office of the privacy commissioner
new south wales

information and privacy commission
new south wales

Report of the Privacy Commissioner under Section 61B of the *Privacy and Personal Information Protection Act 1998*

February 2015

Letter of Transmission

office of the privacy commissioner
new south wales

The Honorable Don Harwin MLA
President, Legislative Council
Parliament of NSW
Parliament House
Macquarie Street
Sydney NSW 2000

The Honorable Shelley Hancock MP
Speaker, Legislative Assembly
Parliament of NSW
Parliament House
Macquarie Street
Sydney NSW 2000

Dear Mr President and Madam Speaker,

In accordance with section 61B of the *Privacy and Personal Information Protection Act 1998* (PPIP Act), I am pleased to present the *Report of the Privacy Commissioner under Section 61B of the Privacy and Personal Information Protection Act 1998*.

I provide this report to the Parliament for tabling as provided in section 61D(1) of the PPIP Act, to be laid before that House of Parliament on the next sitting day of the House after it is received.

Yours sincerely,

Dr Elizabeth Coombs

NSW Privacy Commissioner

23 February 2015

Table of Contents

Executive Summary

office of the privacy commissioner
new south wales

Privacy is a dynamic area and one upon which everyone has a view.

The debate around information communication technologies, the economics of personal information and changes in community expectations and behaviour intensifies with each new technological device and well publicised data breach. Against this background, public trust in the regime for protecting privacy and personal information is of significant importance, and the effective protection of individual privacy remains a key strategic issue for the NSW Government, public sector agencies and the public.[1]

1. NSW Independent Commission Against Corruption, Response to the invitation to provide feedback on the operation of the PPIP Act in 2013 – 2014.

How well has the NSW *Privacy and Personal Information Protection Act 1998* been operating and what challenges are posed to NSW's privacy regime?

The *Privacy and Personal Information Protection Act 1998* (the PPIP Act) has stood the test of time well. It continues to serve a valuable public policy purpose, a purpose that has grown in relevance with the growth in technology and increasing incursions into the privacy of individuals. At the same time, amendments would be constructive; on one hand to better protect the privacy of individuals and on the other, to assist the operation of NSW public sector agencies.

The world is very different from 1998 when this legislation was enacted and changes are required to adapt to how we now live, work and play. The 12 legislative information protection principles remain relevant and appropriate but need to better reflect the changes that have occurred over time in information communication technologies and service provision, and their impacts upon the privacy of the people of NSW.

Many of the issues raised by the public and public sector agencies concern the exponential growth in technology and its impact upon how our society operates. The public is concerned about 'big data' and data mining, surveillance, identity theft, on selling of personal information, 'big brother' and metadata interception, risks in the shared economy, vulnerability particularly of seniors and younger children, seemingly insecure storage of personal information by organisations including ammunition retailers and the excessive amount of personal information collected for mundane transactions – amongst other things!

The NSW Parliament created an obligation on the Privacy Commissioner to report to Parliament on the annual operation of the PPIP Act. This report provides an overview of the operation of the Act from 1 July 2013 to 30 June 2014. Drawing on work undertaken during this period and feedback from members of the public, privacy practitioners, government departments, non-government organisations and the heads of oversight agencies, the report identifies issues for legislative action as well as action by the Privacy Commissioner, agencies and members of the public.

In an increasingly global world, individuals, public sector agencies and businesses operate across State, Territory and national boundaries. One privacy regime covering all Australia jurisdictions would simplify the current legislative landscape, however, the processes to achieve this would be neither quick, easy nor necessarily successful. Aligning NSW privacy legislation more closely with that of the Commonwealth, and other State and Territory jurisdictions, through amendment to the core principles of the PPIP Act will assist. I recommend, as have others before me, the introduction of provisions covering the movement of personal information outside of NSW and the right to anonymity where lawful and practicable. I also recommend the introduction of mandatory reporting of serious data breaches particularly if this provision is introduced into Commonwealth legislation. A shift from old style reactive compliance to proactive and effective incorporation of privacy in organisational governance and culture is the future and the adoption of the 'privacy by design' principle provides the vehicle to achieve this shift.

As Privacy Commissioner I welcome steps by the NSW Government and its agencies to improve policy development, service planning and service delivery which will increase access to government services by ordinary citizens provided there is no reduction in the level of privacy protection for individuals. The focus upon the customer and the development of a 'one stop government shop' and a 'one Government client' facility is an opportunity to place privacy respectful practices at the heart of customer services and build trust with the community.

I am concerned about the lack of formal privacy protection for clients of some State Owned Corporations (SOCs) and recommend that all NSW SOCs be subject to privacy regulation. This can be achieved by ensuring coverage either by the PPIP Act or the Commonwealth Privacy Act.

I recommend amendments to the PPIP Act to ensure no diminution in the protection of privacy and personal information in the outsourcing of government services to private sector and not for profit service providers, and realise that greater support is required by agencies and myself to assist non-government service providers' ▶

Executive Summary (continued)

privacy management practices. I also recommend that the important privacy right of being able to know what personal information is held about you, and the right to see and correct your personal information reside solely in the PPIP Act and not in the *Government Information (Public Access) Act 2009* (GIPA Act). This would simplify the current multiple arrangements and remove the administrative complexity imposed on NSW public sector agencies.

Changes in technologies including the advent of 'big data' and cloud computing as well as the increasing use of surveillance devices are high in the public's consciousness. The challenges and risks to privacy protection posed by these developments require strategies to utilise such technologies while protecting the privacy and personal information of individuals. Similarly, data sharing and data mining concern the public. Appropriate methodologies for data sharing and de-identification of data are required to enable agencies to utilise the sector's data for policy development and service planning while protecting the privacy of individuals whose personal information is being utilised.

Legislative amendment is not the only means to achieve better privacy practices. The behaviours of individuals, organisations as well as public sector agencies all play a part and are important components of protecting privacy. How agencies conduct their business has significant implications for privacy protection. Similarly, individuals need to take steps to protect their personal information. Some of the issues raised by agencies reflect the need for greater organisational capability in understanding privacy and its governance. This can be reflected in the management of privacy risks and sometimes, in the erroneous use of privacy as a reason not to provide information requested or to maintain 'information bunkers'. I seek to establish projects with other agencies for example, the Department of Premier and Cabinet and the Public Service Commission both of who have important leadership roles across the NSW public sector and interests in these issues.

Throughout the year, the overall commitment to good privacy frameworks and practices has been apparent across NSW public sector agencies. There have been some strong performers and some others still to understand the importance of privacy in establishing a strong customer service ethos and organisational accountability. More assistance is required for agencies and I acknowledge that support to date has been insufficient.

I summarise the further guidance requested by agencies. Improved resourcing however is required to enable this to occur. The formation in January 2011 of the combined Information and Privacy Commission was to provide amongst other things, significant increases in resources to privacy. This needs to be recognised. The recommendations of this report form the work program for the Privacy Commissioner in 2015 and should inform the resourcing for the priority projects identified in this report.

I would like to thank the members of the public who gave their time to indicate their expectations and concerns around privacy, to Secretaries and privacy contact officers within agencies, to those non-government organisations who provided information of their understanding of their privacy responsibilities, and to the integrity agencies who gave their feedback and insights. I also want to thank the staff of the Information and Privacy Commission who assisted with preparing this report. Lastly, very sincere thanks to Ms Jan McClelland of McClelland and Associates who contributed beyond measure to the analysis of material and development of the report.

Dr Elizabeth Coombs
NSW Privacy Commissioner

Key Recommendations

PRIVACY BY DESIGN

The IPPs within the PPIP Act to include an overarching principle of 'privacy by design'. *Recommendation 8, page 23.*

COVERAGE OF THE PPIP ACT STATE OWNED CORPORATIONS

All NSW State Owned Corporations should be covered by privacy legislation. *Recommendation 3, page 20.*

ACCESSING PERSONAL INFORMATION

Access to and amendment of personal information to be governed solely by the PPIP Act and access to non-personal (Government) information be governed by the GIPA Act. *Recommendation 12, page 25.*

ANONYMITY & PSEUDONYMITY

The PPIP Act to be amended to include principle of anonymity and pseudonymity where lawful and practicable. *Recommendation 9, page 23.*

PRIVACY BREACHES

The PPIP Act to be amended to provide for mandatory notification of serious breaches of an individual's privacy by a public sector agency similar to that proposed to be provided in the *Privacy Act 1988 (Cth)*. *Recommendation 10, page 24.*

SURVEILLANCE

Privacy Commissioner to prepare guidance for agencies on the use of surveillance technologies. *Recommendation 23, page 34.*

Key Recommendations (continued)

CONTRACTED SERVICES & CONTRACTORS

The PPIP Act to be amended to clearly cover contracted service providers and contractors. *Recommendation 4, page 21.*

The Privacy Commissioner to provide guidance and assistance to non-government organisations in meeting their obligations and to manage implementation of contracts and reporting on compliance. *Recommendation 6, page 21.*

SHARING 'PERSONAL INFORMATION' FOR POLICY ANALYSIS & PLANNING PURPOSES

A Code of Practice to be developed to enable information sharing for planning and policy analysis purposes between agencies. *Recommendation 30, page 39.*

INFORMATION TECHNOLOGY SECURITY

ISO/IEC 27018 standard covering privacy, security and cloud services to be considered for inclusion in the NSW Government's Information Security Management Systems Policy. *Recommendation 18, page 32.*

GOVERNMENT SERVICE PROVISION

The alignment of the PPIP Act and emerging service provision models particularly of the 'one government customer' to be examined and a report prepared if amendment of the PPIP Act is indicated. *Recommendation 27, page 37.*

FIREARM REGULATION AND RISKS TO INDIVIDUAL PRIVACY AND PUBLIC SAFETY

NSW Police Force review the processes and systems relating to the register of firearm ammunition purchases to ensure compliance with relevant legislation while ensuring the protection of privacy of personal information of purchasers. *Recommendation 24, page 35.*

1

Introduction

1 Introduction

The *Privacy and Personal Information Protection Act 1998* (PPIP Act) is designed to protect the personal information and privacy of NSW citizens. Along with the *Health Records and Information Protection Act 2002* (HRIP Act) it provides the privacy regime for NSW public sector agencies.[2]

Since its introduction nearly 20 years ago, technology has changed the way we work, live and play. Challenges to privacy abound and the ability of the PPIP Act to meet these challenges has been questioned. Assessing the 'fitness' of the PPIP Act is enabled under the PPIP Act by section 61B, which requires the Privacy Commissioner to prepare a report on the annual operation of the Act generally, and across all public sector agencies for the 12 months preceding the end of the financial year. Typically, this report has formed part of the Privacy Commissioner's annual report to the NSW Parliament.

The growth in the significance of privacy matters and privacy's increasing prevalence in the affairs of NSW public sector agencies has led me to prepare a separate section 61B report on the operation of PPIP Act for the financial year 2013 – 2014.

The purpose of the report is to provide an insight into the operation of the Act from the perspective of the Privacy Commissioner, NSW public sector agencies, privacy practitioners, non-government organisations and members of the public, and to identify key strategic and operational issues of interest and concern in the protection of the privacy and personal information of the citizens of NSW. It is not meant as a comprehensive analysis of privacy issues facing NSW; it is a distillation of those matters arising throughout 2013 – 2014 that reflect issues arising from the operation of the PPIP Act, and those matters that concerned members of the public and principally the NSW public sector.

A consolidated list of recommendations is set out in Section 8 of this report (see page 51).

2. The *Health Records and Information Protection Act 2002* has broader application than 'NSW public sector agencies' applying to both public and private health service providers and organisations above a certain size holding health information.

2

Background to the PPIP Act

2 Background to the PPIP Act

2.1 The *Privacy Committee Act 1975*

New South Wales was one of the first jurisdictions in the world to introduce legislation dealing specifically with privacy protection when the New South Wales Privacy Committee was established under the *Privacy Committee Act 1975*. The legislation was introduced into Parliament in February 1975 by the then Coalition Government. The legislation was informed by the report on the law of privacy by Professor W. L. Morison tabled in Parliament in April 1973.[3] The report recommended that there should be general legislative provision for the protection of the privacy of the individual against threats existing and foreseeable. The view taken was "because the subject of privacy is affected by rapid social and technological change, imperfect understanding of the background factors, and the lack of development of privacy policies at the present time, this should take the form of the establishment of a continuing privacy body to perform information-gathering functions and recommend legislation, while at the same time performing remedial functions of a limited kind, rather than general legislation at this time attempting finally to determine rights of privacy".

The then Attorney-General and Minister of Justice, the Hon J. C. Maddison, MP saw the concept of privacy as "essentially a component part of freedom" and difficult to define.[4] The Hansard records of the Parliamentary debate on the legislation indicate concern about the increasing use of computers and balancing the rights of individuals to privacy with the public interest of access to information in the delivery of services by the public and private sectors. These were key considerations of the Parliament. There was particular acknowledgement by the Attorney General that government departments, both in the State and in the federal sphere, could not do their work without information and statistics about citizens, "Much of this information is necessary to determine social policy, housing needs, census needs, eligibility for financial assistance, and a lot of other statistical data." A caution was sounded "Though much of this is necessary, we should always be on guard against the tendency of some government departments or officials to gather information for its own sake, without adequate justification, and to intrude on privacy in the process."[5]

In 1992 the Independent Commission Against Corruption reported on its Inquiry into the unauthorised release of government information. This investigation found evidence of a massive illicit trade in the sale of personal information held by the NSW Government agencies. The Commission noted:

> "The whole question of management of the increasing amount of confidential information held by the Government and its agencies, is in need of urgent attention. Until there are clear policies, adequate protection and effective laws, cherished privacy principles will be at risk, and the scope for widespread corruption will remain."

The Inquiry recommended privacy laws to rebuild public trust in government.[6]

Private members' Bills were introduced into the NSW Parliament in 1991 and 1992. In the 1994, the then Attorney General, the Hon. John Hannaford, MLC, introduced the *Privacy and Data Protection Bill*. The Bill did not proceed following the 1995 change of government.[7]

2.2 The *Privacy and Personal Information Protection Act 1998*

The *Privacy and Personal Information Protection Act 1998*, introduced 23 years after the P*rivacy Committee Act 1975* by the then Labor Government, recognised the rapid developments in technology that had occurred during those years and the need for more detailed and extensive legislation to address the demands of evolving information technologies, community and international expectations for effective privacy safeguards, and in particular the need for the development of standards in relation to data handling. In his second reading speech[8] the then Attorney General, the Hon J. W. Shaw MP commented on the massive increase in the storage capacity of computers, the establishment of wide area networks, the Internet and optic fibres allowing for the rapid transmission of digitised audio and video data. He observed that information technology made records of personal information more vulnerable to abuse as it

3. Professor W. L. Morison, Law School Sydney University, commissioned by Commonwealth and State Attorney Generals to report on reform of the law of privacy.
4. NSW Parliament Hansard, Legislative Assembly, Second Reading Speech, 20 February 1975, pp 3,745-3,750.
5. Ibid.
6. NSW Independent Commission Against Corruption, *Report on the Unauthorised Release of Government Information, Volumes 1-3*, August, 1992.
7. NSW Attorney General's Department, *Review of the Privacy and Personal Information Protection Act, 1998*, 2004.
8. NSW Parliament, Hansard, Legislative Council, 17 September 1998.

enabled the storage of vast amounts of personal data at low cost for indefinite periods of time, the instantaneous retrieval of personal data, the centralisation and linkage of personal data and the rapid and extensive transmission of personal data.

The Attorney General pointed to a 1994 survey commissioned by the Federal Privacy Commissioner that showed that "74 per cent of Australians considered the confidentiality of personal information to be a very important social issue, even more important than the economy and the environment. Most of those surveyed believed that government should pass legislation to ensure that privacy is protected."

The Attorney noted that government is one of the main collectors and users of personal information and that effective safeguards are a vital part of government's compact with the community. The Attorney General reminded the Parliament that the need to provide for safeguards in relation to the release of personal information held by NSW government agencies was highlighted in the ICAC's 1992 "Report into the Unauthorised Release of Government Information". That inquiry revealed an illicit trade in personal information involving government departments, the police, lawyers, financial institutions and private investigators. As well as drawing attention to the corrupt conduct involved in this trade, ICAC was very critical of the lack of any coordinated and consistent government policy dealing with the storage and release of information.

The Attorney General explained that the legislation applied information privacy principles only to the public sector at that stage as it had been decided that the application of data protection principles to the private sector should be done in a uniform manner on a national basis.

Hansard records the Attorney General in the second reading speech saying, "The purpose of the bill is to promote the protection of privacy and rights of the individual by the recognition, dissemination and enforcement of data protection principles consistent with international best practice standards... The data protection principles do not attempt to define the meaning of 'privacy' but seek to establish principles for dealing with personal information in an open and accountable manner."[9]

Rather than attempting to legislate a 'right to privacy', the Parliament adopted a principle based approach to the protection of privacy and personal information by NSW public sector agencies – NSW Government agencies, local councils and universities. The 12 information protection principles guide agencies in ensuring the protection of personal information when carrying out their roles and functions.

The Act very clearly sets out the obligations upon public sector agencies in their management of personal information and in addition, establishes a broader scope through certain statutory functions of the Privacy Commissioner which address privacy more generally. This broader championing role is reflected in the PPIP Act's full title that is, "An Act to provide for the protection of personal information, and for the protection of privacy of individuals generally; to provide for appointment of a Privacy Commissioner; to repeal the *Privacy Committee Act 1975*; and for other purposes." The Act expressly makes provision for the broader role of the Privacy Commissioner by the ability to conduct inquiries and to investigate privacy-related matters as the Privacy Commissioner thinks appropriate. These reserve powers are important in addressing strategic and systemic issues not the subject of complaints by individuals.

The PPIP Act provides flexibility to meet the particular needs of agencies, including law enforcement and investigation agencies through legislative exemptions. It also provides flexibility to modify the application of the principles by agencies by way of Codes of Practice or Public Interest Directions to meet particular needs while ensuring protection of the privacy and personal information of citizens.

9. Ibid.

3

Approach to reporting

In preparing the report I have cast the net widely to obtain qualitative and quantitative data on the operation of the Act. This has included:

- A survey of members of the public on key privacy issues, their experience with public sector agencies in resolving privacy issues and their awareness of privacy legislation and the role of the Privacy Commissioner
- Examination of the impact of emerging information communication technologies and key privacy issues
- An invitation to all Secretaries of Departments and other agencies to provide their views on key strategic and operational issues and the operation of the Act
- An invitation to NSW accountability organisations such as ICAC and the NSW Ombudsman to provide their views on key strategic and operational issues and the operation of the Act
- An invitation to the Information and Privacy Advisory Committee to advise of the issues relevant for inclusion in the report
- Review of the sections on privacy in the annual reports of Departments and statutory bodies required under annual reports legislation
- A survey of privacy practitioners in NSW public sector agencies including departments, agencies, councils and universities
- A survey of non-government organisations to ascertain their knowledge and understanding of privacy legislation and its impact on their work
- An invitation to the President of the NSW Civil and Administrative Tribunal (NCAT) to provide any information or comment on the operation of the PPIP Act.
- A review of complaints and internal reviews notified to the Privacy Commissioner in the period 2013 – 2014
- An analysis of requests for exemptions from provisions of the PPIP Act by public sector agencies
- Examination of matters handled throughout 2013 – 2014.

Where relevant aspects of the *Health Records and Information Protection Act 2002* (HRIP Act) are included but the focus of the report is upon the PPIP Act.

It is not possible to cover all matters arising from the operation of PPIP Act over the period 2013 – 2014 but discussion following reflects the complexity and nuances that arise in privacy and the application of the legislation.

Many agencies provided very detailed submissions raising practical issues experienced working with the PPIP Act. These are summarised in Attachment 2 Part A. Many agency privacy officers also provided feedback. They reported that in terms of their role, there were no changes to their agencies' legislative or administrative arrangements with implications for their administration of the PPIP Act. Also, the PPIP Act overall did not raise difficulties in terms of agency operations (71%). The feedback is summarised in Attachment 2 Part B.

4

Privacy issues identified by the public

Security, disclosure, use and collection of personal information were the major reported issues of concern to members of the public. The matters that the community felt should be covered by NSW privacy legislation were protection of personal information held by either the public or private sectors, the ability to enjoy the privacy of one's own home, privacy of personal communications and physical privacy such as freedom from surveillance.

This section provides a summary of the major issues identified by the public through the consultation for this report and the flavour of these views and concerns.

Consent for the provision, use and sharing of personal information

"The gov't should not collect my info without my consent..."

"Please form controls governing drone use, distribution of recorded imagery or voice material without consent from all people involved..."

"No private information should be shared without express permission or the person's knowledge!"

Excessive collection of personal information

"I am concerned that for transactions of a mundane nature my date of birth is required. I think this is overkill. I would prefer that a less intrusive method of verification could be used."

"I'm concerned about the collection and management of my personal information by the Opal card operators... Why do they need so much personal information about me?"

"At what point will it be legislated that entering competitions/subscribing to newspapers/getting an Opal card especially when they want you to register online, that the amount of information given is limited? To what is essential?"

Insecure holding of personal information collected

"As a firearm owner our details are being given when we purchase ammo and logged into a book that can be seen by anyone."

"She insists on playing the answering machine messages out loud in front of other staff and visitors to the office. These messages include personal and health information. It was reported... but they have failed to act."

Surveillance (drones, Opal card, neighbours)

"The potential proliferation of drones (in the future) by persons for no good purpose other than to sticky beak and harass private citizens i.e. invasion of one's personal space."

"Opal card tracking our movements."

"The impact on the psychology of people who are born into a society that surveils all its citizens does not seem like a healthy direction..."

Big data and data mining

"The power of big computing – big data, data analytics, data sharing – does have a real role in improving services, improving outcomes – but it does contain some genuine risks in terms of greater governmental controls/intrusions (and subsequent losses of freedom)."

"I am concerned about the volume of information being collected by groups such as Google, Facebook and Apple, particularly given the multiple jurisdictions they operate across."

Trustworthiness of those holding personal information

"People with your information can't be trusted."

Use of personal information and on-selling

"The public needs to know who shares what information and under what circumstances."

"On-selling of personal information once collected."

Specific initiatives and technologies

"A whole new area of invasion of privacy has been opened with the registration of Opal public transport cards."

"I am most concerned regarding social media outlets and the security of these especially in the long term."

4 Privacy issues identified by the public (continued)

Privacy and public safety risks arising from firearm regulation

"I feel that having personal details recorded when purchasing ammunition is a risk these records are easily stolen and can be used by criminals to target firearms owners. Showing the relevant licence still achieves the same goal and is safer."

