office of the privacy commissioner
new south wales

NSW Informational Privacy Rights:

Legislative Scope and Interpretation - Employer, Employee, and Agent Responsibilities

A Special Report under Section 61C Privacy and Personal Information Protection Act 1998

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

The Office of the NSW Privacy Commissioner is located at:

Office address:
Level 3, 47 Bridge Street
Sydney, NSW 2000

Postal address:
PO Box R232
Royal Exchange NSW 1225

Free call:
1800 IPC NSW
(1800 472 679)

Direct line: (02) 9258 0066

Fax: (02) 8114 3756

Email: privacy@ipc.nsw.gov.au

Web: www.ipc.nsw.gov.au/privacy

If you are deaf or have a hearing or speech impairment, you can call us through National Relay Service (NRS) on 133 677 or if you like the assistance of an interpreter, call us through the Translating and Interpreting Service (TIS) on 131 450.

ISBN: 78-0-9876237-0-6

Letters of Transmission

The Hon. Trevor Khan MLC
A/President, Legislative Council
Parliament of NSW
Parliament House
Macquarie Street
Sydney NSW 2000

20 February 2017

Dear A/Mr President,

In accordance with the section 61C of the *Privacy and Personal Information Protection Act 1998* (PPIP Act), I am pleased to present the following Special Report to raise awareness of the issues outlined within and to aid the development of appropriate legislative, policy and procedural responses.

A copy of the report has been provided to the Attorney General as Minister responsible for this legislation as specified under section 61C(1) of the PPIP Act.

I provide this report to the Parliament for tabling.

Yours sincerely,

Dr Elizabeth Coombs
A/NSW Privacy Commissioner

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

20 February 2017

Dear Madam Speaker,

In accordance with the section 61C of the *Privacy and Personal Information Protection Act 1998* (PPIP Act), I am pleased to present the following Special Report to raise awareness of the issues outlined within and to aid the development of appropriate legislative, policy and procedural responses.

A copy of the report has been provided to the Attorney General as Minister responsible for this legislation as specified under section 61C(1) of the PPIP Act.

I provide this report to the Parliament for tabling.

Yours sincerely,

Dr Elizabeth Coombs
A/NSW Privacy Commissioner

Commissioner's Foreword

In discussing the impact of new technologies on privacy, Professor Butler commented:

> *"While in a democratic society the state may have an interest in preserving the autonomy of its citizens from invasions of their privacy, the value of such prohibitions may depend upon the willingness of the relevant authorities to prosecute transgressions. In any event, it is the individual who has his or her dignity or autonomy affronted that has the greater interest in preventing or redressing the wrong. Any appropriate legislative response should therefore make provision for reparation for individuals who have been aggrieved by invasions of their privacy."*1

Misuses of personal information and data breaches are not random events; they result from poor organisational governance and practice, and the conduct of employees and contractors. Organisations, whether public or private, generally do the 'right thing', as do employees and contractors, but data breach notifications and complaints to my Office are increasing. This is not isolated to NSW. In 2016, the Queensland Crime and Corruption Commission revealed that the misuse of confidential government information was not just one of the most common corruption allegations made, but an increasing percentage having almost doubled from 2014-15.

Members of the public have every right to expect that their personal information is not being placed at risk by poor organisational practices, nor accessed by or disclosed to anyone who does not have legitimate authority to use it. When such incidents occur, it is important that those affected have recourse.

NSW privacy legislation has stood the test of time well overall, but there are gaps, as outlined in my 2015 statutory report on the operation of the *Privacy and Personal Information Protection Act,1998* (PPIP Act). The gaps this report focuses on, concern the action that can be taken by individuals when public and private organisations' employees intentionally breach privacy requirements, and when public sector contractors do not handle personal information according to the legislation.

The proposed improvements entail amendments to the PPIP Act and the *Health Records and Information Privacy Act, 2002* (HRIP Act) to increase the accountability of employees and contractors. The amendments are not novel; they are working successfully in other laws, and their adoption will make provision for reparation by individuals who have been aggrieved by incursions into their privacy.

The report is made as a special report to the NSW Parliament under section 61C of the PPIP Act to raise awareness of these issues and to aid the development of appropriate legislative, policy and procedural responses. Public debate and action are needed in this important area given the rapid changes the NSW public and service providers are experiencing as a consequence of the advances in digital technology.

This report is the product of the work of members of the Office of the Privacy Commissioner. I particularly acknowledge the primary contribution of Mr Nick Yetzotis, without his work this report would not have been possible. I also thank Ms Amy McKenna for the design work for this report.

Dr Elizabeth Coombs
A/NSW Privacy Commissioner

[1] Professor Des Butler (2014) "The dawn of the age of the drones: An Australian Privacy Law perspective" 37(2) *University of NSW Law Journal* 434, 469.

Executive Summary

Many areas of law regulating the responsibilities of government agencies and private service providers include provisions that require those organisations to have comprehensive systems in place for the protection of the rights of persons with whom they have dealings, for example tort, anti-discrimination, and workplace safety laws. Similarly, and additionally, laws and administrative systems are also in place to protect the property that organisations hold from corrupt exploitation by employees and their agents.

