the purpose of the register' are, in terms of the public register provisions
- the plan must nominate who the current Privacy Contact Officer is for that agency, and how they may be contacted
- the plan must explain how internal reviews will be conducted for that agency (eg. whether centrally or locally in dispersed agencies)
- the plan must state whether any privacy code of practice applies to the agency, and if so how
- the plan must state whether the agency will seek to rely on any temporary public interest determinations, and if so, explain how they apply
- a requirement on agencies to update their plan within 3 months of any of the above information changing (ie. such as the person nominated as the Privacy Contact Officer, or the creation of a new public interest determination for that agency)

Recommendation:

- ❖ That section 33 be amended to delete the requirement for privacy management plans to be sent to the Privacy Commissioner.
- ❖ That section 33 be amended to require agencies to keep their privacy management plans up-to-date, and publicly available via their website and other mechanisms.
- ❖ That section 33 be amended to require agencies to include in their privacy management plans the following information:
  contact details for their Privacy Contact Officer
  the purpose of each public register held by the agency
  the existence of any public interest determinations applying to that agency
  the existence of any codes applying to that agency

Annual reporting requirements

Section 33(3) provides:

> (3) The annual report of each public sector agency must include:
>
> (a) a statement of the action taken by the agency in complying with the requirements of this Act, and
>
> (b) statistical details of any review conducted by or on behalf of the agency under Part 5

As this provision is buried in the middle of a provision dealing with privacy management plans, it would appear doomed to a low rate of compliance. It is suggested that this should be a stand-alone provision in the PPIP Act with own heading, or that it be incorporated into the Annual Reports Act instead.

In either case, it is also suggested that this provision could provide more guidance on what 'statistical details' means. We have advised agencies[251] that as a matter of best practice the following should be considered:

- the number of internal review applications lodged during the year
- the number of internal review applications finalised during the year
- the outcomes of each internal review that was finalised (eg: the IPP / Code / public register provision(s) at issue; the finding - breach found or no breach found; any remedy or action proposed or taken)
- the number of matters lodged in the ADT during the year
- the results of any ADT matters finalised (determined or settled) during the year

Recommendation:

- ❖ That section 33(3) be incorporated within the Annual Reports Act or made a separate provision of the PPIP Act.
- ❖ That the annual reporting requirements of an agency include a requirement to report on the number of internal review applications lodged during the year, the number of internal review applications finalised during the year, the outcomes of each internal review that was finalised, how many matters were lodged in the AD, and; the results of any ADT matters finalised (determined or settled) during the year.

[251] See our newsletter to Privacy Contact Officers from April 2003.