"I am concerned that the purchase of ammunition in NSW requires provision of firearms licence details AND drivers licence details including home address. The combination of these two sets of private information exposes me to potential theft and compromises my personal safety, with no demonstrable public safety benefit."

"My issue in particular is regarding firearms legislation, namely the NSW Ammunition bill. There have been several recent incidents of these records being specifically targeted and stolen. To purchase ammunition, I am required to provide my name, address, firearms license number and type of ammunition purchased. Talk about a shopping list for firearms theft."

Vulnerability of certain groups (seniors, children)

"As I am a senior I hope privacy regulations relating to seniors will be strengthened; special consideration I think for seniors as we are quite vulnerable at this age."

"I have grave concerns for the privacy and rights of my children given the proliferation of collection of personal information in day to day activities."

Challenges obviously exist in addressing many of these concerns; some are outside the natural jurisdiction of the PPIP Act such as those relating to Google and social media companies. Moreover, where information is volunteered as in social media, we all need to think carefully about the information we provide about our family, our friends and ourselves. It not only may be irretrievable but stored electronically for a very long time if not permanently.

I will continue to monitor privacy issues of concern to the public to inform advice and other recommendations for the NSW Parliament and the Attorney General.

The responses to the survey of members of the public are set out in Attachment 1.

5

Operation of the Act

5 Operation of the Act

5.1 Definition of 'personal information'

The PPIP Act is primarily concerned with 'information privacy' rather than physical privacy or the notion of being 'left alone'. The Act does not define 'privacy'.

The legislative definition of 'personal information' revolves around the ability to identify an individual. It shares much in common with definitions in the legislation of other jurisdictions but differs in some significant ways. Unlike for example, the definition of personal information in the Commonwealth *Privacy Act 1988* the NSW legislation includes in its definition the personal information of people who have been deceased for up to 30 years.

The PPIP Act's definition of 'personal information (section 4(1)) means information or an opinion that allows the identity of an individual to be reasonably ascertained. The notion of 'reasonableness' means the definition is not 'black and white'. It puts the onus upon agencies to interpret and assess if their actions will lead to an individual's identity being 'reasonably ascertained'. Some agencies have raised the difficulties of providing unambiguous advice to operational units within the organisation.[10] While it is not possible for legislation to cover all the parameters of "reasonably ascertained", guidelines published by the Privacy Commissioner would assist agencies.

The remarkable technological advances in the collection and linkage of information have been accompanied by the advent of the information economy where personal information is a highly valued economic resource. The means to collect, share and use electronic personal information, the devices themselves, are increasingly sophisticated and capable of functions that once would only have been considered as belonging in science fiction.

We all now use a range of technological equipment each of which has its own identifying unit number and the ability to transmit electronic information without our express instigation. These technological devices, their identifying numbers and their usage pose interesting questions as to what constitutes 'personal information' and their identification or contribution to the identification of individuals.

The interconnection of uniquely identifiable embedded computing devices through the internet has further increased this complexity. Known as the 'internet of things', these devices are diverse in their use ranging from portable devices such as smartphones, digital watches, to large stationary installations such as bridge or motorway tolling gateways to mobile and complex systems used in aviation, vehicular transport systems and even health technologies. This interconnection and our strong and close reliance upon our technological devices each of which is uniquely identifiable, will continue to raise challenges for the Act's definition of 'personal information'.

As more and more technologies such as smartphones, security devices or drones are used by public sector agencies in their business operations, the more the PPIP Act's definition of personal information will be tested. An emerging issue is whether the PPIP Act's definition of personal information includes information captured, used and transmitted by such devices.

Recommendations

The Privacy Commissioner to:

1) develop guidelines on the concept of "reasonably ascertained" identity to assist NSW public sector agencies
2) provide a research paper to the Parliament on the implications of the increasing convergence and capacity of information communication technology for privacy and the definition of personal information in the PPIP Act.

10. Department for Education and Communities, Submission to *Report on the Operation of the Privacy and Personal Information Protection Act 1998,* 2014.

5.2 Coverage of the Act

5.2.1 State Owned Corporations

Despite the significant amount of personal information held by NSW SOCs they are currently exempt from NSW privacy legislation. The PPIP Act applies to 'public sector agencies' that is, State Government agencies, local councils and universities, bodies providing data services on behalf of these organisations (and any prescribed in regulations) but not SOCs.

The entities currently known as SOCs and operating as such for practical purposes are Networks NSW (comprising the three electricity network companies Essential Energy, Endeavour Energy and Ausgrid), the Port Authority of NSW (the amalgamation of Sydney Ports Corporation, Newcastle Port Corporation, Port Kembla Port Corporation), Hunter Water Corporation, Water NSW, Sydney Water Corporation, Superannuation Administration Corporation (Pillar), Landcom (trading as UrbanGrowth NSW), Forestry Corporation, Delta Electricity and TransGrid.[11]

Under section 6F of the Commonwealth Privacy Act, SOCs may opt in to the Commonwealth privacy regime but unless the SOC requests to be prescribed under the *Privacy Act 1988* (Cth), Commonwealth legislation does not apply to NSW SOCs. At present, three of the ten SOCs are prescribed organisations under the Commonwealth regime, that is, Essential Energy, Ausgrid and Endeavour Energy. This means that only those consumers, the customers of these three SOCs, have formal privacy protection and avenues for external redress for any complaints.

Review of annual reports and privacy policies show the majority of SOCs state they comply with either Commonwealth or NSW privacy legislation. A number of SOCs including Sydney Water, Water NSW and TransGrid, refer to being bound to the IPPs in the PPIP Act. Other SOCs refer to being bound to the *Privacy Act 1988* (Cth) including Transgrid, Landcom and the Forestry Corporation although not prescribed under the *Privacy Act 1988* (Cth).

The recognition by SOCs of the importance of privacy and the responsibilities is positive, however, their service users do not have the same level of protection as if there was formal legislative coverage. Voluntary compliance by a SOC with NSW privacy legislation does not provide external review of the complaint handling. This is in stark contrast to the options available to customers of the three SOCs covered by Commonwealth privacy legislation and the customers of other NSW public sector agencies. This inconsistency is clearly not desirable and needs to be addressed. This was noted in the response of the Department of Premier and Cabinet to my invitation to comment on the operation of the PPIP Act.[12]

The rationale at the time for the exclusion of SOCs from the PPIP Act was to ensure a level playing field between SOCs and commercial businesses. Overtime, views of the nature of the relationship between SOCs and Government have altered. Recent NSW legislative action has included SOCs in the Government sector; specifically, section 3(1) (g) of the *Government Sector Employment Act 2013* includes SOCs in the definition of the government sector. SOCs are already covered by the *Government Information (Public Access) Act 2009* (GIPA Act), which enables the public to access government information.

Private sector businesses above a certain size are required to comply with Commonwealth privacy legislation but only three of the ten NSW SOCs are prescribed under the *Privacy Act 1988* (Cth), although all of the ten meet the annual turnover requirement.

This regulatory gap in SOCs' responsibility for the personal information they collect, use and hold results in inconsistent privacy protections for consumers. This needs to be addressed as the community has heightened concerns around the collection, storage, use, and disclosure of their personal information and expects Government to provide protections for their personal information and privacy as shown by recent research.[13]

The statutory review of the PPIP Act undertaken by the Attorney General's Department in 2004 recommended that all NSW SOCs should be subject to privacy regulation.[14]

11. The SOCs listed in the *State Owned Corporations Act 1989* but have been sold are Eraring Energy (to Origin Energy) and Macquarie Generation (to AGL).

12. Department for Premier and Cabinet, Submission to *Report on the Operation of the Privacy and Personal Information Protection Act 1998*, 2014.

13. Office of the Australian Information Commissioner, *Community Attitudes to Privacy Survey. Research Report*, October 2013.

14. NSW Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, Recommendation 12, p34-37, 2004.

5 Operation of the Act (continued)

I am concerned to see a formal accountability framework in place for the protection of personal information and handling of privacy complaints arising from SOCs' operations.

Recommendation

3) All NSW SOCs should be subject to privacy regulation so that either:
   a) the PPIP Act applies to SOCs not covered by the *Privacy Act 1988* (Cth); or
   b) those currently not prescribed under the *Privacy Act 1988* (Cth), are prescribed.

5.2.2 Contracted services and contractors

The outsourcing of services traditionally provided by the government sector to the non-government sector where the workforce can include both employees and volunteers, needs to be well managed to ensure continuity of protection for personal information and the privacy of service users and third parties.

In this outsourcing, the NSW government requires these organisations to deliver services to citizens and to meet compliance obligations and standards required of NSW public sector agencies so there is no loss of quality in services provided. It is therefore incumbent on public sector agencies to ensure all compliance obligations for personal information are specified in contractual terms, to provide guidance and assistance to non-government organisations (NGOs) in meeting their obligations and, to manage the implementation of contracts including measuring, monitoring, benchmarking and reporting on compliance. Responsibility for complaints handling, internal reviews and statistical reporting on privacy matters also need to be addressed in contractual arrangements with the non-government sector.

Survey responses from NGOs[15] indicate the need to strengthen the requirement for contracts between the NSW government and NGOs for service provision to specify the requirement to comply with relevant privacy laws, and for reporting regimes to include privacy compliance measures and regular audits of compliance. This survey indicated a need for targeted communications and resources for NGOs outlining their obligations under the PPIP Act, the HRIP Act and the *Privacy Act 1988* (Cth).

The NGO survey results also highlight the need to raise awareness among NGOs about the responsibility of the NSW Privacy Commissioner to assist them to meet their privacy obligations. It also suggests the need for resources and training for NGOs in meeting their privacy compliance obligations under NSW legislation and for peak bodies to develop their capability in providing assistance to NGOs.

This is not a new issue; the statutory review of the PPIP Act undertaken by the Attorney General's Department in 2004 recommended that PPIP Act should provide a structure for binding non-government organisations contracted by public sector agencies.[16] Amendment to the PPIP Act would place beyond doubt the obligations for protecting personal information of users of contracted services, particularly where other enabling legislation does not contain such provisions.

Some agencies have obligations under other legislation to ensure contractual or other commercial arrangements include compliance with the PPIP Act. An example is Roads and Maritime Services which under section 66, *Road Transport Act 2013* must require a party to these contractual arrangements for the provision of special number plates, to comply with the PPIP Act. This is not common however.

In addition to NSW public sector agencies, the PPIP Act applies to "a person or body that provides data services" (section 3 public sector agency (g)(i)) but not explicitly to other service providers under contract to a public sector agency. Some agencies have raised questions about the coverage of contracted services providers who do not provide "data services" but who provide services involving personal information.

It was raised that the PPIP Act, be aligned to other jurisdictions' legislation by amendment to require agencies entering into a contract with an organisation contracted as a service provider where the organisation will manage personal information complies with NSW privacy legislation.[17] Another aspect raised was for the scope to include contractors such as sole traders who may be providing services other than 'data services' but which involve privacy or personal information.

15. Summarised in Attachment 3.

16. Op cit, Recommendation 13, p37, 2004.

17. Department of Premier and Cabinet, Submission to *Report on the Operation of the Privacy and Personal Information Protection Act 1998,* 2014.

It has been drawn to my attention that section 53 of the *Anti-Discrimination Act 1977* provides a useful model for consideration in ensuring there is no diminution in privacy protection through provision of government services by other bodies.

Recommendations

4) The PPIP Act to be amended to clearly cover contracted service providers and contractors who may be involved in services other than 'data services'.
5) Privacy compliance obligations are specified in contractual terms for the outsourcing of the provision of government services by public sector agencies to non-government organisations.
6) The Privacy Commissioner to assist agencies to provide guidance and assistance to non-government organisations in meeting their obligations and to manage the implementation of contracts including measuring, monitoring, benchmarking and reporting on compliance.

5.2.3 What is 'an agency' for the purpose of use and disclosure of information?

In 2011, NSW Government entities were consolidated into nine clusters reflecting nine broad policy areas of Government. These clusters bring together a group of entities to allow similar and complementary Government services to be coordinated more effectively within the broad policy area of a particular cluster. There are many different entities and governance arrangements within clusters and accountabilities can be unclear.[18]

Some agency submissions raised the issue of cluster structures and the entity of agencies within the cluster for the purpose of use and disclosure of information. The concern was whether sharing personal information between agencies with separate status within the same cluster, is a use rather than a disclosure for which consent may be required.

Practical issues depend this clarification for example, Transport for NSW felt if information sharing within the same cluster was categorised as a use, the privacy notice for use by agencies in the cluster could simply state that information supplied will be used within the cluster to fulfil the purpose for which it was supplied, or a directly related purpose.[19]

Section 4B of the PPIP Act provides that regulations may declare whether an agency is part of or separate from a public sector agency and sets out the requirements for such regulations. To avoid any doubt and confusion among agencies particularly in the context of the establishment of clusters of agencies, it would be appropriate to consider the making of a regulation under Section 4B.

Recommendation

7) The Privacy Commissioner confer with the Department of Premier and Cabinet and the Department of Justice about the making of a regulation under Section 4B of the PPIP Act clarifying which agencies are part of or separate from public sector agencies for the purposes of the PPIP Act.

18. NSW Department of Premier and Cabinet, *NSW Public Sector Governance Framework*, February 2013.
19. Transport for NSW, Submission to *Report on the Operation of the Privacy and Personal Information Protection Act 1998,* 2014.

5 Operation of the Act (continued)

5.3 Information Protection Principles

NSW privacy legislation as in many other jurisdictions, is principles based. Rather than seeking to prescribe each and every action that should be taken to protect privacy and personal information it sets down core elements, principles, as the best practice approach for NSW public sector agencies. The principles are based on those used by the former NSW Privacy Committee.[20]

The information protection principles (IPPs) in the PPIP Act and the health privacy principles (HPPs) in the HRIP Act provide guidance for agencies in relation to the collection, storage and security, access to and amendment of, use and disclosure of personal information and health records. Legislative exemptions from the IPPs provide for the particular needs of law enforcement and investigative agencies. Legislative provisions for Codes of Practice and Public Interest Directions provide mechanisms to modify the application of the principles for agencies' particular business needs. The latter provisions involve the Privacy Commissioner in ensuring the most privacy respectful modification of the application of the IPPs to these specific circumstances.

5.3.1 Harmonising jurisdictional information protection principles

The NSW Law Reform Commission in *Report 123: Privacy Principles* (Report 123) made recommendations in relation to the introduction of modified uniform privacy principles. A number of agencies also submitted that there would be administrative efficiencies in a single set of privacy principles that apply across Australia to both public and private sectors.[21]

Submissions from the Department of Education and Communities and Transport for NSW raise this issue as they engage with businesses and Commonwealth bodies that must comply with Commonwealth privacy laws. Other agencies, for example NSW Health however commented that this was not an issue as recent changes to Commonwealth legislation do not apply to NSW agencies.

While I support the notion of uniform privacy principles across Australia and the view of the NSW Law Reform Commission, the realities of achieving national agreement across States and Territories within a reasonable time frame is unlikely however desirable. Amendments to enhance privacy protections or facilitate service and policy reforms in the public interest should not be delayed while national uniform privacy principles are the subject of intergovernmental processes. I would be concerned also to ensure that current privacy protections inherent in the NSW information protection principles are not weakened or drafted in a way that potentially could create uncertainties or reduce privacy rights.

Some amendment of the PPIP Act's principles would achieve greater alignment between privacy regimes across jurisdictions. Other amendments would contribute to more appropriate, effective and efficient management of personal information within NSW public sector agencies.

5.3.2 Privacy by design

'Privacy by design' is an internationally recognised strategic approach to embedding privacy protection within agency operations in a 'win-win' manner. It embeds privacy and data protection throughout the entire life cycle of technologies and business processes, from early design stage to their deployment, use and disposal.

Typically privacy and the protection of personal information are afterthoughts in service and policy reforms and technology system developments. Privacy issues are invariably identified in the implementation phase resulting in less than best practice offerings to the public, failure to maximise trust and respect between the agency and its customers, and all too frequently, blaming of privacy for what is really a failure to adequately plan and manage privacy obligations. Because thought is not given to privacy protection at project commencement, the protection of personal information comes off badly as its frequently claimed that design modification for example, to remove unnecessary collection of personal information, is "too expensive" when initial analysis and planning could have avoided this.

Privacy Victoria in mid-2014 formally adopted 'privacy by design' as the required approach to avoid expensive retro-fitting technological solutions to ensure compliance with privacy legislation.[22]

20. The original principles were adopted as the Data Protection Principles to apply when dealing with complaints handled directly by the Privacy Commissioner rather than by oversight of agencies' internal reviews.

21. NSW Law Reform Commission, *Report 123: Privacy Principles*, (Report 123).

22. https://www.privacy.vic.gov.au/domino/privacyvic/web2.nsf/pages/privacy-by-design.

A number of agencies in their submissions commented on the lack of an overarching strategic focus in PPIP Act, and subsequent organisational blindness to ensuring systemic approaches to the protection of personal information and privacy. Establishing 'privacy by design' as the overarching principle IPP would assist in addressing these issues.

'Privacy by design' is a concept developed back in the 90's, by Dr Anna Cavoukian, Information & Privacy Commissioner, Ontario, Canada to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems. 'Privacy by design' advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organisation's default mode of operation.[23] 'Privacy by design' was recognised as the global privacy standard in a resolution by the International Conference of Data Protection and Privacy Commissioners in 2010.

Recommendation

8) The IPPs within the PPIP Act to include an overarching principle of 'privacy by design'.

5.3.3 Anonymity and pseudonymity

"I am concerned that for transactions of a mundane nature my date of birth is required. I think this is overkill. I would prefer that a less intrusive method of verification could be used."[24]

Over the 12 months issues have arisen in relation to individuals who object to the collection of personal information in order to obtain services. Other jurisdictions, for example the Commonwealth and New Zealand are addressing this issue by including provisions for the anonymity of individuals to be protected and/or for individuals to use pseudonyms to protect their privacy when lawful and practical.[25] Such provisions allow individuals to choose to remain anonymous or to use a pseudonym when providing information to government agencies in those situations where it is lawful and practical to do so when personal information is collected, stored, used and disclosed.

The NSW HRIP Act already enables this with HPP 13 providing "Wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves when entering into transactions with or receiving health services from an organisation".

In terms of ensuring alignment between Commonwealth legislation and the amendment of the PPIP Act to address this public concern, the Commonwealth *Privacy Act 1988* is the appropriate reference with Australian Privacy Principle 2 providing individuals with the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter where it is lawful or practical to do so.[26]

The statutory review of the PPIP Act undertaken by the Attorney General's Department in 2004 noted that the Commonwealth's then principles and the Victorian and Northern Territory IPPs all contained principles relating to anonymity, and recommended incorporating within the IPPs the right to anonymity in addition to regulating the use of unique identifiers.[27] Such an amendment has the benefit also of aligning NSW's privacy requirements with those of the Commonwealth as sought by a number of public sector agencies.

Recommendation

9) The PPIP Act be amended to include the principle of anonymity and pseudonymity where lawful and practicable, similar to Australian Privacy Principle 2 in the *Privacy Act 1988* (Cth).

23. Dr A. Cavoukian, *Privacy by Design. The 7 Foundational Principles.* Information & Privacy Commission, Ontario, Canada, https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf Revised: January 2011, originally published: August 2009.
24. Survey comment received from member of the public, 2014.
25. The NZ Government has indicated it will adopt the recommendation of the New Zealand Law Commission *Review of the Privacy Act, 1993. Reviewof the Law of Privacy Stage 4*, Report 123, June 2011.
26. *Privacy Act 1988* (Cth), Australian Privacy Principle 2 (Clause 2 Part 1):
    2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.
    2.2 2.1 does not apply if, in relation to that matter:
    (a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or
    (b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.
27. Op cit, Recommendation 9, p31, 2004.

5 Operation of the Act (continued)

5.3.4 Notification of privacy breaches

Currently when a breach of the IPPs occurs there is no requirement upon NSW public sector agencies to notify the Privacy Commissioner, or those individuals whose personal information is involved or third parties. Increasing use of and capacity of information technology increases the potential impact of a breach, particularly when 'big data' is involved.

Notification is an important mechanism to prevent or minimise potential consequences of a breach. Agencies' submissions raise the need to introduce notification of serious breaches of privacy. The Department of Premier and Cabinet for example suggested that amending the PPIP Act to provide for mandatory notification would ensure consistency across jurisdictions (if provided in Commonwealth legislation).

Mandatory notification raises issues such as when is notification appropriate if not in all incidents, and how to ensure notification is productive. Those supporting mandatory notification point out that not all agencies are open about such breaches and notify those affected, while those who see difficulties in mandatory notification, point to unnecessary concern and cost associated with notifying breaches that may have no or small risk to the individuals concerned. Proposed amendments to the *Privacy Act 1988* (Cth) to provide for mandatory notifications to apply only to 'serious breaches' have been under consideration at the Federal level.

Research undertaken by the Federal Privacy Commissioner found that 96% of Australians expect organisations to tell them if their personal information is lost.[28] Data over the period from 1 July 2013 to 30 June 2014 on complaints received by the Privacy Commissioner reveal that the majority concern disclosure of personal information suggesting that notification of breaches would be well received by the NSW public.

Public reporting of organisational performance is a valuable accountability mechanism. To increase accountability for management of personal information collected from NSW citizens the *Annual Reports Act 1984* and related Regulations should be amended to require reporting of serious breaches and actions taken to address and prevent further breaches. This is not sufficient as the sole mandatory action, as the annual reporting timing is unlikely to coincide with the occurrence of breaches and may not be adequately reported to serve as a notification to those whose personal information has been the subject of the breach.

Amending the PPIP Act to require in cases of serious breaches notification to those to whom the personal information relates is appropriate, with agencies assisted by the development of guidelines addressing the parameters of 'serious breach'.

Recommendation

10) The PPIP Act be amended to provide for mandatory notification of serious breaches of an individual's privacy by a public sector agency similar to that proposed to be provided in the *Privacy Act 1988* (Cth).

11) The *Annual Reports Act 1984* and related Regulations be amended to require reporting of serious breaches and actions taken to address the breaches.

5.3.5 Accessing personal information

An important privacy right for individuals is to know what information is held about them. The PPIP Act has two IPPs (6 and 7) relevant to this right. IPP 6 enables people to ascertain whether an agency holds personal information relating to them and IPP 7 provides access to that information (sections 13-14). Many complaints and internal reviews concern the inability to access personal information (see data later in this report on complaints and internal reviews).[29] Some of the complaints concern requests made under the PPIP Act being treated as a request under another piece of legislation and fees imposed.