Collecting, handling, and disclosing personal and health information is a major activity in many modern organisations. As with obligations under other laws and community expectations, in order to deal with information in ways that help organisations maintain the trust of the community and avoid liabilities, an information ethics and governance framework needs to have a central place in every organisations' culture, in prevent privacy breaches and misuse of personal and health information.

NSW privacy legislation provides mechanisms for the enforcement of the informational rights of individuals, and the prosecution of employees and agents for corrupt misuse of personal information held by the organisations that engage them. It also places obligations on the public sector to ensure its agents (such as contractors) handle personal information respectfully. But there are gaps; current NSW privacy legislation does not provide adequate protections when:

- employees of public or private organisations commit intentional privacy wrongdoings.
- public sector contractors do not handle personal information according to the legislation.

This report looks at these issues and proposes legislative solutions that will better secure the privacy rights of individuals by overcoming these two shortcomings by adopting mechanisms already established in other laws.

Recommendations

Recommendation 1:
Amend the PPIP Act and the HRIP Act to allow victims of privacy breaches to have a right to complain against both a public sector agency and relevant employees. That is, to request that the Tribunal make employees second respondents in cases where a public sector agency claims that its data security safeguards were adequate and that the agency should not be liable for the alleged conduct of its employees who contravened privacy law.

Recommendation 2:
Amend the HRIPA Act to allow victims of privacy breaches to have a right to complain against both a private sector organisation and relevant employees. That is, to request that the Privacy Commissioner make employees second respondents in cases where a private sector organisation claims that its data security safeguards were adequate and that the organisation should not be liable for the alleged conduct of its employees who contravened privacy law.

Recommendation 3:
Base amendments of both NSW privacy statutes (PPIP Act and HRIP Act) upon sections 36 and 37 of the Queensland *Information Privacy Act 2009* and section 95B of the Federal *Privacy Act 1988* to enable the public sector to choose to retain responsibility for any privacy contravening conduct of its contractors and subcontractors, or alternatively, to enter into contracts that make contractors and any subcontractors directly liable as if they are public sector agencies.

Recommendation 4:
Amend section 12 of the PPIP Act and HPP5 in Schedule 1 of the HRIP Act to require public sector agencies and private organisations, as may be applicable, to have in place both proactive and reactive measures to prevent data breaches in line with section 53 of the NSW *Anti-Discrimination Act 1977.*

Contents

Part 1: Introduction

Matters coming to the attention of the NSW Privacy Commissioner regularly raise issues of employer, employee and agent responsibilities and the interaction of these under the NSW privacy legislation. These questions arise in statutory work relating to:

- Oversighting privacy investigations conducted by NSW public sector agencies in response to complaints made by citizens;
- Investigating complaints regarding alleged health privacy contraventions by private sector organisations;
- Reviewing public sector agencies' Privacy Management Plans and providing assistance to agencies to better comply with privacy principles;
- Responding to requests for statutory advice from agencies, the private sector and members of the public, concerning unauthorised use and disclosure of personal and health information by employees;
- Making submissions in the NSW Civil and Administrative Tribunal's (NCAT) hearings of privacy complaints.

The purpose of this report is to place in the public domain matters relevant to the responsibilities of employers, employees and agents, such as contracted service providers, for privacy and management of personal and health information.

These matters are growing in importance as advances in technology enable an increasing capacity to collect, store and manipulate vast quantities of information about individuals.

Awareness of the current and future impacts upon the people of NSW has triggered this statutory report to Parliament under section 61C of the PPIP Act. This section enables the Privacy Commissioner from time to time to make a special report on any matter relating to the functions of the Privacy Commissioner to the Presiding Officer of each House of Parliament, and to provide a copy of the report to the Attorney General.

The work of Privacy Commissioners internationally includes giving advice and raising awareness whereby Privacy Commissioners "*frequently play a lead role in laying down how data privacy law is understood and applied, even in contexts where their views on point are only advisory*."[2]

In turn, the Privacy Commissioner's ability to provide sound advice on privacy matters is facilitated by consultation with the broader community. Accordingly, the Privacy Commissioner will consult on the issues and recommendations in this report.

[2] Lee Bygrave, *Data Privacy Law: An international perspective*, 2014, Oxford University Press, Oxford, 4

Part 2: The structure of this report

This report discusses the provisions of the PPIP Act and the *Data Sharing (Government Sector) Act 2015* that regulate informational privacy in the NSW public sector and aspects of the HRIP Act that contribute to health privacy regulation in the public sector and some of the NSW private sector, in order to highlight issues concerning:

- responsibilities of employers and employees, and the situation relating to privacy protection obligations applying to agents that is, contracted service providers;
- legislative interpretation and judgments on these issues;
- the gaps in the regulatory reach of the legislation; and
- possible mechanisms to address these gaps.

The report is divided into two main sections. The first section has seven parts which discuss:

- the significance of data breaches and the harms they cause to individuals;
- the specific way by which the NSW privacy legislation attributes responsibility to employers, employees and agents/contractors;
- the critical place a data governance culture has in protecting privacy;
- the gaps in privacy rights protection in the NSW legislation, and, examples of better regulatory coverage used in other laws; and
- recommendations for amendments to NSW privacy legislation.