Agencies also raised the various forms of access to personal information that currently exist and the administrative workload that arises from different definitions of 'personal information' and legislated access processes. Access to personal information is currently possible under both pieces of privacy legislation, the PPIP Act and the HRIP Act, the GIPA Act and the *State Records Act 1998*.

28. Op cit.

29. Under the HRIP Act many formal complaints concern access. In 2012, the proportion was 46%.

The PPIP Act (and HRIP Act) provide individuals with a right to both access and correct their personal (and health information) without the requirement for payment of a fee for access and correction of personal and health information. In contrast, the GIPA Act does not currently allow for correction of information, although it allows such information to be accessed. On the other hand, the GIPA Act requires the payment of an application fee for an application to be valid (although this can be waived).

In their responses to my invitation to provide comments and suggestions about the implementation of privacy legislation a number of agencies noted the overlap between the PPIP Act and the GIPA Act in relation to requests for access to personal information. Issues of concern to agencies include:

- Individuals often choose to seek access to their personal information under both the GIPA Act and PPIP Act adding to the workload and cost to agencies in considering such requests
- Applicants seeking access to personal information under the GIPA Act must pay for such a request while no application fee is required under the PPIP Act
- That someone has sought information under the PPIP Act does not exempt an agency from dealing with a similar request for access under the GIPA Act.

The overlap between the GIPA Act and the PPIP Act (and the HRIP Act) in relation to access to personal information was the subject of consideration by the NSW Ombudsman in 2009.[30] The NSW Ombudsman recommended that there be a clear distinction and separation between the GIPA Act and privacy legislation in relation to requests for access to personal information. Specifically the Ombudsman recommended that the PPIP Act deal with access to all personal information and health records while the GIPA Act deal with access to non-personal information.[31]

I support the clarification and simplification of NSW privacy and information access legislation as recommended by the NSW Ombudsman so that the PPIP Act covers the access to and amendment of personal information by NSW public sector agencies, and the GIPA Act covers access to non-personal information held by NSW public sector agencies. There is no necessity or utility in maintaining access to personal information via legislation concerned with government information.

I would be concerned to see the adoption of a proposed alternative approach to addressing the overlap between the GIPA Act, the PPIP Act and the HRIP Act in relation to access to personal information whereby access to personal information is only provided through the GIPA Act. This proposal would involve the removal of the provisions to access and correct personal and health information from the PPIP Act and the HRIP Act respectively and for access to personal information to be governed solely by the GIPA Act. This could reduce the capacity of NSW citizens to obtain information from private health services providers and has the potential to erode current privacy protections. I strongly oppose this.

The rights to access and to correct personal and health information are important privacy rights that need to be retained. The ability to obtain records without incurring a fee that currently exists under the PPIP Act is important and needs retention.

A different issue raised by an agency concerned updating the PPIP Act for electronic storage of personal information.[32] Specifically, section 10(f) of the PPIP Act requires agencies to inform people of the name and physical address of agencies involved in collecting and holding their personal information thereby advising which entity is responsible for the personal information. It's possible that the provision also assists to let individuals know where their personal information is held or where to lodge a request for access to personal information. With the formation of clusters and the introduction of 'one Government service centres' a closer examination of this issue and its connection to enabling individuals to know how to access the personal information held about them is indicated.

Recommendations

12) Access to and amendment of personal information be governed solely by the PPIP Act and that access to non-personal information (government information) be governed by the GIPA Act.

13) Consideration be given to amending the PPIP Act section10 (f) to reflect changes in technology for collecting and storing personal information and changes in service provision models.

30. NSW Ombudsman, *Opening Up Government. Review of Freedom of Information*, 2009.

31. The NSW Ombudsman also recommended that the PPIP Act be the single piece of legislation governing protection of privacy and personal information (including health information) in NSW.

32. Op cit, 2014.

5 Operation of the Act (continued)

5.3.6 Inter-jurisdictional or transborder disclosure

As outlined in my Annual Report tabled in October 2014, I have been working to increase the level of protection for personal information transferred out of NSW. Currently there is no protection under the PPIP Act for personal information moved out of NSW or to another Commonwealth agency within NSW's geographical boundaries. This is contrast to the privacy regimes of Victoria, Queensland, the Commonwealth and international jurisdictions where regulation governs the movement of personal information between jurisdictions.

Agencies such as Roads and Maritime Services, the Department of Family and Community Services and NSW Health have raised the need for protection for personal information transferred out of NSW.

Rather than a Privacy Code of Practice as required by the PPIP Act, the Attorney General has indicated the preferred option is to seek legislative reform to address the current lack of protection. I strongly endorse this proposed course of action.

I will continue to press this gap be addressed. Amendment has the added benefit for agencies of aligning NSW's privacy regime to that of the Commonwealth and other major states.

Recommendation

14) The movement of personal information outside of NSW or to Commonwealth agencies be protected by amendment of the PPIP Act in the manner of health privacy principle 14, Schedule 1, HRIP Act.

5.4 Exemptions and Codes of Practice

The PPIP Act provides mechanisms for the IPPs to be modified or not applied in activities of public sector agencies by way of:

- the definition of personal information (section 4)
- the functions of courts, tribunals and royal commissions (section 6)
- exemptions for law enforcement agencies (section 23)
- exemptions for investigative agencies (section 24)
- exemptions where non-compliance is authorised or required (section 25)
- exemptions where non-compliance would benefit the individual concerned (section 26)
- Specific exemptions (ICAC, ICAC Inspector and Inspector's staff, NSW Police Force, PIC, Inspector of PIC and Inspector's staff and NSW Crime Commission) (section 27)
- Other exemptions relating to the Ombudsman, Health Care Complaints Commission, Anti-Discrimination Board, Guardianship Board and Community Relations Commission (section 28)
- Modification of the IPPs by Privacy Codes of Practice (section 30)
- Exempting agencies from complying with principles and codes through Public Interest Directions (section 41)

'Public Interest Directions', as exemptions under section 41 are known, are the most common form of requests from agencies for variation in the application of the IPPs or Privacy Codes of Practice. Public Interest Directions are made with the approval of the Attorney General and only where the Privacy Commissioner is satisfied that the public interest in requiring the public sector agency to comply with the IPP(s) or Code is outweighed by the public interest in making the Direction. (The HRIP Act has a similar provision under section 62.)

There is no quantitative data on the usage of these exemptions other than feedback from agency privacy practitioners in which the majority (52%) reported that their agency did not utilise instruments such as the Public Interest Directions or Privacy Codes. Nearly one third indicated their agency did utilise these instruments (32%) while 17% did not know.

From 1 July 2013 to 30 June 2014, there were a total of five requests for exemption from the IPPs upon which

I consulted with the Attorney General and received his approval to make the following Directions:

- Department of Justice:
  - exemption under section 41 of the PPIP Act and section 62 of the HRIP Act to allow information sharing between participating agencies in the Youth on Track Program, a trial strategy to reduce juvenile offending through case management and early intervention. Two Public Interest Directions were made
  - exemption under section 41 of the PPIP Act for the Life on Track Program to enable the Department to collect personal information from NSW Police Force in order to contact individuals who may be eligible or suitable for the Life on Track program.
- The NSW Ombudsman:
  - the Investigative Functions Direction under section 41 of PPIP Act be expanded to allow non-compliance with section 18 of the PPIP Act in order for the agency to disclose information to a complainant for the purpose of reporting to them the progress of an investigation into a complaint made by that person; or to provide the complainant with advice on the outcome of the complaint and any action taken as a result of the complaint. The amendment was made as part of the broader review and renewal of the Public Interest Directions expiring 31 December 2013.
- Department of Family and Community Services:
  - for the disclosure of personal information to non-government organisations seeking personal information held by Community Services for the purpose of contacting individuals to market their services. The Privacy Commissioner was not satisfied that the public interest test was met.

During the period 1 July 2013 to 30 July 2014 nine section 41 PPIP Act Public Interest Directions were reviewed and renewed including:

- Direction on Processing of Personal Information by Public Sector Agencies in relation to their Investigative Functions
- Direction on the Disclosure of Information to Victims of Crime
- Direction on the Collection of Personal Information about Third Parties by NSW Sector (Human Services) Agencies from their Clients
- Direction relating to the Redfern Waterloo Case Coordination Project
- Direction for the Department of Family and Community Services and Associated Agencies
- Direction on Disclosures of Information by the NSW Public Sector to the National Coronial Information System
- Direction on Disclosures of Information by Public Sector Agencies for Research Purposes
- Direction relating to the Disclosure of Information to Credit Reporting Agencies, and
- Direction on Information Transfers between Public Sector Agencies.

These Directions were made on 23 December 2013 to commence from 1 January 2014 to 30 June 2015. In line with the recommendations of the NSW Law Reform Commission, I view Public Interest Directions as a short-term rather than an ongoing mechanism for exemption from the IPPs or privacy Codes. Where a case has been made for ongoing exemption, legislative or regulation change or development of a privacy Code of Practice is a better mechanism. The 2004 statutory review of the PPIP Act recommended that where necessary ongoing exemptions should be included in the Act or Regulations. The review went further to recommend that future variation to the Act for exemptions should be by way of Regulation only.[33]

Over the year and in the submissions to this report, difficulties with the Direction on Disclosures of Information by Public Sector Agencies for Research Purposes have been raised. This Direction was made some 15 years ago and the difficulties of understanding wording and coverage are real. As these exchanges are not a 'one off' occurrence, the better approach is to have the legislation amended to provide for the exchange of information for research purposes and other purposes similar to those listed in section 10 of the HRIP Act. The HRIP Act is regarded as providing a useful model suitable for adoption more generally. The 2004 statutory review of the PPIP Act also recommended that the exchange of information for research purposes be included in the Act or a Regulation made.[34]

33. Op cit, Recommendation 21, p59, 2004.
34. Op cit, Recommendation 15, p44.

5 Operation of the Act (continued)

The Department of Family and Community Services commented that PPIP Act Codes of Practice and Public Interest Directions might not be sufficiently broad to support cross agency service delivery and data sharing functions and sharing of information with NGOs.[35] It was suggested that a clear statement within the PPIP Act about the circumstances in which information can or should be shared is required.

The Department of Education and Communities raised issues arising from the operations of schools and their responsibility for student welfare and safety. These are complex issues involving students, parents, third parties as well as education professionals. As Privacy Commissioner, these are of concern to me and I will discuss with the Department the suitability of a specific Code of Practice to address the issues raised.

Recommendation

15) The PPIP Act be amended to provide for the use of personal information for research and other purposes similar to those listed in section 10 of the HRIP Act.

5.4.1 Specific exemptions from principles – law enforcement and investigative agencies

The Independent Commission Against Corruption, the NSW Police Force, the Police Integrity Commission and the NSW Crime Commission have important roles in our community. The application of privacy principles and legislation need to be applied carefully to such agencies so as to ensure a balance between facilitating the significant public value contribution made by such agencies and avoiding a 'secrecy' shield behind which government agencies hide.[36,37]

The PPIP Act has exemptions (Division 3) that seek to achieve this balance. These have been comprehensively examined in the NSW Law Reform Commission's report and recommendations made. During the period under review, the meaning of "law enforcement" and "administrative and educative functions" has been raised.

It is not possible within this report to examine this complex issue in detail but I acknowledge the NSW Law Reform Commission's recommendation that the Privacy Commissioner issue guidelines to assist in the interpretation of the legislation.[38]

Transport for NSW and Roads and Maritime Services sought clarification as to the interaction between law enforcement exemptions and the disclosure of personal information outside of NSW. This issue could be addressed by amendment of the transborder provisions of the PPIP Act referred to in section 5.3.6.

5.4.2 General issues

One agency suggested that the core protection principles in the PPIP Act would be strengthened if the language and structure were simplified, with the IPPs contained in a Schedule to the Act, as is the case with the HRIP Act. The statutory review of the PPIP Act undertaken by the Attorney General's Department in 2004 recommended that the PPIP Act be restructured using the HRIP Act as a model so that the IPPs and exemptions are set out in a Schedule to the Act.[39]

Recommendation

16) The PPIP Act be restructured to set out the IPPs and exemptions in a Schedule to the Act.

35. Department of Family and Community Services, Submission to *Report on the Operation of the Privacy and Personal Information Protection Act 1998,* 2014.
36. NSW Law Reform Commission, *Report 127: Protecting Privacy in NSW,* May 2010.
37. NSW Parliament, Hansard, Legislative Council, 17 September 1998.
38. Op cit, Recommendation 5.5., 2010
39. Op cit, Recommendation 2, p19.

5.5 Privacy Commissioner Functions

The Privacy Commissioner has a range of functions prescribed under section 36 of the PPIP Act (and section 58 of the HRIP Act).

These functions can be broadly divided into those championing privacy and addressing matters arising in the broader privacy landscape, and those concerned with assisting NSW public sector agencies.

In championing privacy generally, the statutory functions of undertaking inquiries and investigations, making public statements, publishing reports, conducting research and education, and recommending legislative, administrative or other action in the interest of the privacy of individuals, are critical. The PPIP Act singles out developments in technology in relation to reports and recommendations concerning legislative, administrative or other action in the interest of the privacy of individuals (section 36(2)(j)).

The Privacy Commissioner in assisting agencies has the statutory functions of, amongst other actions, publishing guidelines, promoting adoption and compliance with the IPPs and Codes of Practice, monitoring compliance, and initiating and recommending Privacy Codes of Practice. The majority of agencies want the Privacy Commissioner to issue guidelines to assist them to interpret and apply the IPPs. This was particularly requested for areas of consent, use, and disclosure.[40]

The Privacy Commissioner also has certain responsibilities under other pieces of legislation for example, the *Child Protection (Working with Children) Act 2012* section 40A in relation to exempt workers, and the *Road Transport Act 2013* section 57(2) in relation to approving protocols between Roads and Maritime Services and the NSW Police Force for the release of photographic images.

5.5.1 Championing privacy

The championing of privacy is particularly important in sector-wide policy, information communication technology and governance areas. Over the preceding year, the ever-advancing capacity of information technology has been a constant sector-wide matter and a constant theme in feedback from members of the public and agencies.

There is recognition within the NSW Government of the obligation to protect personal information. The 2012 *NSW Information Communications Technology Strategy* commits to strengthening electronic information security measures across the NSW public sector.[41] Similarly, the *NSW State Plan*'s commitment to promote the community's right to 'Open Government' has recognised that it is important to ensure appropriate safeguards are in place to protect privacy while enabling access to government information.[42]

Championing privacy will be most effective when it leads to cultural change within the NSW public sector and the broader community. I agree with the Department of Premier and Cabinet that promoting cultural change which emphasises the benefits of good practice personal information management as an organisational asset and important accountability will stand agencies in good stead in establishing trust with the community and restoring accountability to Government.[43]

In achieving this cultural change, key central agencies can facilitate the process. The Australian Public Service Commission has led federally by including privacy and the management of personal information in their *APS Values and Code in Practice*.[44] Similarly the Department of Premier and Cabinet and the Public Service Commission can assist in the adoption of a proactive privacy respectful culture; the Department through its leadership role for the NSW public sector governance and the Public Service Commission in its role in promoting and maintaining the government sector core values.

Championing privacy requires more than reliance upon regulatory powers; input into policy is critically important especially in the development of significant initiatives. Similarly, establishing privacy in the mainstream of public sector administration through incorporation in governance arrangements for government sector agencies and employees, in review mechanisms such as performance audits undertaken by the NSW Auditor General and other mechanisms are also important. As a small regulator with very limited resources, this is also likely to be a more effective approach.

40. Agency submissions responding to the invitation to provide feedback on the operation of the PPIP Act during 2013 – 2014.

41. NSW Department of Finance and Services, *2012 NSW Information Communications Technology Strategy*, May 2012, pps6,32-35.

42. NSW Government, *NSW 2021: A Plan to Make NSW Number One*, http://www.nsw.gov.au/2021, p58.

43. NSW Department of Premier and Cabinet, Submission to the *Report on the Operation of the Privacy and Personal Information Protection Act 1998,* 2014.

44. Australian Public Service Commission, *APS Values and Code in Practice*, www.apsc.gov.au/publications-and-media/current-publications/aps-values-and-code-of-conduct-in-practice

5 Operation of the Act (continued)

As Privacy Commissioner I am frequently called on to comment on proposed new policies, business processes and technology solutions for an individual agency, a number of agencies or whole of government. Sometimes I am approached at point of planning for the new policy, business process or technology solution. At other times I am approached after the solution has been developed. The Department of Finance and Services (now Office of Finance and Services within the Treasury portfolio) has consistently sought input in a proactive manner as has some other agencies such as Service NSW.

Intertwined with cultural change is the capacity and capability of the public sector. The Department of Premier and Cabinet pointed to work identifying the limited knowledge and understanding and in some cases, misinformation and misunderstanding of privacy legislation in relation to information sharing. The Department suggested a review of agency and cluster capacity and capability in relation to information sharing and exchange could be conducted, particularly as they relate to the interpretation and application of privacy legislation, and that further measures could be introduced such as capacity building reform or enhanced enforcement powers under legislation to address serious systemic issues. I agree with this suggestion and recommend accordingly.

The awareness of the public to privacy risks and their responsibility for protecting their personal information and that of family and friends is raised through events such as Privacy Awareness Week, and international days for example Data Privacy Day. Public speaking and media engagements are also valuable in this regard. The loss of the Commission's training and education position in 2013 due to budgetary saving requirements has been sorely felt. While training activity does continue, it is more *ad hoc* and reactive and consequently, less likely to be as effective. This is of concern to me. Raising the awareness of privacy generally is a statutory function of the Privacy Commissioner.

Recommendation

17) The Public Service Commission, in conjunction with the Privacy Commissioner, undertake a review of agency and cluster capacity and capability in order to identify strengths and limitations and develop strategies to develop staff to meet the customer needs in management of their personal information.

5.5.1.1 Information technology security

In the information technology and 'big data' era, protection of personal information relies upon rigorous management of personal information.

The Auditor General stated in 2010:

> "The public sector legitimately gathers and uses personal information about citizens, and shares it within and outside government. But personal information can be misused with potentially serious consequences. If the wrong people get access to sensitive personal information an individual can suffer financial loss or damage to their credit rating, have their medical records compromised, or suffer from threats and harassment.
>
> The people of NSW have every right to expect their and their families' private details are secure regardless of which government agency holds it."[45]

Privacy legislation requires sensitive information collected from the public not to be divulged to unauthorised persons and only used for the purposes agreed by the subject. This places a duty of care on the agency collecting such data to ensure that adequate safeguards are in place for their information (and other) systems to prevent its unauthorised disclosure.

The Auditor General's 2010 report highlighted the need for "clear, mandatory, minimum standards that agencies sign up to, scrutiny of performance against these standards."[46] In response, the Information Security Guideline was introduced to require NSW Government agencies to establish and maintain their Information Security Management System (ISMS) in compliance with AS/AZS ISO/IEC 27001:2005 *Information technology – Security techniques – Information security management systems – Requirements (ISO 27001).*[47]

In this context and as technology continues to evolve and social norms or 'cyber manners' and legal frameworks struggle to keep pace, it is imperative that agencies not only adhere to government standards for the storage and security of data but that they also undertake periodic testing of information technology for possible privacy breaches as an inherent part of their risk management strategy.

45. NSW Auditor – *General's Report, Performance Audit, Electronic Information Security*, October 2010.
46. Ibid.
47. NSW Government, *Premier's Memorandum M012-15 Digital Information Security Policy*, November 2012.

The NSW Government has addressed a number of risks to personal information through policies such as its *Social Media Policy* and the *Bring Your Own Device (BYOD) Policy*.

Good information or records management practices lead to good management of personal information. The creation, management, protection and ultimate retention or disposal of the records generated in the course of everyday business whether paper or electronic is primarily concerned with the evidence of an organisation's activities. This is not an inconsequential activity and is closely interrelated with the protection of personal information.

The NSW Government *Information Classification and Labelling Guidelines* support the *Digital Information Security Policy*. The Policy requires that all information classified on or after 1 January 2014 will be classified in a manner consistent with the Australian Government security classification system. These guidelines apply to the classification and labelling of information in any format, including records in physical and digital format. This is a valuable initiative however the Guidelines pose some issues in relation to personal information.

The issues raised by agencies include the reference to the Commonwealth *Privacy Act 1988* in the list of Distribution Limiting Markers as confusing agencies as to the application of Commonwealth privacy legislation. Another issue raised is that the current guidelines do not separately address health information. Health information is classified as "Sensitive: Personal". NSW Health advised it is considering whether a submission should be made recommending a separate dissemination-limiting marker for personal health information, consistent with NSW HRIP legislation.[48]

In presentations to public sector agencies and private sector organisations throughout the year I emphasised that good records management is integral to leading privacy management practice and effective corporate governance.

In early 2015, the NSW Audit Office will table a performance audit report on the security of IT systems examining whether agencies have implemented appropriate and effective controls over IT system security and integrity including databases containing private and confidential information. I will read this report with interest to see what findings and recommendations are made and which may require follow up from my office.

5.5.1.2 Cloud computing

Developments in technology now allow data to be stored and processed in "the cloud". The cloud consists of massive data bases maintained by well-known large corporations as well as smaller lesser-known companies. The benefits of cloud computing stem from its usefulness, value for money, flexibility and reliability but it has significant implications for privacy.

Cloud computing does not need to be a 'privacy hazard'. A rigorous accountability framework and sound operational practices are effective risk management strategies.

In terms of governance requirements, in 2014 the then Department of Finance and Services introduced a draft *NSW Government Cloud Service Policy and Guidelines* to facilitate the acquisition of cloud-based solutions. The inclusion of the ISO/IEC 27108 standard introduced in mid-2014 to cover privacy, security and cloud services in the NSW Government's *Information Security Management Systems Policy* and *Cloud Services Policy and Guidelines* are possible mechanisms to strengthen cloud services providers' capacity to meet agency needs while ensuring privacy protection.

Operationally, it is critical that agencies undertake due diligence of the cloud provider's credentials, security and privacy frameworks, and their previous compliance record with relevant legislation before considering entering into contracts. It is also critical that contractual arrangements and provisions embed privacy and data protection in relation to collection, custody and ownership, use, storage, access to, disclosure and sharing of the information, business continuity, data disposal and exit strategy. Processes and accountabilities relating to the management of privacy issues and complaints that might arise during the contract term also need to be thought through, clearly documented and communicated to agency staff, cloud provider personnel and affected clients. Contractual arrangements should be subject to periodic audits as part of agency Audit and Risk plans and a broader whole of government review of the *Cloud Services Policy* undertaken by the Office of Finance and Services.