The second section, the Annexures, sets out:

- the complaints resolution mechanisms and the responsibilities of those who become involved in complaint resolution;
- mechanisms available and used in related areas in NSW;
- the elements of a good data security governance framework; and
- the ways in which other laws hold employers responsible for the negligent or intentional conduct of employees or agents as a point of comparison with the way in which the NSW Court of Appeal has interpreted the NSW privacy legislation.

To avoid unnecessary complexity the report focuses on the PPIP Act. The HRIP Act is discussed only to illustrate particular points as relevant.

Part 3: The significance of data breaches

Privacy is undermined by the curious, the malicious, by criminal interests, by inadequate information management systems, by employees' failure to comply with the systems, by poor understanding of obligations and by inadequate governance.

Recent reports highlight the need for sound organisational information governance within public sector agencies and service providers contracted to those organisations.[3]

Public and private organisations collect and hold vast quantities of personal information in order to deliver modern services. Storage in computerised databases brings together, in one place, large quantities of personal information about individuals. This makes it easily accessible for legitimate purposes, but also potentially, for unauthorised and unlawful purposes. The risks to individuals, whose personal information can be used by those motivated by mischief, is increased as a result.

In 1992 the Independent Commission Against Corruption (ICAC) concluded an Inquiry into "*a massive illicit trade in Government information …… conducted with apparent disregard for privacy considerations, and a disturbing indifference to the concepts of integrity and propriety*."[4] The information in question was held by public sector organisations and traded by employees. It concerned the financial, health and personal details of many citizens. The monetary value of this information made it extremely lucrative for those engaged in this illicit trade.

Now 25 years later, data flows between public sector organisations, from these organisations to the private sector, and from the public sector to the community sector have increased even more in volume. Technology makes it easy to trigger a movement of information making the individuals more vulnerable to improper flows of personal data without their consent and without legitimate reason.

Big data research creates a requirement for the bulk transfer of personal, and often sensitive, information away from the control of the primary data custodians. This expands the risks of misuse of data and identity theft by individuals and organised underground markets.

Data breaches are a significant social issue and are regularly reported in the press. Recent research shows data breaches are on the rise, both in terms of frequency and the significance of the harm they cause. Research data in the United States of America suggests that 52% of breaches were mostly the work of malicious insiders.[5] The same trends have been reported in Canada in the areas of civil liability and regulatory action.[6] The Digital Guardian has also recently reported on the significance of the issue.[7]

Data breaches are not random events or 'just accidents'. They result from poor organisational governance and the behaviour of employees and contractors or a combination of the two. As organisations have increased the strength of their IT security systems to withstand hackers, attackers are "*using new and effective ways to get people in organisations to help them circumvent security controls*."[8] No organisation can assume a data breach will not happen to them. Unlawful curiosity and corrupt use, and wrongful disclosure of personal information can be committed by employees of both public and private organisations as well as all types of organisations including those entrusted with safeguarding the community's interests.

For example, information regarding unauthorised handling of information by police in the United Kingdom shows there were 2,315 incidents from June 2011 to December 2015.

[3] Victorian Commissioner for Privacy and Data Protection (2017) *"Review of Informational Governance in the Department of Health and Human Services (DHHS),* January Melbourne

[4] Independent Commission Against Corruption (1992) *Report on Unauthorised Release of Government Information*, Sydney, *Vol 1, 3*

[5] Covington, Inside Privacy (30/4/14) "*Data breaches on the rise in 2014,*" at: https://www.insideprivacy.com/data-security/data-breaches-on-the-rise-in-2014/

[6] Canadian Medical Association Journal, News (6/3/12) "*Medical privacy breaches rising*;" Information and Privacy Commissioner of Ontario (2015) "Detecting and deterring unauthorised access to personal health information," at: www.ipc.on.ca

[7] The Digital Guardian (27/6/16)

[8] ComputerWeekly.com (27/5/15) *Social engineering attacks,* at: http://www.computerweekly.com/news/4500247025/Social-engineering-attacks-more-complex-than-ever-says-expert

How these incidents are dealt with and the outcomes are relevant to this report. In relation to these UK incidents, the police forces took the following actions:

297 (13%) resignation or dismissal.
70 (13%) conviction or caution.
258 (11%) written or verbal warning.[9]

Unauthorised information handling has not only occurred within law enforcement bodies. Again in the United Kingdom, there were high numbers of data breaches with a concentration of incidents in the health sector with a high probability that human malice was the cause.[10]

There is no reason to believe that human nature and these behaviours or their drivers are isolated to countries overseas and are not manifested in NSW. To the contrary, it seems if the particular events and behaviours reported by ICAC in 1992 are any indication, that to deny the need to manage this risk would be foolhardy.

Recently, public officials in New South Wales and other Australian states have been convicted for improper access to, and disclosure of, official records.[11] Currently, breaches of the privacy legislation by employees are more likely to be treated as 'misconduct' and handled by the Human Resource Divisions of public sector organisations than brought to the attention of the Privacy Commissioner's Office. As there are no mandatory data breach notifications provisions under the PPIP Act, the quantum of occurrences is unknown. Not all States are in this position however and some have statistical information which illuminates the issue.