While a new and emerging technology such as cloud computing can pose potential risks to privacy, there are

48. NSW Department of Premier and Cabinet, Submission to *Report on the Operation of the Privacy and Personal Information Protection Act 1998,* 2014.

5 Operation of the Act (continued)

a range of technological and other solutions including international standards that can be employed to mitigate privacy risks and promote compliance and good practice. In mid-2014, a specific international standard was introduced for privacy, security and the cloud which has potential to provide cloud clients with the necessary information on how information moved to the cloud is safeguarded and processed, and what happens if they move to another provider or their provider terminates its operations or changes the terms of its policies.

Recommendations

18) ISO/IEC 27018 standard covering privacy, security and cloud services be considered for inclusion in the NSW Government's *Information Security Management Systems Policy*.

19) The Privacy Commissioner in conjunction with the Office of Finance and Services develop model clauses for inclusion in cloud computing contracts to ensure the protection of privacy and personal information, covering the collection, custody and ownership, use, storage, access to, disclosure and sharing of the information, business continuity, data disposal and exit strategy.

20) Agencies include periodic audits of the implementation of the NSW Government *Cloud Services Policy* in their audit and risk plans.

21) The Auditor General conduct a post implementation review of the NSW Government *Cloud Services Policy* within two years of date of commencement of the policy in which privacy management and compliance is a component of the review.

5.5.1.3 'Big data' requires 'big privacy'!

A comment received from a member of the public was:

> "The power of big computing – big data, data analytics, data sharing – does have a real role in improving services, improving outcomes – but it does contain some genuine risks in terms of greater governmental controls/intrusions (and subsequent losses of freedom)."[49]

As we have seen from media reports, highly personal 'big data sets' are a prime target for hackers and criminal elements. But more regularly, data breaches arise from within an organisation – either from human or computer error.

The evolution of information communication technologies have given rise to new challenges in ensuring the protection of privacy and personal information by public sector agencies, private sector organisations and individuals and to new forms and expressions of governance – one of which is information governance.

In the past, some of the chief protections for privacy were that it was just so difficult to collate and link personal information. In 1996 the Hon. Michael Kirby observed:

> "Some of the chief protections for privacy arose from the sheer costs of retrieving personal information, the impermanency of the form in which that information was stored; and the inconvenience experienced in procuring access (assuming its existence was known)."[50]

The advent of 'big data' holding vast amounts of information for a digital eternity, has removed these *ad hoc* safeguards.

Agency submissions reflect mixed perceptions around 'big data'. On one hand, agencies indicated concerns around the risks posed by 'big data' and data mining but at the same time raised concerns that the advantage to policy development and services planning would be lost if the ability to collate and interrogate data, including personal information, was not appropriately used.

The Department of Family and Community Services observed that the growth of big data and techniques for processing data makes it easier to identify individuals from a relatively small number of de-identified data items and warned of the potential for inadvertent disclosure of personal information through the release of big data, for example where disparate datasets, individually de-identified, could potentially be linked or combined to re-identify individuals, resulting in a disclosure of personal information.[51]

The risk of inadvertent disclosure of personal information through the release of big data was seen to be potentially exacerbated in situations where responsibility for open government and open data differs, or is located within

49. Survey comment received from member of the public, 2014

50. The Hon. Justice Michael Kirby in *Privacy and the Cyberspace International Council for Computer Communication*, ICCC Newsletter, 1996, p5.

51. Op cit.

a number of different functional areas within an agency (such as across ICT, Communications, Records or Information Access), and not managed in the context of the NSW Government's parallel commitment to maintaining protection for personal information. The risks also increase when there are inconsistent approaches or poorly developed approaches across government to sharing information.

It is imperative that public sector agencies be required to report possible 'big data' breaches of privacy and protection of personal information to the Privacy Commissioner. An earlier recommendation on mandatory notification of serious breaches of privacy has been made. A remaining issue concerns the ability to be able to investigate such breaches. Current resourcing is neither keeping apace with requests for assistance from agencies nor the handling of complaints. My ability to conduct urgent investigations into major breaches is extremely limited; yet such breaches are likely to be high profile and of a serious nature. It is important that adequate resourcing is available if such investigations need to be undertaken.

Recommendation

22) The Privacy Commissioner's ability to conduct urgent investigations into large-scale breaches of public concern be enabled by provision of additional resources on a one-off basis for this specific purpose.

5.5.1.4 Surveillance

A member of the public commented:

> "The impact of the psychology of people born into a society that surveils all its citizens does not seem like a healthy direction..."[52]

This comment reflects some of the concerns felt by the community about surveillance. Developments in technology such as security cameras, technology devices and drones have facilitated the physical surveillance of individuals in private and public locations, often unbeknown to the individual under surveillance.

In the survey responses received from the public, surveillance is a major privacy concern and driven by a broad range of triggers. The introduction for example of the Opal electronic transport card has been seen by some as enabling the tracking of private citizens going about their ordinary lives.[53] Communications around the ability to purchase unregistered cards or to travel without personal information linked to the card's use either has not occurred sufficiently widely or not been understood as concerns about providing identifying information to Opal enabling links to people's activities, financial arrangements and travel movements were raised.

I receive numerous concerns from members of the public about the use of surveillance devices not just in public places but also in private settings and by private individuals such as neighbours. Workplace surveillance is a topic also frequently raised. While integrally related to privacy, workplace surveillance is covered by separate legislation, the *NSW Workplace Surveillance Act 2005*. The enquiries and complaints regularly received about surveillance in the workplace revolve around concerns of unreasonable intrusion into the personal lives of employees through CCTV, computer and tracking technologies such as Global Positioning System (GPS) and monitoring of employees' email and internet access and usage.

Local councils have raised questions around their ability to use surveillance devices and best practice in doing so. The Parliamentary Committee oversighting the performance of the Privacy Commissioner has sought advice specifically on 'drone surveillance'.

While the PPIP Act does not provide protection of privacy and personal information in private situations, it does provide protection where the information is collected, stored, used and disclosed by public sector agencies. The intent of the Act includes the "protection of the privacy of individuals generally". In the case of law enforcement usage, although the PPIP Act exempts NSW law enforcement and investigation public sector agencies from the IPPs for purposes of law enforcement and investigation, it is imperative that the collection, storage, use, disclosure and disposal of personal information captured by such devices comply with the spirit of the PPIP Act in that the information is only collected for lawful purposes, is stored securely, is used and disclosed only for the purposes for which it was collected and is disposed of as soon as practical.

52. Survey comments received from members of the public, 2014.

53. Ibid, 2014.

5 Operation of the Act (continued)

The former Administrative Decisions Tribunal (ADT), now the NSW Civil and Administrative Tribunal (NCAT), considered surveillance in public places in 2013 in a matter involving the use of CCTV cameras by a Council to capture photographic information on individuals for security purposes. The Tribunal found that the collection of this personal information by these means and use of the information for these purposes without the consent of individuals the subject of the surveillance, was in breach of the PPIP Act. Subsequently the NSW Government through Regulation changes allowed Councils to collect information using such devices and for such purposes without being in breach of NSW privacy legislation.

A recent United Nations human rights report examined the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale. The conclusion was there is a clear and pressing need for vigilance in ensuring the compliance of any surveillance policy or practice with international human rights law, including the right to privacy, through the development of effective safeguards against abuses. The report also pointed out that other rights may be affected by mass surveillance, the interception of digital communications and the collection of personal data, including the rights to freedom of opinion and expression.[54]

The guidance or rather, lack of guidance on surveillance provided by the Privacy Commissioner was raised, as captured by the following concern: "The lack of information on the IPC website about surveillance laws and responsibilities by public sector agencies, other than local councils."[55]

Surveillance takes a variety of forms from the caring concern of a neighbour who may closely watch their next-door neighbour through to authorities watching 24x7 an individual who poses a threat to public safety. To determine where along this continuum surveillance is appropriate is not necessarily easy and agencies need clarification on their obligations. As Privacy Commissioner, I recommend that the following principles guide decisions on the deployment of surveillance:

- There is adequate justification for any reduction in the privacy of the individual or community arising from the use of surveillance
- The surveillance deployed is proportionate to the risk identified
- There are protections against compromising the privacy of third parties
- The surveillance is appropriate, efficient and effective in terms of the expenditure of public money
- There is independent scrutiny and evaluation
- Where appropriate, people are informed personally of the surveillance or where this is not practicable, through other forms of communication
- The material gained through surveillance is securely stored and available to only those who have a valid reason to use it and it is destroyed when it has no further use
- There is a set period for review to examine the case for continued deployment.

Given the rapid advancement of the use of technologies for surveillance it is imperative that guidance is provided.

Recommendation

23) The Privacy Commissioner prepare guidelines on the use of surveillance technologies.

5.5.1.5 Firearm regulation and risks to individual privacy and public safety

A significant number of respondents to the survey of the public in October 2014 expressed concern at privacy issues relating to the additional requirements added to the *Firearms Act 1996* relating to the supply of ammunition. This concern was unexpected, as the matter had not been raised throughout the year. The Shooters and Fishers Party also made very detailed representations on this issue and the administration of the Firearms Registry by NSW Police.

The primary reported privacy concern was the risk to firearm owners and the broader community arising from the operational implementation of the requirement for retailers of ammunition to maintain a register of sales of ammunition that includes the name and address of purchasers of ammunition. These registers are said to be regularly stored insecurely and that in

54. United Nations, *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, A/HRC/27/37, June 2014

55. Survey comment received from member of the public, 2014

many cases information is recorded manually in registers left open on shop counters and accessible to other purchasers of ammunition and potentially other members of the public in general. As a consequence, the possibility of people having access to the names and addresses of purchasers of ammunition is seen to place purchasers at risk as targets of potential theft of the firearm(s), ammunition or household belongings. Representations also suggested that the collection of the personal information (names and addresses of ammunition purchasers) is not necessary as such details are already recorded for firearms licence holders and that the only record of purchase required should be the firearm licence holder number. The views strongly expressed were that the information collected intruded unreasonably on the personal affairs of the individual concerned. In relation to the administration of the Firearms Register, the concerns were also that personal information is not stored securely, is too widely accessible and that previous concerns raised have not been adequately addressed.

The concerns relate to the IPPs for collection, disclosure and secure storage of personal information. In relation to the management of personal information involved in the sale of ammunition by retailers, Commonwealth privacy legislation rather than the PPIP Act applies. The NSW Police Force has broad exemptions for law enforcement functions but I am mindful however of the possibility of unintended consequences to the safety of individuals and the community. I'm concerned to ensure that the arrangements for the collection, security and storage, access to, use and disposal of personal information relating to the purchase of ammunition or registration of firearm ownership address any privacy risks including those that may lead to safety risks for individuals and the community.

Accordingly, I have raised with the NSW Police Commissioner the feedback received to ensure that the Firearms Register and implementation of provisions relating to the sale of ammunition reflect the IPPs insofar as is possible without adversely affecting law enforcement. A performance audit by the Auditor General's office may be an appropriate mechanism to assess whether the public policy aims have been achieved and the management of any risks that may be emerging.

Recommendations

24) The NSW Police Force review the processes and systems relating to the register of firearm ammunition purchases to ensure compliance with relevant legislation relating to the register while ensuring the protection of the privacy and personal information of purchasers.

25) The Privacy Commissioner to raise with the NSW Auditor General the inclusion of this matter in the forward performance audit program of the Audit Office.

5.5.1.6 The 'shared economy'

An emerging issue raised through the consultation was the issue of 'shared economy'. It was drawn to my attention that the use of 'shared economy' services has increased markedly and merits inclusion as an issue to be monitored from a privacy perspective.

The large and growing new 'shared economy' where people order taxis, rent beds, cars, boats and other assets directly from each other, co-ordinated via the internet, is hugely popular according to reports.[56]

Companies collecting personal information from individuals are likely to be covered by an established privacy regulatory framework, but the protection of the privacy or personal information of individuals doing business either directly or indirectly with individuals or smaller companies involved in the 'shared economy', is uncertain. It's unclear what privacy regulation applies to such transactions and what protections and recourse individuals have if their personal information is treated in a manner different to what was agreed or understood. Commonwealth privacy legislation may more likely apply.

The point has been made however, that some public sector agencies may need to examine their regulatory role in relation to services provided by the 'shared economy'. From the privacy perspective it's important that the regulatory framework includes appropriate management of the personal information and privacy. And while it seems unlikely, if NSW public sector agencies intend to use 'shared economy' services they

56. The Economist, *The Rise of the Sharing Economy: On the Internet Everything is for Hire*, 9 March 2013.

5 Operation of the Act (continued)

need to be satisfied that the arrangements meet the information protection principles of the PPIP Act and that such obligations are documented in contractual provisions and subject to monitoring and review.

The privacy impacts generally of the 'shared economy' warrant monitoring. The Privacy Commissioner meetings both nationally and with international jurisdictions can assist the examination of the privacy impact of services provided through the 'shared economy'. Possible future action if required might entail for example, the Privacy Commissioner in conjunction with the Office of Finance and Services developing model clauses for contracts with shared economy providers to ensure the protection of privacy and personal information. Such model clauses should cover the collection, custody and ownership, use, storage, access to, disclosure and sharing of the information, business continuity, data disposal and exit strategy.

I will report further on this issue if it poses a risk to privacy.

5.5.2 Assisting NSW public sector agencies

5.5.2.1 Public sector agency accountability for privacy management

It is clear from the PPIP Act and the second reading speeches accompanying the introduction of the legislation, the NSW Parliament intended the protection of privacy and personal information to be integral to the functions and operations of public sector agencies.[57] It is also clear from annual report legislation that the Parliament expects agencies to be accountable for and report on action taken to ensure compliance with privacy legislation.[58] These expectations are reflected in the requirement for all agencies to develop and publish privacy management plans and to describe in their annual reports actions taken to ensure privacy protection. A summary of actions reported by agencies in their annual reports for the 2012 – 2013 year is provided in Attachment 5.

The functions of the Privacy Commissioner are designed to assist agencies as well as championing privacy generally. The submissions from Secretaries reinforce this need and also highlight that agencies feel that more could be done by the Privacy Commissioner to assist them acquit their responsibilities proactively. This request echoes that received from practitioners for more training. Their point is justifiable, however the ongoing lack of resources has prevented the provision of assistance to agencies to the level sought.

Agencies identified the need for guidance from the Privacy Commissioner in relation to a range of matters including:

- How the various pieces of legislation including the PPIP Act, HRIP Act and the Commonwealth *Privacy Act 1988*, apply to agencies; which agencies have obligations to comply with which IPPs and which agencies are permitted to depart from which IPPs because of exemptions in the PPIP Act, Codes of Practice and Public Interest Directions; which, if any, Australian Privacy Principles apply to agencies
- How NCAT decisions and the NCAT's interpretations of the law apply to agencies in different situations
- Best practice in relation to interagency exchange of information with a focus on:
  - Obtaining consent
  - Examining the purpose of the information exchange/release
  - Custodianship during and after data release/use
  - Appropriate de-identification mechanisms
  - Data brokerage services
  - Security and communication processes
  - Processes for managing unforeseen uses of exchanged data.

Suggestions on how the Privacy Commissioner might assist agencies included:

- Development of a tree diagram including legal requirements and elements of good practice, supported by interactive and digital tools, additional face to face training and case studies
- Provision of advice by the Privacy Commissioner on the impact of case law on interpreting the privacy legislation. The Department of Education and Communities commented that case law is an important source for interpreting the privacy legislation and it would assist the Department if an annotated version of the PPIP Act or other documentation of the direction of case law was available

57. NSW Parliament, Hansard, Second Reading Speech, Legislative Assembly, 17 September 1998.

58. *Annual Reports (Departments) Act 1985* and *Annual Reports (Departments) Regulation 2010*.

- The identification of recurring issues and guidance on how to address these
- Regular bulletins on recurring issues and other developments in the privacy area.

As Privacy Commissioner I agree that the assistance provided to agencies has not been to the level required in this era of rapid technological change. It is of concern to me that through an inability to meet the stated needs of agencies, there may be a lesser level of privacy protection available to individuals and the community or a reduction in the accountability for such protection.

The *Privacy Governance Framework*, which I launched in November 2014, is designed to promote a culture of privacy respect and protection from the highest levels in public sector agencies. The Framework is an online privacy tool that will assist Secretaries and senior management to implement a 'privacy by design' approach to move beyond compliance to proactively winning the trust of stakeholders, staff and customers. It provides a foundation for agencies to understand privacy legislation, the relevant references and their obligations.

The existence of the Framework also provides a means to address the additional guidance sought by agencies on the privacy legislative landscape and clarification of the roles and expectations of agencies in relation to privacy management. To meet agency needs, the framework needs to be further developed to include examples of leading practice, summaries of NCAT decisions and their implications for agencies as well as interactive tools and training resources as suggested by agencies. Further development will facilitate the integration of privacy management in the corporate governance and culture of public sector agencies.

Privacy governance does require attention. While one agency commented their privacy complaints management has informed continuous improvement of business processes and systems, only 7% of practitioners reported in the preceding year that the Audit and Risk Committee work program undertook any performance reviews on privacy compliance or data collection systems. Further, 77% reported that no privacy impact assessments were undertaken during 2013 – 2014.[59]

Recommendation

26) The *Privacy Governance Framework* developed by the Privacy Commissioner be further developed to:
   a) include examples of leading practice, interactive tools and training resources and summaries of NCAT decisions and their implications for agencies
   b) provide guidance for public sector agencies as to the matters to be included in their annual reports on the implementation of privacy legislation.

5.5.2.2 Changing nature of government and service provision

Roads and Maritime Services noted that the recent Government policy has been to view customers as a single customer seeking to be provided with "government services" from a variety of government service providers fronted by Service NSW.[60] The notion of a 'one government customer' is an issue warranting examination of how the PPIP Act relates to the concept of a single customer with multiple service providers. This issue was raised also by Transport for NSW.[61]

This is an important initiative with important public policy and privacy considerations relating to consent, collection, sharing of personal information and other IPPs. I support steps taken by the NSW Government and its agencies to improve service provision to the people of NSW. Many in the community and in agencies would welcome improvements in the ease and efficiency of interactions with public agencies. It is important to me as Privacy Commissioner, that these aims are achieved without reduction in the privacy protections owed to service users and associated third parties.

Recommendation

27) The alignment of the PPIP Act and emerging service provision models particularly of 'one government customer' be examined and a report prepared if amendment of the PPIP Act is indicated.

59. Privacy Practitioner Survey undertaken in the preparation of the *Report on the Operation of the Privacy and Personal Information Protection Act 1998,* 2014.

60. Op cit.

61. Op cit.

5 Operation of the Act (continued)

5.5.2.3 Consent

Consent is an important concept in privacy as it allows individuals to exercise a degree of control over their personal information and the ability to decide how much personal information will be provided to others. This is a significant issue as the ability to collect, use and disclose personal information has grown exponentially with advances in communication technologies.

Consent is key mechanism in building trust between individuals and Government. Rebuilding trust was an important plank in the NSW Government's 2011 *State Plan 'NSW 2021'*. The Department of Premier and Cabinet identified the benefits flowing from building trust through obtaining consent and suggested that guidance material could be developed to assist agencies in understanding how to obtain consent.[62] Roads and Maritime Services also commented on the importance of gaining customer consent to the use and disclosure of personal information at the point of collection, particularly from the perspective of the formation of agency clusters and the establishment of NSW Service Centres with a single customer model.[63]

The Australian Law Reform Commission's *Report 108* identified the meaning and elements of consent, which included 'express consent or implied consent', and the requisite elements consent that must be met.[64] These were identified as voluntariness, capacity to understand, provide and communicate. The Australian Law Reform Commission (ALRC) stated that whether consent is voluntary depends on whether the individual has a clear option not to consent.

The ALRC's report discussed 'bundled consent' noting that it was difficult to give free and informed consent when presented only with broad or vague statements concerning possible use or disclosure, or when told that services would not be provided in the absence of consent.

Agencies and individuals over the past twelve months have sought advice or raised issues with 'consent'.

Recommendation

28) The Privacy Commissioner develop and publish guidance on the requirements of consent.

5.5.3 Sharing 'personal information' for policy analysis and planning purposes

A number of agencies raised perceived limitations of the PPIP Act and existing Codes of Practice in supporting data sharing and information exchange necessary for their agency's service delivery functions and responsibilities. I acknowledge cross agency initiatives and the 'one government customer' service model would be assisted by the ability to analyse service usage data. I am concerned however, that this occurs within a framework of appropriate protections for the privacy and personal information of individuals. Some of the issues involved are related to those discussed in 'Big Data'.

Frequently, de-identification of personal data into aggregated data sets is seen as the solution. At the same time that the capacity of technology has advanced to enable the storage of vast quantities of data and the analysis of the same, so too has the ability to re-identify individuals through sophisticated algorithms that enable 'constructive re-identification'.

NSW Health identified some central operational concerns:

- confidence that personal information is sufficiently de-identified when using or disclosing information for purposes other than that for which the information was collected
- assurance that security controls are in place which effectively protect personal information in the increasing number of data collections storing personal information for a multitude of management purposes
- assurance that data linkage issues which arise within the health system, and with data linkage systems with other agencies, are proactively identified and addressed early.[65]

The Department of Family and Community Services also expressed the view that methods currently used for

62. NSW Department of Premier and Cabinet, Submission to *Report on the Operation of the Privacy and Personal Information Protection Act 1998,* 2014.
63. NSW Roads and Maritime Services, Submission to *Report on the Operation of the Privacy and Personal Information Protection Act 1998,* 2014.
64. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice (ALRC Report 108),* August 2008.
65. NSW Ministry of Health, Submission to *Report on the Operation of the Privacy and Personal Information Protection Act 1998,* 2014.

de-identifying personal data might not provide effective protection for personal information and may not avoid the legislative protections that extend to personal information about individuals whose identity can reasonably be ascertained. The Department suggested that the Privacy Commissioner could promote anonymisation standards and methods that agencies could confidently apply to data sharing in compliance with the PPIP Act.

The Canadian Ontario Privacy Commission has increased the profile of methodologies that reliably de-identify personal information for data linkage and sharing. There would be significant public policy value in a project to identify and investigate methodologies that enable the safe use of personal information in de-identified, aggregated data sets.