In Queensland, in one year to June 2016 the Crime and Corruption Commission undertook 15 investigations related to abuse of confidential information by employees. These resulted in 81 criminal charges and 11 disciplinary recommendations. Despite the existence of potential criminal offences, the Queensland Crime and Corruption Commission reported the misuse of confidential information remains one of the most common types of corruption allegations referred to them.[12]

Statistics for similar investigations in NSW could not been located. But in recent times there has been an accelerating trend of data breach incidents and expressions of concern that have come to the NSW Privacy Commissioner's attention. These include:

1. Employees of public and private organisations improperly accessing and disclosing the personal information of customers and other employees for their own purposes. For example, to use:
   - against their colleagues in neighbourhood disputes;
   - health information in witness statements in family law or inheritance disputes;
   - other people's personal identifiers to avoid paying their own parking fines and highway tolls;
   - to discredit another person in workplace disputes.
2. Researchers obtaining medical records, including identity details, from health service providers without patient consent and then sending spam to the subject person.
3. Public officials sending broadcast emails to large numbers of recipients without using the "blind copy" facility of the email software, resulting in large numbers of people learning about the personal affairs of others without legitimate reason;
4. Students undertaking practical training in public sector agencies, taking home records with personal information of clients and then losing these records, or they are stolen;
5. Public agencies losing portable equipment or machinery that have inbuilt data storage units with personal or health information;
6. Public officials and government contractors mailing hard copy correspondence to wrong addresses;

[9] Big Brother Watch (2016) "Safe in police hands? How police forces suffer 10 data breaches every week and still want more of your data," at: www.bigbrotherwatch.org.uk

[10] Information Commissioner's Office (29/4/16) "*Data security incident trends*" at: www.ico.gov.uk

[11] Examples from the criminal courts are: *Salter v The Director of Public Prosecutions (NSW)* (2011) NSWCA 190 – police officer; *Hughes v R* (2014) NSWCCA 15 – police officer; *Braimah- Mahamah v R* (2016) NSWDC 138 - prosecuting lawyer; *Cogan v Velkovski* (2016) WASC 158 – police officer. In June 2015 a person engaged to do work at the NSW Ambulance was convicted at the Downing Centre Local Court, Sydney for giving the health information of NSW Ambulance employees to a private solicitor.

[12] Queensland Crime and Corruption Commission (May 2016) "*Confidential information: Unauthorised access, disclosure and the risks of corruption in the Queensland public sector*"

7. Poor software design that leads to large scale data leaks;
8. Using personal information for in-house human research or releasing it to external researchers without a privacy impact assessment or a compliance check against privacy legislation; and
9. Information transfers to organisations without due diligence checks on the adequacy of data security measures to protect data from insider abuse and external attacks.

As pointed out, in 2016 by the Queensland Crime and Corruption Commission, *"Once information is released from an agency without proper authority, there is no guaranteed control over it. Even if the original release was not intended to cause harm, the agency cannot know who may come to possess it or how they might use it."*[13]

This Office frequently hears from members of the public of the consequences of intrusions upon privacy and breaches of personal and health information. The nature of our work means, however, that the detail of those individual cases cannot be discussed unless they are in the public arena.

One matter in the public arena concerning a grievous and offensive breach of privacy which NSW privacy legislation could not address was brought to the attention of the Parliament. The report of the NSW Parliament's Standing Committee on Law and Justice's Inquiry into *Remedies for the serious invasion of privacy in New South Wales* describes this case in sufficient detail.[14] The case of "Witness A" best describes, on the one hand, the devastating impact a privacy breach causes on the victim, and on the other hand, the absence of adequate enforcement of rights in NSW.

Witness A gave evidence to this Inquiry of the NSW Parliament's Standing Committee on Law and Justice. She described how, while under anaesthesia in a private hospital for a routine gynaecological procedure, a nurse took a photograph for non-work related purposes of Witness A's genitals using her iPhone.

Witness A was informed five weeks later when she was told that the nurse had shown the photograph to other nurses, who then made a complaint to the hospital. Witness A had to take leave from work due to the effect upon her. Her fears were that the photograph would end up on the internet, would be seen by her students, and as she was residing in the area of the nurse's residence, she feared that her child may be shown the photograph. Witness A paid for the costs of psychological assistance and for the costs of the services of a solicitor. She also actively sought redress to prevent a repeat of this behaviour occurring to other patients. All of her efforts were to no avail.

The HRIP Act's provisions for corrupt disclosure or use of health information apply to public sector officials not those in the private sector.

The NSW Privacy Commissioner acknowledged to the Committee the inadequacy of privacy law and said:

> "[*Disseminating intimate images without consent] most definitely is not acceptable behaviour. It is extremely offensive. It gives us a sense of a different way that violence can be perpetrated in our community than it once was. Once you could shut your door on people who wished to attack you. But now with cyber identity and a cyber profile there is the means to put things out beyond just your immediate circle to the whole world. It is incredibly damaging to the individual. It strikes at the heart of who they are and what they are."*[15]

Witness A's evidence captured the impact upon people of serious and offensive invasions of privacy, when she said:

> "*I felt I had no hope of controlling its distribution and my world fell apart.*
>
> *….I was worried I would see this image plastered on the internet and lose my teaching career."*[16]

---

13 Queensland Crime and Corruption Commission (May 2016) "*Confidential information: Unauthorised access, disclosure and the risks of corruption in the Queensland public sector,*" 3.

14 NSW Parliament, Standing Committee on Law and Justice (March 2016) Report - *Remedies for the serious invasion of privacy in New South Wales*, Sydney.

15 A fuller description of this case is at: NSW Parliament, Standing Committee on Law and Justice (March 2016) Report - *Remedies for the serious invasion of privacy in New South Wales*, Sydney, 20 -21

16 Reported at The Lamp – NSW Nurses & Midwives' Association (14/5/2016), at: www.nswma.asn.au/call-for-privacy-law-reform-after-not-so-smart-phone-abuse

The Committee recommended a statutory tort action to provide remedy for victims, such as Witness A, for horrendous breaches of their privacy.[17] The Government did not accept this recommendation and instead announced it would introduce legislation to make 'revenge porn' a criminal offence. It also did not accept the recommendation that the Privacy Commissioner be given the ability to make orders for non-financial remedies (such as apologies).

The commitment to address 'revenge porn' is supported, but this criminal offence if introduced, will not address the privacy breach experienced by Witness A nor provide others like her, with a remedy.

Criminal offences are effective means of society expressing in the strongest terms the odium with which certain conduct is regarded but they do not provide control to the victim of the privacy breach on their complaint or provide for the outcomes and remedies available in the complaints process under privacy legislation. Prosecution is an action by the State; it does not necessarily vindicate the complainant's privacy right.

The absence of civil remedies for serious invasions of privacy makes it even more important that the NSW privacy legislation protects individuals and provides real mechanisms for those who experience privacy offences, to have their complaints considered and those who perpetuated serious breaches of their privacy held to account.

[17] NSW Parliament, Standing Committee on Law and Justice (March 2016) Report - *Remedies for the serious invasion of privacy in New South Wales*, Sydney, 9

Part 4: NSW privacy legislation

The NSW privacy legislation protects privacy by:

- Providing the Privacy Commissioner with functions and certain powers to deal with issues that affect the privacy concerns of the community (sections 36, 37, 38 PPIP Act);[18]
- Regulating the conduct of public sector agencies, and the private sector in some circumstances, regarding information privacy;
- Providing reserve powers to the Privacy Commissioner to investigate matters affecting the privacy of individuals more generally.

The legislation does not provide for a general right to privacy,[19] but focuses on obligations to handle the personal and health information held by organisations to facilitate their functions, in accordance with specified principles in PPIP Act and the HRIP Act and described below.

The privacy right is found in principles contained in international human rights instruments.[20] The rights in the privacy legislation enabling a complainant to seek remedies are consistent with those principles. The Appeal Panel of the NSW Tribunal described the PPIP Act as a "*landmark piece of human rights legislation*."[21]

As principles based legislation to be applied consistently with Australia's international obligations, the interpretation of privacy law must not restrict or dilute the operation of the privacy protections it provides.[22]

Privacy obligations

The PPIP Act sets out 12 Information Privacy Principles. These are legal obligations, with which NSW public sector agencies must comply when they collect, store, use, disclose or dispose of personal information (section 20). The principles are:

- **IPP 1:** Collection of personal information for lawful purposes *(section 8)*
- **IPP 2:** Collection of personal information directly from individual *(section 9)*
- **IPP 3:** Requirements when collecting personal information *(section 10)*
- **IPP 4:** Other requirements relating to collection of personal information *(section 11)*
- **IPP 5:** Retention and security of personal information (section 12)
- **IPP 6:** Information about personal information held by agencies (section 13)
- **IPP 7:** Access to personal information held by agencies (section 14)
- **IPP 8:** Alteration of personal information (section 15)
- **IPP 9:** Agency must check accuracy of personal information before use (section 16)
- **IPP 10:** Limits on use of personal information (section 17)
- **IPP 11:** Limits on disclosure of personal information (section 18)
- **IPP 12:** Special restrictions on disclosure of personal information (section 19)

The application of the principles to public sector agencies may be modified by privacy codes of practice [section 20(2)] or public interest directions issued under section 41.

Complaints made by individuals usually concern the 'use' and 'disclosure' principles.

---

18 When exercising these functions the Commissioner does not have determinative powers and can only provide advice and recommendations.

19 As is also the case in other Australian States and Territories: *Jurecek v Director, Transport Safety Victoria* [2015] VCAT 253, [57]; discussing the equivalent Victorian legislation

20 These being the 1948 Declaration of Human Rights and the International Covenant on Civil and Political Rights, stated in *Commissioner of Police v District Court of NSW* (1993) 31 NSWLR 606

21 *Vice Chancellor, Macquarie University v FM* [2003] NSWADTAP 43, [41]

22 *Jurecek v Director, Transport Safety Victoria* [2016[VSC 285, [61] & [64]

The "Use" Principle (section 17) regulates how an agency may use personal information. In summary:

- The agency must "hold" this information in relation to its functions or the services it provides.
- A use must be for the purpose regarding which the information was collected.
- A use may be for another purpose, directly related to the purpose of the original collection.
- A use for another purpose must be with the person's express or implied consent. [23]

A use for another purpose can occur without consent if it is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or another person.