It is also appropriate that the Privacy Commissioner in conjunction with relevant agencies such as the Department of Premier and Cabinet and the Office of Finance and Services, undertake research and provide guidance to agencies on appropriate and acceptable methodologies for de-identifying data and linking data so as to protect the privacy and personal information of individuals. Possible mechanisms such as a Privacy Code of Practice should be included in this examination if a need is identified.

As Privacy Commissioner I welcome initiatives to improve service provision and increase the accuracy of planning and success of public policy development. It is important to me as Privacy Commissioner, that these aims are achieved without reduction in the privacy protections owed to those whose personal information (and possibly of third parties) is used in such projects. I maintain that protecting privacy while using personal information for planning, policy development, research, service delivery and quality improvement purposes is critical to public confidence in government administration.

The 2004 statutory review of the PPIP Act saw the issuing of guidelines as one way to address this issue.[66] A Code of Practice comprising a reliable methodology could be an effective mechanism also.

66. NSW Attorney General's Department, *Review of the Privacy and Personal Information Protection Act 1998*, p59, 2004.

Recommendations

29) The Privacy Commissioner in conjunction with relevant agencies, establish a project to identify and investigate methodologies that enable the safe use of personal information in de-identified, aggregated and linked data sets so as to protect the privacy and personal information of individuals.

30) The appropriateness of a Code of Practice to enable information sharing for planning and policy analysis purposes between agencies be examined and developed if such a need is demonstrated.

5.5.3.1 Exchange of information for child protection purposes

Two Departments raised issues relating to child protection. The Department of Family and Community Services commented that existing provisions in child protection legislation relating to the exchange of information between agencies may not be adequate to exempt the Department and associated agencies from privacy legislation. There has been an increasing use of memoranda of understanding and protocols for the exchange of information. While such mechanisms serve a useful function they do not and cannot override privacy laws provisions for collection, use and disclosure of personal information. The Department also observed that while Privacy Codes of Practice under the PPIP Act (and HRIP Act) can be used to authorise exchange of information with other government and non-government organisations, such provisions have been underused to date.

The Department of Education and Communities raised issues in relation to the interaction between the information sharing provisions under Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998* and the PPIP Act including the lack of understanding that Chapter 16A overrides the PPIP Act. The Department recommended that a note be inserted in the PPIP Act to refer to Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998* to confirm that it overrides PPIP Act and that consideration be given to including in the PPIP Act provisions similar to those in Chapter 16A, to enable agencies which provide services to clients to exchange information in relation to a person's safety, welfare or wellbeing.

5 Operation of the Act (continued)

Recommendation

31) The Departments of Family and Community Services and Education and Communities confer with each other and the Privacy Commissioner in relation to the development of a Code of Practice for the exchange of information in relation to the management of child protection issues.

5.5.3.2 The impact of organisational restructures

A number of agencies commented on the impact of organisational restructures on privacy management in their agencies, particularly the formation of agency clusters. This ranged from practical issues such as developing whole of Department Privacy Management Plans to replace separate plans for each agency within the cluster, through to compiling a schedule of protocols with clauses for renewal and databases containing personal information.

The NSW Ministry of Health advised that privacy is factored into health structural reforms, strategy and planning and operational service delivery initiatives. Dedicated privacy officer positions have been established at all tiers of the new structure for delivery of health services throughout NSW to ensure that privacy is integral to service planning and delivery.

The Department of Family and Community Services commented that organisational restructures can impact on how agencies are defined and consequently how Codes of Practice and Public Interest Directions apply to them. Agency comments reinforce the importance of considering privacy management in organisation restructures including clarifying functional areas and positions with responsibility for privacy management and reviewing relevant instruments such as Codes of Practice and Public Interest Directions to ensure alignment with the new structure and business needs of the agency.

It has been raised with me there is a greater risk of privacy breaches as restructures occur and staff are dislocated, sometimes alienated and who as a result, either neglect their responsibilities for appropriately managing personal information or depart with personal information incompletely deleted from electronic devices. I am aware of these risks and as Privacy Commissioner, they are of concern to me.

The protection of personal information and data needs to be a formal part of administrative arrangements underpinning organisation restructures. Change management plans need to clarify functional areas and positions with responsibility for privacy management and review of relevant instruments such as Codes of Practice, Public Interest Directions and Privacy Management Plans to ensure alignment with the new structure and business needs of the agency as required.

5.5.4 Provisions enabling the Privacy Commissioner to obtain information from agencies

The ability to obtain relevant information is critical for undertaking the functions of the Privacy Commissioner particularly inquiries, reviews and investigations. Under the PPIP Act sections 37, 38 and 42 enable the Privacy Commissioner to obtain information from agencies to undertake the Privacy Commissioner's functions set down in section 36.

While agencies generally take privacy protection and their obligations under the Act seriously, these provisions are of great value in assisting investigations and other important functions. No issues or matters arose in the period under review that suggested these sections be amended.

5.6 Oversight by Parliamentary Committee

I met with Joint Committee on the Ombudsman, the Police Integrity and the Crime Commission as part of its General Hearing on 18 February 2014 and provided advice on privacy issues subsequently raised by the Committee. I also provided to the Committee articles on 'drone surveillance'.[67] The Committee has indicated that it has an ongoing interest in this issue and has requested the Privacy Commissioner keep the Committee advised of developments.

67. *The Regulation of Civilian Drones: Impacts on Public Safety; Understanding the Drone Epidemic; The Regulation of Civilian Drones: Applications to the Surveillance of People* authored by Dr R. Clark, University of NSW.

5.7 Complaint handling, Internal Reviews and Tribunal Review

Information on complaints, internal reviews and referrals provides a useful insight into the operation of the Act and assists in identifying opportunities for continuous improvement of privacy management within NSW public sector agencies. Under the PPIP Act, the avenues by which individuals can have privacy complaints dealt with are:

- Complaint to (or by) the Privacy Commissioner under Division 3 of the PPIP Act (sections 45 to 51)
- Internal review of the conduct of a public sector agency under Part 5 of the Act (sections 52 and 53)
- Administrative review of the agency's conduct by the NSW Civil and Administrative Tribunal (NCAT) under Part 5 of the Act (sections 55 and 56).

Data held by the Commission shows that 157 internal review complaints and 96 formal complaints were managed during the period 1 July 2013 to 30 June 2014. For both categories, the majority of complaints concerned the disclosure of personal information followed by use of personal information and the inability to access personal information. Almost two thirds of total complaints (60.5%) concerned State Government agencies. More detail showing the breakdown of complaints including internal reviews, by legislation or privacy principle is provided in Attachment 4.

The survey of members of the public revealed that few had made a formal privacy complaint. More detail of the survey responses of members of the public is in Attachment 1.

5.7.1 NSW Civil and Administrative Tribunal Review

Unpublished statistics provided by NCAT show that during 2013 – 2014, 34 relevant applications were finalised, in which:

- 12 applications withdrawn
- 5 settled
- 3 decision affirmed
- 5 dismissed (no appearance)
- 1 dismissed (no jurisdiction)
- 7 dismissed (other reasons)
- 1 contravention found and decision set aside.

A review of published decisions by NCAT in the period 1 July 2014 to 30 June 2013 provides an insight into types of issues and IPPs under consideration by the Tribunal:

- Alleged breach of section 18 of PPIP Act in relation to the inappropriate disclosure of personal information by an employee of a NSW public sector agency to a third party and the inappropriate use of that information by the third party
- Alleged breaches of disclosure under section 18 and 19 of the PPIP Act
- Alleged breaches of section 15 (alteration of personal information) and section 16 (accuracy of personal information) of the PPIP Act
- Review of internal review provisions of the PPIP Act
- Amendment of personal information under clause 8 of schedule 1 of the HRIP Act
- Collection, use and disclosure of personal information under the PPIP Act
- Commentary on section 15 (alteration of personal information) of the PPIP Act
- Alleged contravention of HPP5 storage and security of information of the HRIP Act
- Disclosure of health information to a third party of the HRIP Act
- Accuracy of health information of the HRIP Act
- Storage and security of health information of the HRIP Act.

Consistent with feedback from the public, disclosure of personal information is high on the list.

5.7.2 Privacy Commissioner's conciliation of complaints

The Privacy Commissioner does not have a determinative role under the PPIP Act in relation to complaints but oversights agencies' investigation of those privacy complaints that proceed through the PPIP Act internal review process. Individuals under the PPIP Act can either:

- directly complain to the Privacy Commissioner who can attempt to resolve the issue by conciliation, investigation or referral to another person or body for investigation,[68] or
- seek an internal review by the agency of concern and if not satisfied with the outcome of the internal review and seek a review of the agency's process by NCAT.

68. Section 45 of the PPIP Act and section 42 of the HRIP Act enable complaints to be made to the Privacy Commissioner.

5 Operation of the Act (continued)

Typically allegations of breaches are managed through the internal review provisions. This has been a response to section 55 of the PPIP Act which establishes that a person can only apply to NCAT after an internal review by a public sector agency has been conducted. Where an individual elects to make a complaint to me, and I decide to conciliate, this has the consequence of depriving that individual of access to an appeal process through NCAT.

Section 50 of the PPIP Act provides that I may make a written report of findings or recommendations in relation to a complaint dealt by me under the Act and I may give this report to the complainant, and to others materially involved in matters concerning the complaint.

But the PPIP Act is silent in relation to my capacity to require compliance with any of my recommendations unlike the Commonwealth jurisdiction where the Privacy Commissioner has determinative powers. Consequently while Alternate Dispute Resolution (ADR) processes may be applied to resolve disputes between parties, in certain circumstances where no agreement is reached, I am unable to resolve the privacy dispute further. A similar situation exists under the HRIP Act through section 46(7) HRIP Act, whereby I am unable to take further action after the conclusion of the conciliation proceedings, whether or not the parties reach any agreement as a result of the proceedings.

The right of appeal to NCAT in privacy complaint handling is important to NSW citizens; it is a powerful means of external review of an agency's decision. In light of this, the ADR mechanisms in the NSW privacy regime may not be the better option for complainants. Despite my support for alternative dispute resolution mechanisms, I have significant reservations about alienating this means of redress for complainants by attempting to resolve an individual's complaint by conciliation.

This situation is different to that under the GIPA Act. It is appropriate to modernise the complaint handling mechanism under the PPIP Act so individuals seeking a review of a complaint conciliated by the Privacy Commissioner can take their matter to NCAT. This approach is specifically limited to cover conciliation of complaints by the Privacy Commissioner requested by individuals who allege a breach of their privacy.

Recommendation

32) The PPIP Act be amended to:

a) require agency compliance with the recommendations of the Privacy Commissioner arising from the conciliation of a complaint to the Commissioner

b) provide for the right of appeal to NCAT in relation to findings and recommendations of the Privacy Commissioner in respect of the conciliation of a complaint

c) remove the restriction in section 46(7) of the HRIP Act on the Privacy Commissioner taking any further action as a result of conciliation proceedings.

5.7.3 Who can request and who can undertake Internal Reviews?

Section 53 of the PPIP Act gives an aggrieved person the right of internal review by the agency whose conduct is the subject of a complaint. As noted by previous Privacy Commissioners, a 'person aggrieved' is a wider concept than a 'person whose personal information is in issue'. Despite this, the approach has been to advise that the request for an internal review needs to be made by the person whose personal information is the subject of the complaint. A number of matters have come to the Privacy Commissioner that suggest that it would be valuable to clarify in the PPIP Act that 'representative claims' can be subject to internal review.

The Department of Education and Communities raises the issue of standing to request an internal review. The Department has recommended that the PPIP Act be amended to provide that unless a person is under 18 years old or lacks capacity, a parent/guardian couldn't make a complaint on their behalf. It requires further examination and discussion with the Department.

Part 5, section 53(4) specifies who can undertake an internal review for an agency. In addition to this being undertaken by the Privacy Commissioner if requested by the agency, the person must be someone who is directed by the agency, not substantially involved in the conduct which is the subject of the review, and who is an employee or officer of the agency.

The statutory review of the PPIP Act undertaken by the Attorney General's Department in 2004 recommended that agencies should be able to outsource their internal review obligations to appropriately qualified agents (Recommendation 24). This would provide greater flexibility particularly for smaller agencies. The amendment of the PPIP Act to include explicitly coverage of contracted service providers and contractors is a prerequisite requirement for this amendment.

Recommendation

33) The PPIP Act be amended to:

a) clarify that 'representative' claims can be the subject of the internal review process and review by NCAT, and

b) allow agencies to outsource their undertaking of the internal review.

5.7.4 Time frames applying to Internal Reviews

The Department of Education and Communities sought a timeframe within which complainants can apply to NCAT for review. Since then NCAT has introduced a time frame of 28 days from advice of the outcome of an internal review to lodge an application. I considered this period too short; recommending 60 days instead, and I note that the statutory review undertaken in the Attorney General's Department in 2004 stated that "Commissioner and the Tribunal agree that applications to the Tribunal should be made within 60 days of an applicant being advised of the outcome of an internal review", and recommended this time period.[69]

Another issue raised concerns delays in responding to agencies. The PPIP Act gives the Privacy Commissioner the role of oversighting agencies' internal reviews. Agencies are required to consider material submitted by the Privacy Commissioner. The Office of the Privacy Commissioner has been rightly criticised for the delay in responding to agencies' requests for input prior to finalisation of the internal review report.[70] This is an issue both of resourcing and the process for determining priorities for allocation of resources.

I appreciate the frustration of agencies in receiving early feedback from the Privacy Commissioner on internal reviews of their complaints. However, limited resources currently preclude me from responding more promptly. Nonetheless it is important that agencies receive early feedback on internal review of complaints and I support the recommendation for a specified time frame within which the Commissioner must respond and that the Commissioner be resourced accordingly to enable that time frame to be met. It is an important accountability that should not only apply to agencies conducting the internal review but also to the oversighting Privacy Commissioner.

Recommendation

34) The PPIP Act be amended to specify a time frame within which the Commissioner must respond to a notification by an agency of an internal review and if no response is received within this time frame the matter can be deemed to be finalised by the agency and that the Privacy Commissioner be resourced appropriately to enable this time frame to be met.

5.7.5 Annual report complaints data of departments and statutory bodies

5.7.5.1 Departments

Public reporting of privacy practices, breaches and complaint handling is an important accountability mechanism. Some provisions are in place for Departments and statutory bodies for their privacy practices.

Under clause 6(b) of the *Annual Reports (Departments) Regulation 2010*, Departments (as defined in section 3 of the *Annual Reports (Departments) Act 1985*) are required to include in their annual reports statistical details of any review conducted by or on behalf of the Department under Part 5 of the PPIP Act.

Annual reports reviewed for 29 Departments revealed:

- 7 Departments reported that they had received requests for internal reviews
- The total number of requests for review across the seven departments was 79
- The number of requests for review ranged from one received by one department to 45 received by another department
- 57 of the internal reviews were reported as completed in which:

69. NSW Attorney General's Department, Review *of the Privacy and Personal Information Protection Act 1998,* p71 and Recommendation 26, p72, 2004.

70. Department of Education and Communities, Submission to *Report on the Operation of the Privacy and Personal Information Protection Act 1998,* 2014.

5 Operation of the Act (continued)

- Breaches were found in 6 matters
- No breaches were found in 9 matters
- No outcomes were reported in relation to 42 matters.

5.7.5.2 Statutory bodies

Clause 10(3)(b) of the A*nnual Reports (Statutory Bodies) Regulation 2010* requires statutory bodies (defined in section 3 of *Annual Reports (Statutory Bodies) Act 1984*) to include in their annual reports statistical details of any review conducted by or on behalf of the body under Part 5 of the PPIP Act.

Annual reports of a sample of 34 statutory bodies revealed:

- 9 statutory bodies reported that they had received requests for internal reviews
- The total number of requests for review across the nine statutory bodies was 43
- The number of requests for review ranged from one received in one statutory body to 18 received in another statutory body
- 22 internal reviews reported as completed in which:
  - Breaches were found in 5 matters
  - No breaches were found in 7 matters
  - No outcomes were reported in relation to 10 matters.

The material provided in the annual reports for both Departments and statutory bodies varied from sparse to comprehensive. Room exists for improving this important accountability to the community in accord with the goals expressed in the NSW Government's *State Plan NSW 2021 Outcome Area – Restore Accountability to Government*. Amending the annual report requirements to include reporting of serious breaches of privacy as recommended in section 5.3.4 would improve accountability in a beneficial manner.

6

Interaction with other legislation

6 Interaction with other legislation (continued)

While the PPIP Act and HRIP Act are the major pieces of legislation in NSW that govern privacy management, other legislation contain provisions that relate either directly to the Privacy Commissioner or to the management of personal information by the agencies concerned. These include the *Road Transport Act 2013*, *Service NSW (One-stop Access to Government Services) Act 2013*, *Child Protection (Working with Children) Act 2012* and *Government Information (Public Access Act) 2009* (GIPA Act).

In the period covered by this report, the major interactions that have arisen concern the GIPA Act.

6.1 Access to personal information

Access to personal information is currently possible under the PPIP Act, the GIPA Act and the *State Records Act 1998*.

As Privacy Commissioner, I've found that personal information is quite distinct from government information as stated by the NSW Ombudsman in his 2009 Report *Opening up Government*.[71] Accordingly personal information is best accessed under privacy legislation to simplify and reduce administrative demands upon agencies. This issue has been discussed in detail under "Section 5.3: Information Protection Principles" where I recommended access to and amendment of personal information be governed solely by the privacy legislation (the PPIP and HRIP Acts) and access to non-personal information (government information) be governed by the GIPA Act (Recommendation 12).

6.2 Treatment of excluded information

There is an apparent inconsistency under Clause 2 of Schedule 2 to the GIPA Act and the treatment of 'excluded information' between the Office of the Information Commissioner and the Office of the Privacy Commissioner.

Information about certain NSW Government agency functions is considered 'excluded information' under the GIPA Act. An application seeking excluded information of the agency to which the application is made will be considered invalid under section 43(2) of the GIPA Act. Excluded information also provides the basis for a conclusively presumed overriding public interest against disclosure where an application is made to an agency other than the agency whose excluded information is in issue.

Specifically, clause 2 of Schedule 2 to the GIPA Act provides four categories of excluded information for the Information Commissioner but only three for the Privacy Commissioner as shown following:

- The Office of Information Commissioner – review, complaint handling, investigative and reporting functions
- The Office of Privacy Commissioner – complaint handling, investigative and reporting functions.

The term 'review' is absent from those functions of the Office of the Privacy Commissioner. However, there is an internal review function by agencies detailed in Part 5 of the PPIP Act. The Privacy Commissioner has a role in these reviews as set out in sections 53 and 54 of the PPIP Act. Under section 54 there is a requirement for agencies to inform the Privacy Commissioner of an application for internal review, to keep me informed of progress of the review, then inform me of the findings of the review. I am entitled to make submissions to the agency in connection with the internal review. I am also able to undertake the review if requested by the agency.

Presently my role in the review function may be open to question as to whether or not information provided to me by an agency as required under the PPIP Act is 'excluded information' under the GIPA Act. The effect is that information provided to me as part of the oversight of an internal review potentially would be obtainable under a GIPA application. This is likely to have the effect of constraining openness of agencies around alleged or actual breaches of privacy and undermine my ability to assist agencies.

Amending clause 2 of Schedule 2 to the GIPA Act to include for the Privacy Commissioner, 'review' information in 'excluded information' will ensure that my statutory role in relation to oversighting internal reviews is adequately covered, specifically that internal review information provided to me by an agency, and possibly vice versa, will be considered 'excluded information' under the GIPA Act. This will both protect the privacy of individuals whose information is provided to me, the provision of open and honest information to my office by an agency, and ensure a more robust and effective

71. NSW Ombudsman, *Opening up government. Review of the Freedom of Information Act 1989. A Special Report to Parliament under s.31 of the Ombudsman Act 1974*, February 2009.

review process facilitating the provision of relevant advice and better outcomes.

This outcome is seen to be the purpose for certain information being 'excluded information' under the GIPA Act.

Recommendation

35) The excluded information of the Privacy Commissioner under Clause 2 of Schedule 2 of the GIPA Act include 'review' to enable protection of information provided to the Privacy Commissioner in relation to the internal review function by agencies as set out in sections 53 and 54 of the PPIP Act.

6.3 Consultation with the Privacy Commissioner

The PPIP Act and the GIPA Act each contain provisions that require consultation between the Privacy Commissioner and Information Commissioner.

Under section 94 of the GIPA Act, the Information Commissioner must consult with the Privacy Commissioner before making a recommendation against a decision of an agency that there is an overriding public interest against disclosure of information when the agency's decision concerns a privacy-related public interest consideration.

The Information Commissioner must consult with the Privacy Commissioner before issuing any guideline about a privacy-related public interest consideration that could have the effect of revealing an individual's personal information, or contravene an information protection principle under the PPIP Act or a Health Privacy Principle under the HRIP Act.

The Information Commissioner noted in her *Report on the Operation of the Government Information (Public Access) Act 2009: 2013 – 2014* that she did not make a recommendation for reconsideration of the original decision that there is an overriding public interest against disclosure of information in the majority of decisions that relied on individual rights, judicial processes and natural justice as grounds for refusal. Privacy-related considerations were regarded as a subset of these grounds. I am informed that in the period 1 July 2013 to 30 June 2014 the total number of applications for review under the GIPA Act received by the Information and Privacy Commission where agencies refused access to information on the basis of privacy was 89. In no case did the Information Commissioner recommend under s94 that the agency provide access to the information and consequently no consultations were required with the Privacy Commissioner in relation to these decisions.

Where such a decision is to be made, it is mandatory that the Privacy Commissioner as the officer charged with the responsibility with the administration of the PPIP Act be consulted before any decision is made by the statutory officer empowered to make such decisions. When such consultations occur, as required by section 94 of the GIPA Act, the views of the Privacy Commissioner must be identified and included in any final determinations. It is also important that a record is maintained of section 94 GIPA Act decisions and processes. I have requested that the collection and reporting on such data be included in the development of business requirements for the enhancement of the Commission's case management information system.