The "Disclosure" Principle (section 18) regulates the disclosure of information. A disclosure involves the movement of information, typically outside the agency. (There may be infrequent circumstances where disclosure from one part of an organisation to another may amount to a disclosure for purposes of the PPIP Act.)

The section also raises the question of what is a disclosure for a purpose directly related to the original collection of the information. Consent for section 18 needs to be expressly given and cannot be implied or inferred.

In the same way as Chief Executive Officers and Senior Executives are responsible for compliance with legislation for financial or workplace health and safety activities, they are also responsible for the management of privacy – whether it is informational privacy or the broader concept of privacy. They are responsible for ensuring the public sector agency does not do anything, or engage in any practice, that contravenes an information protection principle (section 21) or a public register provision or any code of practice applying to the agency (section 32), and for the organisation's compliance with complaint handling provisions.

Traditional patterns of work have changed, with the public sector engaging higher numbers of persons to do work as in-house contractors and not as employees. On the increase is also the contracting-out of services that were once delivered by the public sector. Accordingly, the risks of data systems failures and intentional privacy violations now lie with the private sector. It follows that the private sector's responsibilities must be recognised in our law in a way that allows individuals to have a right to complain about alleged privacy breaches.

Some agencies erroneously believe that they can manage this gap in NSW law solely by entering into contracts with their private sector partners. As discussed following in this report, statutory provision is necessary in order to enable appropriate contracts to be made to bind contractors to obligations under privacy law.

The accountability of some non-government and private sector organisations has been raised in the context of serious concerns about their information governance and IT security, as well as their management of personal and health information of their service users.[24] The most illustrative examples of the issues arise from identifying the respective responsibilities of employers, employees and contractors arise from the principle of 'retention and security of personal information.'

Neither piece of NSW privacy legislation defines the terms employer, employee and contractor. Further, the distinction between where employer privacy responsibilities end and where they become the responsibilities of the employee (or agent) is not clear under the PPIP Act. The NSW Court of Appeal's decision in *MT* captures the arguments for supporting the Department's position that it was not liable for the actions of an employee.[25] (See Annexure 1**:** The Special Rule of Attribution, for more detail.)

Identifying when a corporate entity, for example a company, is engaged to do work for an organisation as a contractor is a relatively simple matter. But it becomes more complex when ascertaining whether a natural person is an employee of an organisation or a contractor. This may require careful analysis of

[23] Guidance regarding consent is also available in: Privacy NSW (2004) "*Best Practice Guide: Privacy and people with decision-making disabilities*," 7; NSW Privacy Commissioner (2016) "*Fact Sheet: Consent*"

[24] Raised by in discussions with Privacy Commissioner by peak bodies, statutory independent office holders and senior public sector executives throughout the period 2012 – 2017 and which has been raised in evidence to Parliament and advice to Government

[25] *Director General, Department of Education and Training v MT* [2006] NSWCA 270

the relationship the organisation has created with the persons it engages to do work for it or to undertake a specific task.

While other areas of law provide guidance, each case must be assessed on its own circumstances. Although the issue of control of how a person discharges their obligations is central, the courts examine the totality of the relationship.[26] As each case will be decided on its own facts, this report does not provide a test as to which situations should be considered an employment relationship and which a contractual relationship.

The PPIP Act regulates the conduct of the public sector regarding the life cycle of "*personal information*." The HRIP Act has the same purpose regarding "*health information,*" however only the HRIP Act applies to both public and private sectors.

The two statutes require compliance with the Information Protection Principles and the Health Privacy Principles respectively, subject to various exemptions.

The issues arising from uncertainty as to the coverage of legislative provisions across employers, employees and agents/contractors arise under both pieces of legislation.

Regarding intentional privacy violations by public sector agency employees or agents, the PPIP Act does not attribute civil liability to the public sector employee or agent/contractor. Section 62 of the PPIP Act however creates a criminal offence of corruptly using and disclosing personal information. The same offence is in section 68 of the HRIP Act regarding health information. The concept of corruption includes an act for personal gain.

What entities are subject to the PPIP Act Internal Review complaints scheme?

As the complaints management scheme in sections 52 to 55 PPIP Act allows only public sector agencies to be subject to an Internal Review (complaint) application, the definition of public sector agency is relevant. Section 3 sets down the range of entities subject to the scheme. It includes entities commonly known as government departments and authorities, public universities and local councils. The definition does not include state owned corporations.

Sections 52 and 53 of the PPIP Act relevantly provide:

52 Application of Part
(1) This Part applies to the following conduct:
(a) the contravention by a public sector agency of an information protection principle that applies to the agency,
(b) the contravention by a public sector agency of a privacy code of practice that applies to the agency,
(c) the disclosure by a public sector agency of personal information kept in a public register.

53 Internal review by public sector agencies
(1) A person (the applicant) who is aggrieved by the conduct of a public sector agency is entitled to a review of that conduct.