7

Role of the Information and Privacy Commission in supporting the statutory functions of the Privacy Commissioner

The Information and Privacy Commission (the IPC) came into being on 1 January 2011, from the merger of Privacy NSW and the Office of the Information Commissioner into a Commission within which "the two Commissioners will continue to exercise discrete functions in relation to privacy and access to government information."[72]

The Parliament noted the IPC was to provide:

- consistent information and advice
- coordinated training
- a common point of contact for the public
- administrative and operational efficiencies through shared corporate services, and
- significantly increase the resources available to privacy.[73]

The NSW Parliament recognised that issues around the privacy of personal information and access to government information overlap, and established a single office to administer privacy and access legislation to support both functions equally while retaining important safeguards to ensure the independent management of privacy and information access, consistent with the legislative intent of the PPIP Act and the GIPA Act. These safeguards are two independent and equal Commissioners with provisions that ensure neither Commissioner undertakes the other's functions nor acts in the other's area of responsibility. Additional safeguards are that each Commissioner reports to Parliament on their respective functions within the annual report of the Information and Privacy Commission, and on the operations of their respective legislation in separate reports. Parliament saw the reporting obligations of the Commissioners as a means to ensure transparency and accountability regarding the distribution of resources in the Information and Privacy Commission.[74]

The concern of the Parliament was for the independence of the two rights – the right to privacy and the right to government information and Parliament placed the Privacy Commissioner and the Information Commissioner on an equal footing to ensure unbiased advocates for privacy and access to information.[75]

This concern is reflected in legislative requirements giving the Privacy Commissioner the right to appear and be heard in any proceedings before NCAT in relation to a review under part 5 of the GIPA Act where proceedings involve a privacy-based public interest consideration against disclosure. Further, when the Minister exercises his or her power to recommend the making of a regulation under the GIPA Act, the Minister is required to consult with the Privacy Commissioner when the regulation concerns the protection of individual privacy or a privacy-based public interest consideration against disclosure.

Importantly in complaint handling, where the Information Commissioner intends to recommend that information be released although the original decision made by the agency was not to provide the information due to privacy concerns, the Information Commissioner is required to consult with the Privacy Commissioner. Similar requirements were established for when either Commissioner prepares guidelines that impact upon the other's area of responsibility.

It is imperative the IPC serve both the Privacy and Information Commissioners as envisaged by the Parliament and the work plan and priorities of the Commission reflect the needs and priorities of both Commissioners. It is also imperative that the commitment of Parliament to provide extra resources to privacy through the establishment of the Commission be recognised. Current resourcing does not facilitate the Privacy Commissioner addressing strategic or emerging issues associated with championing the privacy of individuals through the statutory functions of researching and reporting on developments in technology concerning the need for legislative, administrative or other action (section 36 (2) (f),(j),(l)). This capacity is crucial given the (then) Department of Attorney General's decision to establish and fill the Privacy Commissioner position as a part time role.

In a situation where the Information Commissioner is the Chief Executive Officer of the IPC with responsibilities and functions of Heads of other Public Sector agencies under the *Government Sector Employment Act 2013* (GSE Act) including the employer functions of the Government under section 31 of the GSE Act (which include but are not limited to recruitment, assignment of roles and termination of employees), the Privacy Commissioner is reliant on the

72. NSW Parliament, Legislative Council, Second Reading Speech, *Privacy and Information Legislative Amendment Bill, 2010, Hansard, 2010*, p25,689.

73. NSW Parliament, Legislative Council, Right of Reply following Debate after Second Reading Speech, *Privacy and Information Legislative Amendment Bill 2010*, Hansard, 2010, p25,694.

74. NSW Parliament, Legislative Council, Second Reading Speech, *Privacy and Information Legislative Amendment Bill 2010*, Hansard, 2010, p25,689.

75. Ibid.

7 Role of the Information and Privacy Commission in supporting the statutory functions of the Privacy Commissioner (continued)

cooperation and goodwill of the Information Commissioner as CEO to ensure that sufficient resources are deployed to enable the Privacy Commissioner to meet legislative obligations as envisaged by Parliament. It is inconsistent with the intent of Parliament and the ability to meet the statutory functions, for the Privacy Commissioner to be supplicant to the Information Commissioner.

In this context of the challenges outlined in this report and Parliament's intent, it is imperative that the Privacy Commissioner has a discrete budgetary allocation for core statutory functions as outlined earlier in this report. Achieving Parliament's intent to champion privacy generally, to assist NSW public sector agencies and to address the significant privacy matters discussed in this report, requires this allocation as a matter of immediate attention.

Recommendation

36) The IPC budget has specific allocation to enable the Privacy Commissioner to meet the broader statutory requirements of the role specifically undertaking research, publish reports and conduct inquiries and investigations into privacy-related matters.

8

Consolidated list of recommendations

8 Consolidated list of recommendations

Definition of personal information	1) The Privacy Commissioner to develop guidelines on the concept of "reasonably ascertained" identity to assist NSW public sector agencies. 2) The Privacy Commissioner to provide a research paper to the Parliament on the implications of the increasing convergence and capacity of information communication technology for privacy and the definition of personal information in the PPIP Act.
Coverage of the PPIP Act – State Owned Corporations	3) All NSW SOCs should be subject to privacy regulation so that either: a) the PPIP Act applies to SOCs not covered by the *Privacy Act 1988* (Cth); or b) those currently not prescribed under the *Privacy Act 1988* (Cth), are prescribed.
Contracted services and contractors	4) The PPIP Act to be amended to clearly cover contracted service providers and contractors who may be involved in services other than 'data services'. 5) Privacy compliance obligations are specified in contractual terms for the outsourcing of the provision of government services by public sector agencies to non-government organisations. 6) The Privacy Commissioner to assist agencies to provide guidance and assistance to non-government organisations in meeting their obligations and to manage the implementation of contracts including measuring, monitoring, benchmarking and reporting on compliance.
What is 'an agency' for the purpose of use and disclosure of information?	7) The Privacy Commissioner confer with the Department of Premier and Cabinet and the Department of Justice about the making of a regulation under Section 4B of the PPIP Act clarifying which agencies are part of or separate from public sector agencies for the purposes of the PPIP Act.
Privacy by design	8) The IPPs within the PPIP Act to include an overarching principle of 'privacy by design'.
Anonymity and pseudonymity	9) The PPIP Act be amended to include the principle of anonymity and pseudonymity where lawful and practicable, similar to Australian Privacy Principle 2 in the *Privacy Act 1988* (Cth).
Notification of privacy breaches	10) The PPIP Act be amended to provide for mandatory notification of serious breaches of an individual's privacy by a public sector agency similar to that proposed to be provided in the *Privacy Act 1988* (Cth). 11) The *Annual Reports Act* and related Regulations be amended to require reporting of serious breaches and actions taken to address the breaches.
Accessing personal information	12) Access to and amendment of personal information be governed solely by the PPIP Act and that access to non-personal information (Government information) be governed by the GIPA Act. 13) Consideration be given to amending the PPIP Act section10 (f) to reflect changes in technology for collecting and storing personal information and changes in service provision models.
Inter-jurisdictional or transborder disclosure	14) The movement of personal information outside of NSW or to Commonwealth agencies be protected by amendment to the PPIP Act in the manner of health privacy principle 14, Schedule 1, HRIP Act.

Exemptions for research purposes	15) The PPIP Act be amended to provide for the use of personal information for research and other purposes similar to those listed in section 10 of the HRIP Act.
Structure of the PPIP Act	16) The PPIP Act be restructured to set out the IPPs and exemptions in a Schedule to the Act.
Public sector capability in privacy and information management	17) The Public Service Commission, in conjunction with the Privacy Commissioner, undertake a review of agency and cluster capacity and capability in order to identify strengths and limitations and develop strategies to develop staff to meet customer needs in the management of their personal information.
Information technology security	18) ISO/IEC 27018 standard covering privacy, security and cloud services be considered for inclusion in the NSW Government's *Information Security Management Systems Policy*. 19) The Privacy Commissioner in conjunction with the Office of Finance and Services develop model clauses for inclusion in cloud computing contracts to ensure the protection of privacy and personal information, covering the collection, custody and ownership, use, storage, access to, disclosure and sharing of the information, business continuity, data disposal and exit strategy. 20) Agencies include periodic audits of the implementation of the NSW Government *Cloud Services Policy* in their audit and risk plans. 21) The Auditor General conduct a post-implementation review of the NSW Government *Cloud Services Policy* within two years of the date of commencement of the policy in which privacy management and compliance is a component of the review.
'Big data'	22) The Privacy Commissioner's ability to conduct urgent investigations into large-scale breaches of public concern be enabled by provision of additional resources on a one-off basis for this specific purpose.
Surveillance	23) The Privacy Commissioner prepare guidance on the use of surveillance technologies.
Firearm regulation and risks to individual privacy and public safety	24) The NSW Police Force review the processes and systems relating to the register of firearm ammunition purchases to ensure compliance with legislation relating to the register while ensuring the protection of the privacy and personal information of purchasers. 25) The Privacy Commissioner to raise with the NSW Auditor General the inclusion of this matter in the forward performance audit program of the Audit Office.
Public sector agency accountability for privacy management	26) The *Privacy Governance Framework* developed by the Privacy Commissioner be further developed to: a) include examples of leading practice, interactive tools and training resources and summaries of NCAT decisions and their implications for agencies; and b) provide guidance for public sector agencies as to the matters to be included in their annual reports on the implementation of privacy legislation.
Changing nature of Government and service provision	27) The alignment of the PPIP Act and emerging service provision models particularly of 'one government customer' be examined and a report prepared if amendment of the PPIP Act is indicated.

8 Consolidated list of recommendations (continued)

Consent	28) The Privacy Commissioner develop and publish guidance on the requirements of consent.
Sharing 'personal information' for policy analysis and planning purposes	29) The Privacy Commissioner in conjunction with relevant agencies, establish a project to identify and investigate methodologies that enable the safe use of personal information in de-identified, aggregated and linked data sets so as to protect the privacy and personal information of individuals. 30) The appropriateness of a Code of Practice to enable information sharing for planning and policy analysis purposes between agencies be examined and developed if such a need is demonstrated.
Exchange of information for child protection purposes	31) The Departments of Family and Community Services and Education and Communities confer with each other and the Privacy Commissioner in relation to the development of a Code of Practice for the exchange of information in relation to the management of child protection issues.
Privacy Commissioner's conciliation of complaints	32) The PPIP Act be amended to: a) require agency compliance with the recommendations of the Privacy Commissioner arising from the conciliation of a complaint to the Commissioner b) provide for the right of appeal to NCAT in relation to findings and recommendations of the Privacy Commissioner in respect of the conciliation of a complaint c) remove the restriction in section 46(7) of the HRIP Act on the Privacy Commissioner taking any further action as a result of conciliation proceedings.
Internal reviews	33) The PPIP Act be amended to: a) clarify that 'representative' claims can be the subject of the internal review process and review by NCAT, and b) allow agencies to be able to outsource their undertaking of the internal review.
Time frames applying to oversight of internal reviews	34) The PPIP Act be amended to specify a time frame within which the Commissioner must respond to a notification by an agency of an internal review and if no response is received within this time frame the matter can be deemed to be finalised by the agency and that the Privacy Commissioner be resourced appropriately to enable this time frame to be met.
Treatment of excluded information	35) The excluded information of the Privacy Commissioner under Clause 2 of Schedule 2 of the GIPA Act include 'review' to enable protection of information provided to the Privacy Commissioner in relation to the internal review function by agencies as set out in sections 53 and 54 of the PPIP Act.
Resourcing support	36) The IPC budget has specific allocation to enable the Privacy Commissioner to acquit the broader requirements of the role specifically undertaking research, publish reports and conduct inquiries and investigations into privacy-related matters.

Attachments

1 Feedback from members of the public

The survey of members of the public was released in October 2014, supported by media and communications strategies to raise awareness of the survey and encourage participation by people from a diverse range of backgrounds and demographics – 569 responses were received.

Participant demographics

Gender

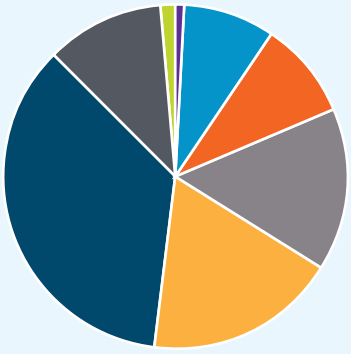
Two hundred and sixty eight (48%) of the 526 respondents who chose to specify their gender were females and 258 (47%) were males. 28 respondents chose not to specify their gender or indicated 'other'. There were 554 respondents who responded to the question.

Age

Responses were received across a range of age groups as shown in the following pie chart. 65% of the 556 respondents who responded to the question on their age demographic were aged 50 or more. 36% of respondents were in the age range 60 to 69 years of age.

Respondents by age group

1.08%	13 to 19
8.45%	20 to 29
9.17%	30 to 39
15.29%	40 to 49
18.17%	50 to 59
35.61%	60 to 69
10.97%	70 years or more
1.26%	Prefer not to say



Cultural identification

Eight respondents identified as being of Aboriginal and Torres Strait Islander (ATSI) background, 71 as people of culturally and linguistically diverse backgrounds and 45 as people with a disability. Numbers were not of a sufficient size to enable reliable cross tabbing of questions by cultural group.

Location

The majority (54%) of participants were from the Sydney metropolitan area (301), 235 from regional NSW, and three were from outside NSW. Seventeen participants chose not to say or not to respond.

Awareness of the Information and Privacy Commission and the PPIP Act

The majority (41%; 229) had heard of the Information and Privacy Commission and 59% (324) had not. 53% of respondents were aware of the PPIP Act and 47% were not.

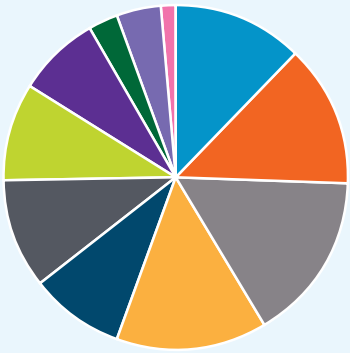
Privacy issues of concern

Concerns about public sector agencies

Respondents were asked to identify privacy issues of concern to them. Concerns about privacy issues in public sector agencies are shown in the following pie chart. Security, disclosure, use and collection of personal information were the issues of most concern to members of the public followed by storage of information, not being told what information is held on you and accuracy of information.

Privacy issues of concern to members of the public in relation to public sector agencies

12.29%	How personal information was collected
13.39%	How personal information was used
15.94%	How securely personal information was held and stored
14.04%	Providing personal information to others
8.87%	Accuracy of personal information held
10.44%	Movement or storage of personal information outside NSW
9.10%	Not being provided with information on what personal information is held about you
7.62%	Not being able to access personal information held about you
2.82%	Responses received to privacy complaints
4.34%	Information and communication about privacy management policies and practices
1.15%	Other



Concerns about private sector organisations

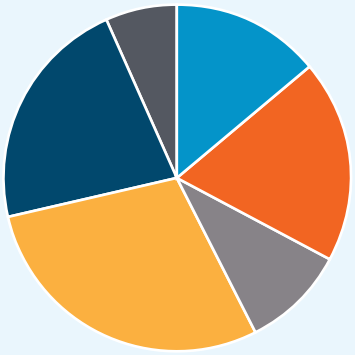
Ninety-five respondents answered that they had concerns about the privacy practice of a private sector organisation such as a retailer or bank in the past 12 months while 228 said they had not had concerns.

Other privacy issues of concern to members of the public

Other privacy issues of concern to members of the public are shown in the following pie chart. Privacy practices of social media, practices of family and friends received the most frequent responses, followed by privacy in private places and producing an evidence of identity in public places.

Privacy issues of concern to members of the public

13.95%	Providing copies of ID when entering licensed premises
19.09%	Surveillance in private places
9.54%	Surveillance in public places
29.07%	Privacy practices of social media providers
21.73%	Privacy practices of family or friends
6.61%	Other



1 Feedback from members of the public (continued)

Privacy issues that members of the public would like to be covered by NSW privacy legislation

Survey respondents identified the following as matters that should be covered by NSW privacy legislation:

- Protection of personal information by NSW private sector (482 responses);
- Protection of personal information by NSW public sector agencies (492 responses), ability to enjoy privacy in own home (436 responses);
- Privacy of personal communications (450 responses); and
- Physical privacy such as freedom from surveillance (244 responses).

Issues members of the public think should be covered by NSW privacy legislation

Privacy complaints

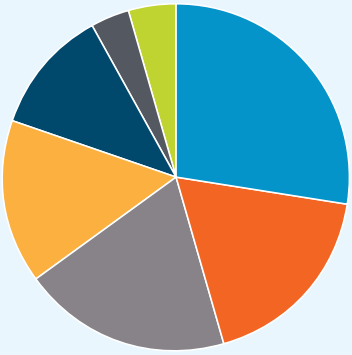
Who would members of the public approach with a privacy concern?

Most respondents indicated that they would approach the NSW or Australian Privacy Commissioner or the relevant public sector agency or private sector organisation if they had a complaint or concern about a privacy matter.

	Number
NSW Privacy Commissioner	357
Australian Privacy Commissioner	233
Relevant public sector agency	252
Relevant private sector organisation	198
Legal representative	149
Other regulatory body	47
Other	56

Who members of the public would approach about a privacy complaint or concern

- 27.63% NSW Privacy Commissioner
- 18.03% Australian Privacy Commissioner
- 19.50% Relevant public sector agency
- 15.33% Relevant private sector organisation
- 11.53% Legal representative
- 3.64% Other regulatory body
- 4.33% Other



Complaints made

Respondents who had made complaints in the previous 12 months

A minority (85 respondents) had raised a concern or complaint about a privacy matter with any of the NSW Privacy Commissioner, Australian Privacy Commissioner, relevant public sector agency, relevant private sector organisation, legal representative, other regulatory body, in the past 12 months. 471 had not.

Subject of Complaint

The complaints concerned use of their personal information (53), disclosure of their personal information (52), storage and security of their personal information (50), collection of their personal information (45), accuracy of their personal information (24), access to their personal information (23), and other issues (20).

Issues complained about

- 16.85% Collection of your personal information
- 18.73% Storage or security of your personal information
- 8.61% Access to your personal information
- 8.99% Accuracy of your personal information
- 19.85% Use of your personal information
- 19.48% Disclosure of your personal information
- 7.49% Other

1 Feedback from members of the public (continued)

Satisfaction with the handling of complaints

The majority indicated that their complaint was not resolved to their satisfaction (71) while 16 respondents indicated that their complaint was resolved to their satisfaction. The reasons provided as to why complaints had not been resolved to the satisfaction of respondents included:

- The recipient of the complaint was dismissive of the complaint
- No one will take responsibility. There has been buck passing and no resolution of the matter. Matter unable to be dealt with at the local level and referred to the regional office or head office of private sector organisations
- Inordinate delay in finalising investigation
- Unsatisfactory response
- Matter ongoing for more than 12 months
- Privacy laws are not enforceable
- No acknowledgement, feedback or reply
- Nothing has changed. Practices complained about continue. Information remains inaccurate
- Vindictiveness by person complained about
- Privacy Commissioner unable to assist
- Agency was rude and dismissive
- Processes relating to the legislative requirement for retailers of firearms ammunition to register purchasers of ammunition have a high level of risk that personal information, such as the firearms owner's private address, will be disclosed and used for improper purposes with potential impact on the privacy and safety of registered firearms owners and their families
- Agency would not accept that their practices constituted an invasion of privacy.

2 Feedback from agencies

PART A – SECRETARIES OF DEPARTMENTS AND HEADS OF AGENCIES

In reporting on the operation of the Act I considered it important to provide secretaries of NSW government departments the opportunity to comment on the operations of the Act and suggestions for improvement. I wrote to government department secretaries and heads of government integrity agencies seeking their views from a strategic perspective on the operation of the PPIP Act, particularly how the Act supports or inhibits departments in meeting their strategic priorities and service delivery obligations to the people of NSW. I also invited comment on:

- key strategic privacy issues;
- which if any of the IPPs have the greatest impact on departments;
- the intersection of NSW and Australian privacy laws;
- the complaints handling/internal review/administrative review provisions of the Act;
- the exemptions provisions of the PPIP Act;
- the impact, if any, of administrative arrangements and/or legislative changes on the administration of PPIP Act in departments;
- any others issues relating to the operation of the PPIP Act; and
- how the Privacy Commissioner and the Information and Privacy Commission (IPC) can support departments in the administration of the PPIP Act.

I received 17 responses including seven from large government departments, and 10 from individual agencies including two from accountability agencies.

Responses ranged across the Premier and Cabinet, Treasury and Finance, Transport, Health, Planning and Environment, Trade and Investment, Justice, Education and Communities, and Family and Community Services clusters.

The departments and agencies responding were:

- Audit Office of NSW
- Department of Education
- Director of Public Prosecutions
- Family and Community Services
- Independent Commission Against Corruption
- Independent Transport Safety Regulator
- Legal Aid NSW
- NSW Civil and Administrative Tribunal (NCAT)
- NSW Crime Commission
- NSW Environment Protection Authority
- NSW Health
- NSW Small Business Commissioner
- Planning and Environment
- Premier and Cabinet
- Public Service Commission
- Roads and Maritime Services
- Transport for NSW
- Treasury.

Key themes

The apparent complexity of the privacy landscape

A number of agencies commented on the apparent complexity of the privacy landscape including the PPIP Act, HRIP Act, Codes of Practice, Public Interest Directions and Commonwealth privacy legislation.

Agencies identified the need for guidance from the Privacy Commissioner in relation to a range of matters including:

- How the various pieces of legislation including the PPIP Act, HRIP Act and the Commonwealth Privacy Act, apply to agencies; which agencies have obligations to comply with which information protection principles (IPPs) and which agencies are permitted to depart from which IPPs because of exemptions in the PPIP Act, Codes of Practice and Public Interest Directions; and which if any of the Australian Privacy Principles (APPs) apply to agencies
- How NCAT decisions and NCAT's interpretations of the law apply to agencies in different situations.
- Best practice in relation to interagency exchange of information with a focus on:
  - Examining the purpose of the information exchange/release
  - Custodianship during and after data release/use
  - Appropriate de-identification mechanisms
  - Data brokerage services
  - Security and communication processes
  - Processes for managing unforeseen uses of exchanged data.

2 Feedback from agencies (continued)

Suggestions for how the Privacy Commissioner might assist agencies included:

- Development of a tree diagram including legal requirements and elements of good practice, supported by interactive and digital tools, additional face-to-face training and case studies
- Provision of advice by the Privacy Commissioner on the impact of case law on interpreting the privacy legislation. The Department of Education and Communities commented that case law is an important source for interpreting the privacy legislation and it would assist the Department if the Commission provided either an annotated version of the PPIP Act or in some other form the direction case law was taking was available
- The identification by the Commission of recurring issues would significantly assist agencies and provide valuable support in the administration of the PPIP Act
- Regular bulletins on recurring issues and other developments in the privacy area.

One agency suggested that the core protection principles in the PPIP Act would be strengthened if the language and structure were simplified, with the IPPs contained in a Schedule to the Act, as is the case with the HRIP Act. The exceptions to each IPP should also set out clearly.

A number of agencies suggested that the closer alignment between the IPPs in the PPIP Act, the health privacy principles (HPPs) in the HRIP Act and the APPs in the *Privacy Act 1988* (Cth) would assist agencies in understanding and meeting their compliance obligations.

Dual coverage by State and Commonwealth privacy legislation

Several agencies identified that they are increasingly covered by both NSW and Commonwealth and in some cases other state and territory privacy legislation. They pointed to the lack of alignment between the IPPs in the PPIP Act and the APPs in the *Privacy Act 1988* (Cth) and the difficulties this causes in terms of compliance and capacity building of staff to meet privacy obligations.

The Department of Education and Communities observed that the different layers of Commonwealth, State and Territory laws and regulations complicate privacy obligations in some instances, noting that a number of the NSW IPPs are similar to but not identical to the APPs in the *Privacy Act 1988* (Cth), and the two sets of legislation have different enforcement regimes. The Department commented that it engages with businesses and Commonwealth bodies that must comply with Commonwealth privacy laws. There is also an imperative in ensuring businesses, contractors and other entities that the Department does business with comply with the NSW PPIP Act in addition to any requirements imposed on them by the *Privacy Act 1988* (Cth).

The Department of Education and Communities observed that increasingly with nationalisation and harmonisation of laws and regulations the Department is required to comply with Commonwealth privacy laws in some of its operations, such as for education and care services. This presents confusion and challenges in ensuring compliance with both Commonwealth and State privacy obligations in these operational areas. The Department recommended that consideration be given to amending the PPIP Act so that it aligns as far as possible with the *Privacy Act 1988* (Cth). Alternatively, that guidance be provided by the IPC on how an agency can simultaneously comply with these Acts.

Transport for NSW commented that the principles and exemptions in the PPIP Act differ markedly from those in the Commonwealth Privacy Act, particularly since the recent amendments to the Commonwealth law. Transport agencies regularly deal with private contractors that must comply with the Commonwealth law, and may also be obliged under their contracts with Transport for NSW to comply with the IPPs in the PPIP Act. Privacy protection would be promoted and confusion would be reduced if the privacy principles in both Acts were more closely aligned.

NSW Health observed that the impact of the amendments to the Commonwealth privacy legislation have not been significant for NSW Health as, for the most part, the legislation is not applicable to NSW Government agencies. The only recent issue for NSW Health has been the development of the NSW Government *Classification and Labelling Guidelines* by the NSW Office of Finance and Services. The Guidelines are committed to transitioning to a system for classifying and labelling sensitive information in a manner that is consistent with the Commonwealth security

classification system. The current Guidelines do not separately address health information and it is classified "Sensitive: Personal". NSW Health is in the process of considering whether a submission should be made recommending a separate dissemination limiting marker for personal health information, consistent with NSW legislation.

Gaps in legislative coverage

The Department of Premier and Cabinet commented on gaps in privacy coverage, noting that the application of the PPIP Act is not comprehensive, and gaps arise with respect to coverage of privacy legislation. For example:

- State Owned Corporations (SOCs) are excluded from the definition of "public sector agency" in the PPIP Act. Only a few SOCs are covered by Commonwealth legislation where included under regulation (Ausgrid, Endeavour Energy and Essential Energy). Therefore a number of NSW SOCs are not currently covered by either Commonwealth or NSW privacy legislation
- Contractors and subcontractors to State and Territory bodies are excluded from the operation of the Commonwealth Privacy Act. The PPIP Act is generally silent on the issue, however it does include persons or bodies providing data services (for example, involved in collecting data) in the definition of 'public sector agency' (section 3 of PPIP Act). Other jurisdictions require that agencies entering into a contract with a contracted service provider (involving the provision of personal information) ensure that the contractor complies with privacy legislation. The Department of Premier and Cabinet commented that there may be benefit in amending the PPIP Act in line with other jurisdictions to ensure that contractors do not engage in practices that would breach privacy principles.

Changing nature of government

A number of agencies commented on the changing nature of government business and service delivery including:

- a focus on evidence based policy and planning;
- a focus on risk assessment and risk management including the assessment of risks in the development of service delivery strategies;
- a shift from single agency service delivery to cross agency and cross sector cooperation and coordination in service delivery to common clients;
- outsourcing to or partnerships with non-government organisations (NGOs) and the private sector for service delivery;
- the growth of big data and enhanced use of technology and information systems to access and analyse data and information from a range of sources for research, planning, service delivery modelling, monitoring and reporting;
- sharing of information with third parties including other government agencies, NGOs, academics, industry (including ICT developers) and members of the public for purposes of research, planning, development of service delivery strategies and monitoring and reporting of outcomes;
- a focus on open data and open government;
- a focus on customer service and providing citizens and business with a seamless positive experience in their dealings with government including the roll out of NSW Service Centres with a 'single customer';
- an increase in transborder transactions;
- increasing demands on information access for law enforcement purposes; and
- the creation of agency clusters.

A number of agencies commented on the operation of the PPIP Act in this context.

The Independent Commission Against Corruption (ICAC)

The ICAC reflected that in its 1992 *Report on unauthorised release of government information* the Commission noted that:

> "The whole question of management of the increasing amount of confidential information held by the Government and its agencies, is in need of urgent attention. Until there are clear policies, adequate protection and effective laws, cherished privacy principles will be at risk, and the scope for widespread corruption will remain."

The ICAC commented that effective protection of individual privacy remains a key strategic issue both for government agencies and the public. The increased amount of personal information collected and retained

2 Feedback from agencies (continued)

by government agencies since the Commission's 1992 report has placed increased emphasis on the need to ensure that there is adequate protection of personal information held by government agencies. The PPIP Act is an essential safeguard in this respect.

NSW Health

NSW Health commented that the central themes emerging for privacy management in NSW Health in the context of strategic and operational developments which require particular consideration are:

- Confidence that personal information is sufficiently de-identified when using or disclosing information for purposes other than that for which the information was collected
- Assurance that security controls are in place which effectively protect personal information in the increasing number of data collections storing personal information for a multitude of management purposes
- Assurance that data linkage issues which arise within the health system, and with data linkage systems with other agencies, are proactively identified and addressed early
- Inter-jurisdictional transfer and use of personal information is in accordance with privacy legislation
- Targeted staff privacy training on privacy obligations
- Emerging social media use in public sector workplaces and managing the intersect between staff and/or client use of social media and privacy obligations
- Issues for managing the balance between appropriate and adequate disclosure of personal information when managing matters of misconduct, corrupt conduct or criminal conduct and other related matters in human resource management.

Inadvertent release of personal information through big data

The Department of Family and Community Services expressed the view that the PPIP Act does not address the possibility of information sharing nor does it equip agencies to ensure personal information is not inadvertently released through 'big data'. The agency observed that the growth of big data and techniques for processing data makes it easier to identify individuals from a relatively small number of de-identified data items. The agency warned of the potential for the inadvertent disclosure of personal information through the release of big data, for example where disparate datasets, individually de-identified, could potentially be linked or combined to re-identify individuals, resulting in a disclosure of personal information. The risk of inadvertent disclosure of personal information through the release of big data could be exacerbated in situations where responsibility for open government and open data differs is located within a number of different functional areas within an agency such as ICT, Communications, Records or Information Access and through inconsistency of approaches across government.

The Department also expressed that view that methods currently used for de-identifying personal data might not provide effective protection for personal information and may not avoid the legislative protections that extend to personal information about individuals whose identity can reasonably be ascertained. The Department suggested that the Privacy Commissioner could promote anonymisation standards and methods that agencies could confidently apply to data sharing in compliance with the PPIP Act.

Data sharing and information exchange

A number of agency comments focused on the perceived limitations of the PPIP Act in supporting data sharing and information exchange necessary for their agency's service delivery functions and responsibilities.

Limitations of Codes of Practice, Public Interest Directions and other mechanisms

The Department of Family and Community Services commented that the PPIP Act Codes of Practice and Public Interest Directions might not be sufficiently broad to support cross agency service delivery and data sharing functions, and sharing of information with NGOs, and that there is a need for a clear statement within the PPIP Act about the circumstances in which information can or should be shared.

Particular issues relating to the exchange of information for child protection

The Department of Family and Community Services pointed to difficulties relating to the exchange of information between agencies involved in child protection commenting that existing provisions in

child protection legislation relating to the exchange of information between agencies may not be adequate to exempt the Department of Family and Community Services and associated agencies from restrictions under privacy legislation. The Department also observed that while privacy Codes of Practice under the PPIP Act and HRIP Act can be used to authorise exchange of information with other government and non-government organisations, such Code provisions have been underused to date.

The Department of Family and Community Services also commented on the limitations of memoranda of understanding and protocols for the exchange of information, noting the increasing use of such instruments to help staff identify when information exchange can occur between agencies and organisations including those in other jurisdictions. The Department commented that while such mechanisms serve a useful function in assisting staff to recognise the difference between personal and non-personal information and drawing attention to information exchanges that are permitted by relevant Codes of Practice, Public Interest Directions or other exemptions, they cannot override permitted collection, use and disclosure under privacy laws.

The Department of Education and Communities also raised issues in relation to the interaction between the information sharing provisions under Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998* and the PPIP Act. The Department commented that there is confusion about the interaction between Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998* and the PPIP Act and a lack of understanding that Chapter 16A overrides the PPIP Act. This can have a serious impact on ensuring the ongoing safety and wellbeing of children and young people. The Department recommended that a note be inserted in the PPIP Act to refer to Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998* and confirm that it overrides the PPIP Act.

The Department of Education and Communities also commented that an unintended consequence of Chapter 16A is that only children and young persons under the age of 18 years are protected due to the definitions under the *Children and Young Persons (Care and Protection) Act 1998*. However a situation may arise where there is the need for a school to exchange information with another service provider in relation to the safety, welfare and wellbeing of a student who is over 18 years old. The Department noted that information exchange cannot currently occur under Chapter 16A or the PPIP Act unless consent is obtained.[76] The Department recommended that consideration be given to including in the PPIP Act provisions similar to those in Chapter 16A to enable agencies which provide services to clients to exchange information in relation to a person's safety, welfare or wellbeing.

Inter-jurisdictional or transborder disclosure

The Department of Family Services expressed concern at restrictions on inter-jurisdictional disclosures under section 19(2) of the PPIP Act. The Department commented that while the proposed Code of Practice under section 19(4) would allow exchanges of information with other jurisdictions it would not resolve privacy or confidentiality obstacles that may prevent similar agencies in other jurisdictions exchanging information with NSW government agencies. The Department proposed that uniform national legislation may be the preferred means of authorising exchanges of information with other jurisdictions rather than relying on changes to privacy laws. This applies particularly in areas such as child protection.

The Department of Family and Community Services also commented that there is a need to consider how best to achieve consistency between differing State and Commonwealth privacy legislative frameworks to assist agencies and NGOs that are subject to both State and Commonwealth privacy laws. Agencies involved in the delivery of services under the National Disability Insurance Scheme and private sector providers of health services who are subject to both Commonwealth and NSW health information regimes were cited as examples.

Roads and Maritime Services (RMS) commented: "Unsatisfactorily, current case law on section 19(2) is to the effect that because section 19(2) has not commenced, transborder disclosure is totally unregulated (i.e. even the normal disclosure rules in section 18 do not apply)."

76. "Consent is not necessary for exchange of information under Chapter 16A. However as it is a principle of the Act that a child or young person should be given an opportunity to express views on personal matters, consent should be sought where possible. Best practice also recommends that consent is sought from family members before information relating to them is exchanged", Department of Community Services, *Interagency Guidelines*.

2 Feedback from agencies (continued)

RMS suggested that consideration be given to repealing section 19(2) and amending section 18 to permit transborder disclosure on the same terms as section 18 but with the additional proviso that the recipient must be located in a jurisdiction with similar privacy laws or that the recipient is contractually obliged to comply with obligations broadly equivalent either with the Act or the Federal legislation relating to the storage, use, disclosure and destruction of personal information.

Capacity assessment and capability across the sector

The Department of Premier and Cabinet (DPC) pointed to previous pieces of work including a review of case studies on information sharing that had identified the limited knowledge and understanding, and in some cases misinformation and misunderstanding, of privacy legislation in relation to information sharing. The DPC suggested that a review of agency and cluster capacity and capability in relation to information sharing and exchange could be conducted, particularly as they relate to the interpretation and application of privacy legislation, and that further measures could be introduced such as capacity building reform or enhanced enforcement powers under legislation to address serious systemic issues.

Promoting Cultural Change

The DPC suggested that promoting cultural change, which emphasises the benefits of good practice personal information management, including an emphasis on consent, might help highlight that privacy is not simply a compliance burden. The DPC commented that case studies on information sharing had identified that open and transparent practices in managing personal information including obtaining consent can build trust between individuals and agencies. The DPC also noted that trust between research and data professionals throughout government was also identified in information sharing case studies as key to building an organisational culture of information sharing.

The DPC suggested that guidance material could be developed to assist agencies in understanding how to obtain consent.

RMS also commented on the issue of gaining customer consent for the use and disclosure of personal information at the point of collection, particularly from the perspective of the formation of agency clusters and the establishment of NSW Service Centres with a single customer.

RMS observed that section 10 of the Act requires an agency to provide its customer with certain information at the time of collection or as soon as practicable thereafter. This is commonly referred to as a "privacy statement" and among other things an agency is required to inform the customer what their personal information will be used for and who it may be disclosed to. Section 17 allows an agency to use personal information for the purpose for which it was collected or a directly related purpose. Similarly section 18 places limits on disclosure but permits disclosure where that is notified in the privacy statement. Hence it is important that the privacy statement describe all potential uses.

RMS commented that it has an unusually large range of functions including driver licensing, vehicle and vessel registration, and the regulation and management of both road and maritime transport (e.g. public passenger transport licensing). When collecting personal information, in the interests of relevance and brevity, RMS has traditionally "tailored" the privacy statement to the particular transaction rather than to refer to all of its functions. This consequently puts a limit on how the information can be used and disclosed under section 17 and section 18. RMS faces the additional challenge that many customers provided their personal information pre-2012 to the former NSW Maritime specifically for maritime purposes, or to the former RTA for road purposes, which means that RMS has to manage customers under a range of very different privacy statements which do not align to its current combined functions.

RMS noted that the recent push in government policy has been to view customers as a single customer seeking to be provided with "government services" from a variety of government service providers. RMS considers that this does not align well with the PPIP Act and recommended that there would be value in reviewing sections 10, 17 and 18 of the PPIP Act to better support the concept of a single customer, if not spanning all NSW agencies then at least within a particular agency, so that the agency can use and disclose the customer's personal information for all the functions of that agency as they exist from time to time. The purpose of the

privacy statement would then inform the person about any extraordinary uses or disclosures outside the normal business of the agency.

In a similar vein RMS commented that section 9 obliges agencies only to collect personal information directly from the customer unless the customer consents to indirect collection. Consideration of exceptions to facilitate "one government customer" would be helpful so that a customer is not required to repeatedly provide personal information (other than health information or sensitive personal information) to government agencies. For example, if a customer notifies one agency that he or she has a new address the customer should not be required to separately notify each other agency. RMS understands that the existing practice in Service NSW is to obtain customer consent for their information to be updated. The agencies' compliance with the Act is then dependent upon the robustness of the consent that is obtained from the customer. This practice presents a privacy risk for customers and for all agencies involved.

The Environment Protection Authority (EPA) commented that in order to uphold its privacy obligations and manage the risk that some submitters, despite the EPA's best efforts, will not be aware their submissions will be made public, staff must manually check submissions for confidentiality requests and if necessary redact personal information. The processes involved in making people aware that publication will occur and in manually checking and redacting submissions are time-consuming for staff and involve significant resources. On the positive side, the PPIP Act's requirements have led to the Department taking a number of initiatives to address privacy. These include the development of an online submission form with strong privacy tools which help prospective submitters with their privacy concerns while ensuring they understand their submission will be made public, and online privacy training for staff.

One agency commented on their experience in handling privacy complaints, suggesting that privacy complaints management has informed continuous improvement of business processes and systems.

The impact of organisational restructures

A number of agencies commented on the impact of structural change on privacy management in their agencies.

The NSW Ministry of Health advised that privacy is factored into health structural reforms, strategy and planning and operational service delivery initiatives. Dedicated privacy officer positions have been established at all tiers of the new structure for delivery of health services throughout NSW to ensure that privacy is integral to service planning and delivery.

The Department of Family and Community Services commented that organisational restructures can impact on how agencies are defined and consequently how Codes of Practice and Public Interest Directions apply to them. The Department is developing a Privacy Management Plan (PMP) for the whole organisation.

A number of agencies advised that they had developed or were developing whole of department PMP to replace separate plans for agencies within the Department.

No obligation to advise of breach of privacy

The DPC observed that currently there is no obligation on an agency to advise an individual, third parties or the Privacy Commissioner of a breach of an individual's privacy by an agency. The Department suggested that amending the PPIP Act to provide for mandatory notification as provided in the Commonwealth legislation would ensure consistency across all agencies.[77]

Definition of personal information

The Department of Education and Communities raised the issue of the definition of 'personal information'. The Department noted that the definition of 'personal information' includes where the identity of an individual "is apparent, or can reasonably be ascertained from the information or opinion." The Department commented that this raises the question of reasonableness. The Department noted that it may be possible to identify a person from core information which does not include a simple name and address, but does contain clues which could be pursued to ascertain who it relates to. This gives rise to the question as to how much extra effort or difficulty would such a step need before it could clearly be said that the identity could not be "reasonably ascertained". The Department commented that the uncertainty that arises impacts on the Department's capacity to provide accurate advice to staff that have responsibility for the implementation of the PPIP Act at

77. Mandatory notification of serious breaches were considered by the Federal Parliament but have not been passed into legislation.

2 Feedback from agencies (continued)

an operational level. The Department recommended that the PPIP Act be amended to clarify the parameters of "reasonably ascertained" or alternatively that guidelines be provided by the Commission on this aspect.

The Department of Education and Training also commented that personal information has a different definition under the PPIP Act and other legislation such as the GIPA Act. This can be confusing for both clients and agencies. The Department recommended that consideration be given to adopting a common definition of personal information in any legislation dealing with personal information.

Standing to make a privacy internal review application

The Department of Education and Communities raised the issue of standing to make a privacy internal review application. The Department noted that section 53 of the PPIP Act provides "a person (the applicant) who is aggrieved by the conduct of a public sector agency is entitled to a review of that conduct." Generally it is appropriate for a parent/guardian to seek a privacy internal review on behalf of their child if they are under 18 years of age or otherwise lack capacity. However, the Department has had cases where a parent has made an application for a privacy internal review on behalf of a child who is over 18 years of age or living independently at ages younger than 18. Sometimes these cases are pursued by parents where the young person whose information the matter relates to is not aggrieved or does not want the conduct reviewed. These cases are time consuming and divert resources in circumstances where the person whose information it concerns has no interest in the matter. The Department recommended that the PPIP Act be amended to provide that unless a person is less than 18 years old or lacks capacity a parent/guardian cannot make a complaint on their behalf. Furthermore, if a person is over 18 years old their consent is required before another party can seek a review on their behalf.

Access to personal information

The Department of Education and Communities commented on issues related to the fact that there is currently an option for a person to seek access to their personal information through both the PPIP Act and the GIPA Act and there is no mechanism to prevent a person from lodging applications for access to information under both Acts. The Department noted that section 59 of the GIPA Act provides that an agency can decide that information is already available to an applicant only if the information is:

a) Made publicly available by the agency in accordance with a legislative instrument other than this Act...

b) Available to the applicant from, or for inspection at, the agency free of charge in accordance with this Act... or

c) Contained in a document that is usually available for purchase.

The Department observed that information obtained through a PPIP Act application is not captured by section 59. This can lead to duplication of work and significant diversion of resources for the Department. The Department recommended that section 59 of the GIPA Act be amended to include where information has been provided under the PPIP Act.

Section 60(1) (b) of the GIPA Act allows an agency to refuse to deal with an application if the agency has already decided a previous application for the information concerned and there are no reasonable grounds for believing that the agency would make a different decision. It is not clear if the 'application' referred to in this section is limited to an application under the GIPA Act or whether it would capture an application under the PPIP Act. Under the current provisions the Department is potentially required to go through the GIPA Act process in relation to a request for access to the same information by the applicant. This is duplication and an unnecessary use of resources.

The EPA noted that it receives a considerable number of GIPA requests each year and many of those applications relate to records containing personal information of third parties. The EPA requested that consideration be given to combining the privacy protocols for both the PPIP and GIPA Acts for consistency and regulatory purposes.

Review rights

The Department of Education and Communities observed that the PPIP Act does not provide a time frame for when an applicant may lodge an application for review to NCAT. Providing for a time period in which to lodge a review request would bring some finality for the Department if the period expires and the applicant

has not exercised their rights. It would also ensure that an applicant who does wish to pursue the matter does so within a reasonable period when it is more likely evidence will still be relatively fresh and more readily available. The lack of finality means the Department is unable to close cases with confidence that the matter is completed and will not be subject to further external review. The Department recommended that the PPIP Act be amended to provide a time period in which an applicant may lodge a review to NCAT.

Costs

The Department of Education and Communities noted that the PPIP Act has no provision for charging an applicant for processing an access to information request. In comparison the GIPA Act provides an application fee of $30 for a personal application may be charged, although processing charges do not apply until 20 hours of processing has been spent. The HRIP Act also enables an organisation to charge a fee for providing access to an individual's health information. The Department commented that it incurs significant expense in processing applications under the PPIP Act in terms of time and resources and the ability to charge a fee can discourage unreasonable or frivolous requests. It also enables an agency to recover some costs that are incurred in processing these applications. The Department of Education and Communities recommended that the PPIP Act be amended to be consistent with the HRIP Act in charging a fee.

Privacy Direction on disclosure of information by public sector agencies for research purposes

The Department of Education and Communities commented on difficulties in interpreting and/or applying the Commissioner's "Direction on disclosures of information by public sector agencies for research purposes". Some difficulties identified include:

- What is considered to be "research purposes"? e.g. is it a request to compile the information into a data set for use by the body requesting it and provide it to others for research be research purposes or data collection?
- The Direction states that "... proposed research has been approved by a committee established for the purpose of giving ethical approval to research projects..." (emphasis added). Unlike universities, the Department does not have its own ethics committee
- The Direction refers to the need to follow guidelines or policies for research purposes which were established at 1 July 2000. It is unclear what this actually means. While the Commission has advised that this is the date from when the Direction applies, this is not clear from a reading of the Direction.