Individuals' requests for Internal Reviews may be made directly to public sector agencies regarding their own conduct. They cannot be made directly to a contractor of a public sector agency about the conduct of that contractor. This creates the gap in the privacy rights available under the PPIP Act.

But this gap does not operate evenly under both NSW privacy statutes.

In contrast to the NSW PPIP Act, the HRIP Act provides jurisdiction to the NSW Privacy Commissioner to investigate complaints concerning the private sector in relation to health information. There is direct liability of some types of private sector organisations under the HRIP Act regarding health information, but the processes to enforce rights differ.

The HRIPA Act, a more modern Act than the PPIP Act, being drafted some four years later, has had the benefit of the learning from matters raised under the PPIP Act. And as more recent legislation, the HRIP Act provides protections that are more responsive to community expectations that those who inflict harm are held to account.

[26] *Holis v Vabu Pty Ltd* [2001] HCA 44

Other relevant NSW Statutes

Other statutes that regulate the operations of public sector agencies also contain a variety of offences for the dealing with information for unauthorised purposes. Section 308H of the *NSW Crimes Act 1900* for example, contains the offence of accessing or modifying computerised records for unauthorised purposes. The fact that the employee is otherwise authorised to access the system for official purposes does not affect the offence.

Privacy regulation also derives from the *Data Sharing (Government Sector) Act 2015*, which enables disclosures of information between public sector agencies.

This Act contains provisions requiring agencies sharing information for purposes of data analytics to comply with the provisions in the NSW privacy legislation and with confidence obligations arising from other laws. These obligations are:

- The data provider and recipient must comply with the privacy legislation (section 5);
- Recipients must comply with confidentiality or commercially sensitive requirements regarding information, arising from contracts or equitable obligations (section 13);
- If an agency provides data to the private sector for analytics work, it must have a contract for the private entity to comply with a privacy law, the *State Records Act* and the Government data security policies that apply to it [section 14(2)];
- The privacy and confidentiality obligations extend to private entities that may work on a project; and
- Section 12(2) obliges recipients of data under the Act, to notify the provider agency and the Privacy Commissioner of a data breach.[27]

In the area of human and/or health research, agencies need to identify the appropriate legal permission for disclosures and uses of personal and health information and consider what processes they should adopt to ensure compliance with the privacy legislation. For example, whether they should comply with the processes in the statutory guidelines issued by the Privacy Commissioner under section 27B of the PPIP Act and HPPs 10 and 11 in the HRIP Act.[28]

[27] Section 12 *Privacy safeguards*
(1) Without limiting section 5(2), a data provider and data recipient must ensure that health information or personal information contained in government sector data that is shared is not collected, used, disclosed, protected, kept, retained or disposed of otherwise than in compliance with the privacy legislation.
(2) If a data recipient that is provided with government sector data that contains health information or personal information becomes aware that the privacy legislation has been (or is likely to have been) contravened in relation to that information while in the recipient's control, the data recipient must, as soon as is practicable after becoming aware of it, inform the data provider and the Privacy Commissioner of the contravention or likely contravention.

[28] The current guidelines on research under both statutes are available at www.ipc.nsw.gov.au/privacy

Part 5: Respective responsibilities of employers, employees and agents

A: Responsibilities of employers and employees

The retention and security principle [section 12(c)] creates obligations on public sector organisations holding personal information to have systems in place to protect against data breaches.[29] The prescribed obligation is to prevent improper access, misuse, disclosure, loss or modification of personal information.

For employers this can present particular challenges as to the level of stringency of the obligations as this depends on what is 'reasonable' in the context of each case. This section is the most relevant provision in this discussion regarding privacy wrongdoings committed by employees of agencies.

A review of NSW Tribunal decisions shows that considerations brought to bear by it on the issue of the quality of data security systems varies over time and by matter. Factors considered include whether there were sufficient notices to warn employees of their obligations not to misuse official information[30] and whether training and monitoring of the use of the system by those who had username authority to access the data, was established.[31]

In another matter involving the loss of a document the Tribunal discussed the following as relevant considerations:

- whether the loss led to a subsequent disclosure or misuse;
- the sensitivity of the information;
- the practical difficulties faced by the school; and
- the significance of any shortcomings in the systems to protect information.[32]

Where the agency is aware of a history of systems failures, the Tribunal expects it to take additional measures to alleviate those known data breach risks.[33]

The Tribunal has considered also the responsibility for making privacy or related notices easy to access and sufficiently informative. The Appeal Panel stated:

> *"As already noted, this primary document might contain a summary, or overview statement, that is then fleshed out by one or more linked documents. The objects of the Act are not satisfied, in our opinion, by steps that require the interested individual to undertake a website navigation exercise directed to a host of documents, and tucked-away paragraphs in those documents. We do not consider it satisfactory as a way of demonstrating compliance with such an important obligation to take the reader or the Tribunal on a website tour of bland passages in documents that are not linked in any comprehensible way."*[34]

The Tribunal has also recognised that information of different levels of sensitivity may require different safeguards depending on the nature of information held and the medium in which it is stored. For example, the Tribunal found that highly sensitive information such as psychiatric information must be held on computerised systems that allow the capacity to track accessing of the records, policies governing the handling of health information and employee training.[35]