The Department commented that the uncertainty that arises from these points impacts on the Department's capacity to provide accurate advice to staff who have responsibility for the implementation of the PPIP Act at an operational level. The Department recommended that the Commission review this Privacy Direction to ensure greater clarity and ease of application.

Serious and imminent threat

The Department of Education and Communities commented on the provisions in sections 17, 18 and 19 of the PPIP Act that if there is a "serious and imminent threat" to the life or health of the individual concerned or another person then personal information may be disclosed or used by the Department. The Department commented that the requirement for the threat to be both serious and imminent could impact on the Department's capacity to address student wellbeing and safety concerns. The Department provided an example of where a school becomes aware that there is a serious but not imminent threat to the life or health of a student and any notification to the parent would be an apparent breach of the PPIP Act. The Department contends that it is the seriousness of the risk alone that should justify disclosure and use of personal information and recommended that the PPIP Act be amended to refer to a serious threat to the life or health of a person only in sections 17, 18 and 19.

Use of photographs in schools

The Department commented that an area that presents practical difficulties for schools in complying with privacy obligations is the use of photographs on school websites and publications. Cases arise where parents may not consent to their child being photographed but their child takes part in a school play or presentation. The school would not want to exclude the child from taking part but if photographs are taken of the play or presentation the child may be pictured. This means the views of one parent may override the views of many other parents. This can place the school in a difficult situation

2 Feedback from agencies (continued)

attempting to balance competing interests. Decisions that favour a single parent over the majority of other parents can lead to conflict within the school community. Schools may lose an opportunity to properly showcase the achievements of their students. The Department recommended that consideration be given to exempting schools from compliance with the PPIP Act in relation to school performances and similar activities.

Internal reviews

The Department of Education and Communities commented that the requirement to consult the Privacy Commissioner before the Department determines a privacy internal review can be helpful in ensuring issues raised by the Commissioner are considered prior to finalising a matter. However this can add a significant amount of time to completing a matter as there is no time frame within which the Commissioner must respond. It would assist if the PPIP Act contained a provision which provided the Commissioner is deemed not to have any comments if a response is not sent to an agency within a specified period of time. This would then enable the Department to determine the application without further delay. The Department recommended that the PPIP Act be amended to provide the Commissioner is deemed not to have any comments if a response to consultation is not sent to an agency within a specified period of time.

Collection and notice requirements

Transport for NSW observed that section 10 of the PPIP Act requires agencies to inform people of the physical address of the agency that holds their personal information. Transport for NSW commented that this requirement does not enhance the protection of customer privacy. The provision seems to reflect a paper-based approach to information retention, and doesn't sit neatly with cloud and other forms of electronic storage. It is also not consistent with the NSW Government cluster structure, where a shared services model is increasingly being used to improve delivery of services to customers.

Clarifying what an agency is for the purpose of use and disclosure of information

Transport for NSW sought clarification on what is an agency for the purpose of use and disclosure of information. Transport for NSW stated its understanding that under the PPIP Act, use of information refers to dealings within an agency, while disclosure refers to the release of information to third parties outside an agency. Transport for NSW observed that the definition of an agency in this regard creates problems for clusters such as Transport. Given that the NSW Government has moved to a centralised cluster structure as a best practice service model, it would be beneficial for agencies and for customers to reflect that structure in the PPIP Act. This would clarify that the sharing of information between agencies in the same cluster is a use rather than a disclosure.

Transport for NSW commented that this would also simplify the privacy notice requirements without compromising privacy protection. For example, customers supply personal information to Transport for NSW for the purpose of receiving a number of services. In order to provide those services, Transport for NSW may need to share information with other agencies in the cluster, such as RMS. The relevant privacy notice needs to specify that information will be shared with RMS even though that agency is in the same Transport cluster and is supplied and used for the same purpose. This can be confusing for customers and unnecessarily cumbersome. If information sharing within the same cluster was categorised as a use, the privacy notice could simply state that information supplied will be used within the cluster to fulfil the purpose for which it was supplied, or a directly related purpose.

Law enforcement exemptions

Transport for NSW sought clarification as to whether section 23(5) (d) (ii) of the PPIP Act applies to offences outside NSW when investigated by law enforcement agencies as defined in the PPIP Act. Transport for NSW noted that the law enforcement exemption in section 23 of the PPIP Act enables personal information to be provided to law enforcement agencies for law enforcement purposes. However, it is unclear if section 23(5) (d) (ii), which provides for disclosure to investigate an offence, includes offences outside NSW. Transport for NSW

commented that logically, that section should have extraterritorial application given that the PPIP Act defines a law enforcement agency to include law enforcement agencies in other States and Territories.

RMS also commented on section 23 exemptions. RMS noted that section 23(5) makes a distinction between "proceedings for an offence or law enforcement purposes" on the one hand and the "investigation of an offence" on the other. RMS commented that the distinction can be confusing and hard to determine in some cases (and in other cases the investigation and the enforcement can occur almost simultaneously). RMS stated that the distinction is an important one because RMS has legal advice that it is likely that "law enforcement" in section 23(5) (a) can refer to transborder law enforcement whereas the "investigation of an offence" in section 23(5) (d) (ii) probably cannot. The rationale for this is that the ordinary presumption against extra territoriality is displaced in the case of "law enforcement" because "law enforcement agency" is defined and is defined to include non-NSW agencies.

RMS explained that the current situation is difficult for NSW because when approached for assistance from non-NSW jurisdictions an assessment has to be made as to whether the information is requested to investigate an offence or protect public revenue or for law enforcement (with only the latter being permissible grounds for disclosure).

RMS recommended that section 23(5) be amended to:

- use a single expression "law enforcement" purposes to replace the current four expressions of "proceedings for an offence", "law enforcement purposes", "investigation of an offence" and "protection of public revenue";
- define "law enforcement purposes" to remove ambiguities;
- adopt (with minor change) the Federal definition; and
- confirm that law enforcement is not limited to NSW.

RMS also recommended the repeal of section 19(7) as the provision is confusing and would not be necessary if it was made clear that the proposed law enforcement exemption in section 23(5) applies both within and without NSW.

RMS also recommended that "law enforcement purpose" be aligned with the Federal definition that includes prevention and detection of offences. This would allow the RMS to use cameras at, for example, school crossings for detection of breaches of rules and avoid impracticalities associated with obtaining the consent of motorists for their vehicles to be filmed at school crossings.

2 Feedback from agencies (continued)

PART B – SURVEY OF PRACTITIONERS

The survey of privacy practitioners was distributed in mid-2014; 83 practitioners responded, with the majority representing local councils.[78] The survey focused on the requirements of the PPIP Act, privacy complaints generally and agencies' internal reviews of formal complaints. In addition, the challenges facing agencies and the capacity of the PPIP Act to meet these challenges were included.

Practitioners' responses indicate the PPIP Act requirement for agencies to advise the public of their privacy arrangements are met overall with 90% of practitioners saying their agency had a Privacy Management Plan as required by the PPIP Act. In addition, a majority indicated that their agencies produced further privacy guidance via privacy policies (55%) and privacy statements (54%). The majority of practitioners reported their agencies mainly advise customers about policies, procedures and practices relating to personal information through their websites (52%), customer service teams (28%) and other mechanisms such as frontline service providers (20%).

In terms of organisational arrangements for privacy, most practitioners reported that one organisational area is designated for privacy management (49%). Almost a third (32%) indicated that there was more than one area, while 19% didn't know. The majority of practitioners reported not receiving any privacy complaints during 2013 – 2014. As most complaints occur in service user interactions at the operational level and many are handled through general complaint handling mechanisms, this is not so surprising. Typically, it's when privacy concerns cannot be resolved through those mechanisms that privacy complaints are transferred to the agency's privacy practitioner. The largest number of complaints reported by one agency practitioner was 55 complaints, with another reporting 17. The highest number of internal reviews conducted by one agency was 40. Twenty-two practitioners reported investigating the complaints received. The majority reported that the findings of these investigations were that no breach of the IPPs occurred. Privacy complaints handled by agencies through their general complaint handling mechanisms do not have to be notified to the Privacy Commissioner.

While 70% of practitioners report information security and privacy management are included in their agencies' Audit and Risk Committee work program, only 7% reported that performance reviews were undertaken on privacy matters or systems in the preceding year. 77% reported that no privacy impact assessments were undertaken during 2013 – 2014. Three practitioners (one from a council, one from a NSW Government agency and one from a university) said that their agency had used a privacy impact assessment as a tool to assess privacy risks in the preceding 12 months. However, almost one in five practitioners indicated that such an assessment might have occurred without their knowledge.

Training was revealed as significant for practitioners. 80% of practitioners' report that their agencies' induction programs for staff included a segment on privacy responsibilities, while 12% indicated privacy was not included and 8% did not know. Most practitioners sought more training and more training resources. In terms of the specific resources sought, there was a theme of tailoring materials for councils and councillors and specifically smaller, rural and regional councils. Many requests were for online training including webinars, however there was a strong emphasis upon attendance training particularly in regional areas. Topics mentioned included case studies, privacy impact assessments, complaint handling, cloud computing and social media. Local councils sought training particularly in relation to development applications. One heartfelt comment on what resources would be useful was "Anything really".

It was difficult for practitioners to report the amount of training undertaken as most did not know. A minority of practitioners were able to give details with one practitioner reporting 500 staff receiving privacy training throughout 2013 – 2014 and another reporting 225.

No practitioner reported changes to their agencies' legislative or administrative arrangements that had implications for the administration of the PPIP Act. In terms of difficulties for agency operations raised by the PPIP Act, 71% reported that there were no issues. The majority of practitioners (52%) reported that their agency did not utilise instruments such as the Public Interest Directions or Privacy Codes of Practice that modify the application of the IPPs, while nearly one third indicated their agency did utilise these instruments (32%), and 17% did not know.

78. The number of privacy practitioners is unknown as a number of agencies employ more than one privacy practitioner and other agencies share the role with other legal or right to information roles.

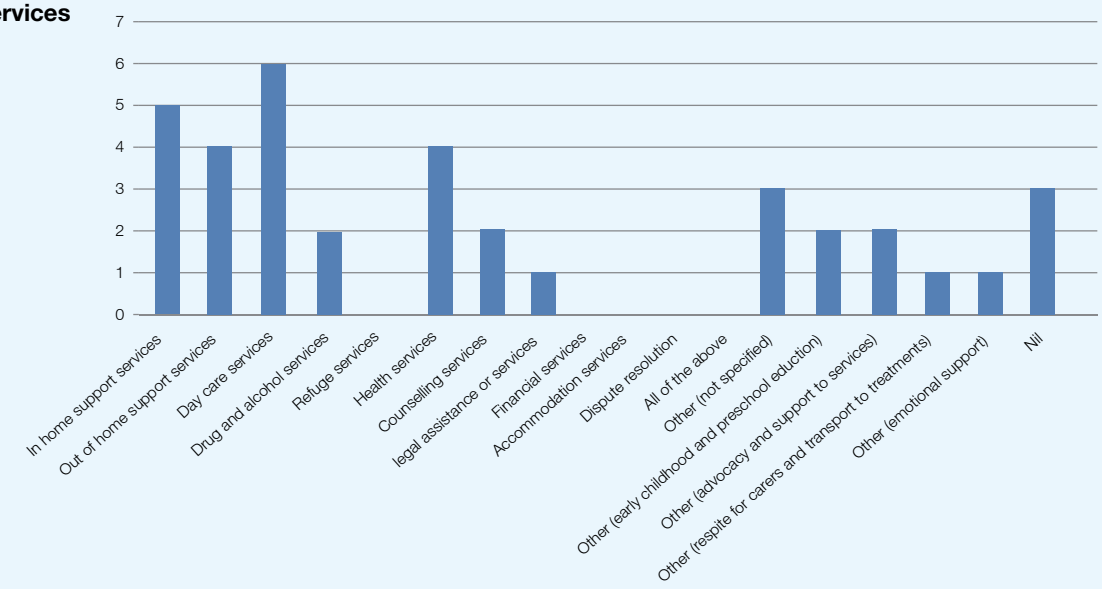
3 Feedback from non-government organisations

The survey of non-government organisations (NGOs) was distributed in October 2014. Responses were received from 26 non-government organisations.

Types of services

The types of services provided by the organisations responding to the survey are set out in the following table. The majority of NGO survey respondents were providing day care services, in home support services, out of home services and health services.

Types of services provided



Client groups served

Client groups served by the responding NGOs were families, children and clients with a broad range of needs.

Client group served	Number of NGOs
Families	13
Children	17
People with disabilities including mental health issues	10
Women	8
Men	8
Aboriginal and Torres Strait Islanders	8
Culturally and linguistically diverse (CALD) communities	7
Remote communities	3

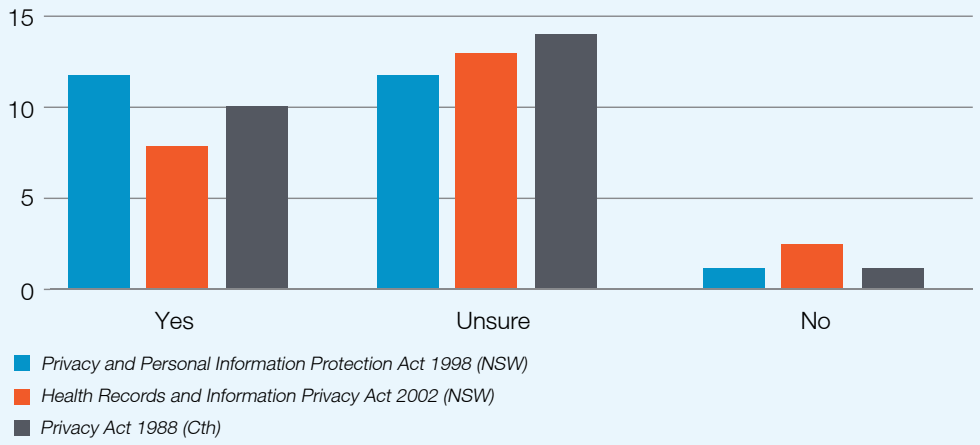
Client group served	Number of NGOs
Older people	8
Domestic violence victims	1
Youth	3
Homeless	2
Domestic violence victims	3
Substance abuse	3
Financial difficulties	2
Refugees/asylum seekers	2
Other (palliative care)	2

3 Feedback from non-government organisations (continued)

Awareness of privacy obligations

The responding NGOs were generally unsure about their obligations under either NSW or Commonwealth privacy legislation as shown in the following chart.

Awareness of State and Commonwealth privacy legislation requirements



Funding and contractual arrangements

Twenty-one of the NGOs (81%) responding to the survey advised that they received funding from the NSW Government. Only one indicated that it did not receive funding from the NSW Government, three provided a nil response and one organisation was unsure.

The majority (20) organisations indicated that they had a service agreement with Government for the provision of the services covered. Five organisations provided a nil response and one organisation was unsure.

Twelve organisations responded that the agreements required them to comply with NSW privacy legislation, the PPIP Act and/or the HRIP Act. One organisation reported that there was no obligation, seven organisations were unsure and six provided a nil response.

Advice and assistance on privacy matters

Fourteen NGOs said they would go to their professional or peak body for any queries they may have regarding their organisation's privacy practices. Twelve NGOs said that they would seek advice from their funding body and four said they would seek advice from a similar organisation. Three said they would seek advice from the Commonwealth Privacy Office, three from the NSW Privacy Office, two from a lawyer and two from other sources including the NGO management office and Medicare Local. Two organisations provided a nil response.

Five NGOs said that they require assistance in implementing NSW privacy requirements in their organisation's operations, 13 indicated that they did not require assistance, six were unsure and two provided a nil response.

Of the five NGOs that said they require assistance in implementing NSW privacy requirements, the sort of assistance that would be useful were online resources (4), online training (3), legal advice (3), enquiry service (2), management advice (2) and face-to-face training (2).

The majority of responding NGOs had not heard of the Information and Privacy Commission (13) although 11 had and two provided a nil response.

4 IPC data on complaints and internal reviews

Complaints (non-internal review)

In the period 1 July 2013 to 30 June 2014, 96 complaints were received relating to State Government agencies (39), private health providers (27), local government (5), universities (1) and other organisations (24). Data on the source of the complaints is not available.

The complaints covered a number of issues including alleged breaches of the information protection principles (IPPs), the health privacy principles (HPPs), privacy issues and general issues relating to the PPIP Act, the HRIP Act and the *Privacy Act 1988* (Cth).

The majority concerned alleged disclosure of personal information particularly of health information, followed by complaints around the ability to access personal information held by a NSW public sector agency.

Focusing just on those complaints made under the PPIP Act, the following table sets out the number received by IPP and relevant legislation. (Those outside the scope of NSW privacy legislation are referred to other relevant bodies.)

Complaints	Number
Information protection principles	
All IPPs	1
IPP 1 – Collection of personal information for lawful purposes	2
IPP 3 – Requirements when collecting personal information	2
IPP 4 – Other requirements relating to collection of personal information	2
IPP 5 – Retention and security of personal information	2
IPP 7 – Access to personal information held by agencies	6
IPP 10 – Limits on use of personal information	3
IPP 11 – Limits on disclosure of personal information	11
Legislation	
IPC legislation/PPIP Act	13
IPC legislation/HRIP Act	19
Commonwealth legislation/ Federal *Privacy Act 1988*	5
Privacy issues/National Privacy Principles/NPP 2 – Use and disclosure	4

4 IPC data on complaints and internal reviews (continued)

Internal reviews

One hundred and fifty seven (157) internal reviews were notified to the Privacy Commissioner from 1 July 2013 to 30 June 2014.

The internal reviews involved a number of agencies including State Government agencies (114), local councils (19), universities (20), statutory bodies (3) and other organisations (1).

The issues that were the subject of the internal reviews included IPPs, HPPs, privacy issues and legislation as shown in the following table.

Internal review	Number
Information protection principles	
All principles	1
IPP 1 – Collection of personal information for lawful purposes	8
IPP 2 – Collection of personal information directly from individual	5
IPP 3 – Requirements when collecting personal information	3
IPP 4 – Other requirements relating to collection of personal information	3
IPP 5 – Retention and security of personal information	21
IPP 7 – Access to personal information held by agencies	11
IPP 8 – Alteration of personal information	1
IPP 9 – Agency must check accuracy of personal information before use	4
IPP 10 – Limits on use of personal information	21
IPP 11 – Limits on disclosure of personal information	45
IPP 12 – Special restrictions on disclosure of personal information	1
Legislation	
PPIP Act	49
HRIP Act	14
Children and Young Persons (Care and Protection) Act 1998	1
GIPA Act	2

5 Reporting on privacy in annual reports

Departments

Under clause 6(a) of the *Annual Reports (Departments) Regulation 2010,* Departments (defined in section 3 of the *Annual Reports (Departments) Act 1985* as a person, group of persons or body specified in Column 1 of Schedule 3 to the *Public Finance and Audit Act 1983*) are required to include in their annual reports a statement of the action taken by the Department in complying with the requirements of the PPIP Act.

A review of annual reports for the 2012 – 2013 indicated that 20 of the 29 Departments listed at Schedule 3 to the *Public Finance and Audit Act 1983* reported on action taken in complying with the requirements of the PPIP Act. Two Departments did not report. Annual reports for seven Departments were not available as they were included in the annual reports for their cluster Department, they were a newly established Department or the reports could not be located. The 20 Departments that reported on actions taken in complying with the PPIP Act reported on a range of initiatives as set out in the following table. The three most frequently reported initiatives were the existence or review of privacy management plans, dedicated privacy officers or teams, and online learning modules.

Initiative	Number of Departments
Privacy management plan (including review of plan and development of department-wide plans for large cluster Departments)	15
Designated privacy officer/team	5
Online learning modules	5
Training and information sessions for staff	3
Guidelines, brochures and leaflets	3
Review of privacy statements to members of the public	3
Online resources available via the Department's intranet	2
Seminars and workshops	1
Presentations to groups, meetings and committees	1
Privacy officer network meetings	1
Maintenance of databases so as to comply with the PPIP Act	1
Audit access to records and other systems to ensure compliance	1
Compliance with best practice code for information management	1
De-identified data used for research	1
Privacy is integral to the exercise of the Department's functions	1
Privacy impact assessments	1
Review of corporate policy instruments	1

5 Reporting on privacy in annual reports (continued)

Statutory bodies

Section clause 10(3)(a) of the *Annual Reports (Statutory Bodies) Regulation 2010* requires statutory bodies (defined in section 3 of the *Annual Reports (Statutory Bodies) Act 1984*) to include in their annual reports a statement of the action taken by the body in complying with the requirements of the PPIP Act.

The Information and Privacy Commission analysed annual reports of 34 statutory bodies including 10 universities. The majority of the sample (28) included a statement of the action taken by the body in complying with the requirements of the PPIP Act. Annual reports were not available for six of the statutory bodies as they were included in larger Department annual reports, the body was newly established or the annual reports could not be located.

Statutory bodies other than universities

The 18 statutory bodies other than universities that provided statements on action taken in complying with the PPIP Act mainly referred to the existence of a Privacy Management Plan and/or the intention to review the Privacy Management Plan to ensure its currency and relevance with organisational changes. Other initiatives reported are set out in the table, right:

Initiative	Number of statutory bodies (non universities
Privacy Management Plan (including review to ensure currency and relevance)	15
Dedicated Privacy Officer	2
Privacy statement for the public on the website	1
Privacy Code of Practice	1
Training sessions	3
Brochure and information leaflets	1
Information available for staff on the website	2
Identifies collections of information that might include personal information and ensure security and protection of the information	1
Network meetings	1
Information provided at point of collection on use and disclosure of any personal information	1
Review of maintenance and storage of information	2

Universities

The reports of 10 universities were reviewed. The universities reported a range of approaches and initiatives to ensure compliance with the PPIP Act. These are shown in the table, right:

Initiative	Number of universities
Privacy Management Plan (including review to ensure currency and relevance)	9
Training	7
Information leaflets/guidelines	5
Online resources	3
Website	4
Privacy assessment	3
Privacy advice	4
Review of systems and processes	3

office of the privacy commissioner
new south wales

information and privacy commission
new south wales

Level 11, 1 Castlereagh Street, Sydney 2000

GPO Box 7011, Sydney NSW 2001

1800 IPC NSW (1800 472 679)

Fax: (02) 8114 3756

ipcinfo@ipc.nsw.gov.au

www.ipc.nsw.gov.au

Our business hours are 9am to 5pm
Monday to Friday (excluding public holidays)