The Tribunal has recognised that agencies' email systems and servers may offer higher data protection than generic email providers. The Tribunal has considered it a downgrading of an agency's data security measures when employees send emails that contain official information to their personal email addresses. The Tribunal stated:

> "*The Privacy Commissioner strongly criticised the emailing of personal information relating to a member of staff to an external web based email address, not secured by the department. I agree that this illustrates a failure by the agency to take reasonable safeguards of documents which obviously contain personal information. The fact that they were sent to a web based email service, rather than a service from which Ms (X) downloaded her mail, thereby*

[29] Corresponding HPP 5 in the HRIP Act that applies to public agencies and the private sector
[30] *NS v Commissioner, Department of Corrective Services* [2004] NSWADT 263, [59]
[31] *SF v Shoalhaven City Council* [2013] NSWADT 94, [170]
[32] *CLT v Department of Education and Communities* [2016] NSWCATAD 98, [30 – 35]
[33] *XW v Department of Education and Training* [2009] NSWADT 73, [92]
[34] *ALZ v Workcover* NSW [2015] NSWCATAP 138, [83]
[35] *ALZ v Workcover NSW (No 2)* [2014] NSWCATAD 122, [31] & [41 – 42]

> *removing them from the server, is of particular concern*." [36]

The Tribunal has reflected the complexity of determining the respective and separable responsibilities of employers and employees in the following matter involving computerised systems used by public hospitals to hold medical records accessible by employees by personal password for service delivery purposes. The complaint was that an employee used the system and then walked away from the workstation on which the computer was situated without logging out. Another nurse exploited the opportunity to access the complainant's records and later disclosed these records for his own personal reasons. The agency's Internal Review accepted that the agency contravened the data security obligation (HPP 5) in the HRIP Act. The Tribunal expressed however the preliminary view that:

> "*This provision is, in my view, primarily directed at the systems and policies an agency has in place to protect health information. It does not necessarily follow from the loss or disclosure of information by an agency or a staff member, or the failure of a staff member to comply with a policy, that the agency's security safeguards are inadequate* …"[37]

In relation to intentional wrongdoings by employees, the NSW Court of Appeal in the *MT* case decided that when an employee uses or discloses personal information held by a public sector agency for personal purposes, a complaint is not about the actual use or disclosure issue.[38] The agency is not liable for the wrongdoing of its employee under the principles of "agency" or "vicarious liability" that derive from the common law. The focus does not stay on the actual wrongdoing of the agency's employee. Rather, the focus shifts to the question whether or not the agency has adequate data security safeguards. It becomes a systemic question, namely, whether or not the agency's measures were reasonably capable to prevent the privacy wrongdoing. This leaves open the possibility for the Tribunal to find that the fact that an employee intentionally defied relevant policies does not make the agency responsible.

In cases where it is determined that the data security systems and policies themselves were reasonable and the agency is not liable, the complainant is left without a remedy for the actual wrong they suffered, as the legislation does not permit complaints to be made directly against the employees who breach privacy "on a frolic of their own."

There are many examples where this has been the finding of complaint investigations undertaken by agencies.

Recent examples of Tribunal decisions are where University employees used and disclosed the complainants' personal information held by the University to the Federal Fair Work Commission in connection with defending a bullying allegation. The University had advised them that it would not represent them in that court action. The Tribunal did not find the University liable on grounds that the use and any disclosure was:

> "… *for a purpose extraneous to any purpose of the University; that is, for Ms A's own purposes in defending a claim against her. Accordingly, the use or disclosure of the applicant's information should not be characterised as a use or disclosure by the University or as conduct of the University*."[39]

Although there is no decision in the NSW Tribunal regarding the intentional misuse or disclosure of the health information of patients or colleagues by an employee of a private health service provider, the same approach would be expected. Again, if the private health service provider shows it has reasonable policies and systems in place, the complainant will be left without a remedy, as a complaint personally against the employee will fail.

Other laws allow either the common law derived principles of "agency" and "vicarious liability" to apply, or, make specific provision that enables a complainant to have a complaint against employee wrongdoers.

Annexure 1 sets out the ways other laws attribute liability to organisations for the

---

[36] *MH v NSW Maritime* [2011] NSWADT 248, [160]

[37] *BZX, BZY & BZZ v Western Sydney Local Health District* [2015] NSWCATAD 210, [34]. At the time of writing a final decision on this complaint does not appear to have been published. The Tribunal was of the view that it was not bound by the agency's concession and that the Tribunal legislation requires it to consider for itself whether there has been a breach of HPP 5.

[38] *Director General, Department of Education and Training v MT [2006] NSWCA 270.*

[39] *CCM v Western Sydney University* [2016] NSWCATAD 234 [40]. Also *BXK v Western Sydney University* [2016] NSWCATAD 235, [30]

conduct of their employees or agents enabling a comparison with the approach of the Court in the MT case under the PPIP Act.

Immediately relevant to this report is section 53 of the NSW *Anti-Discrimination Act 1977*. It provides a useful model for consideration in ensuring there is no diminution in privacy protection in cases of wrongdoing by employees. It covers both the obligations of employers to have measures in place capable of preventing discrimination and harassment as defined in that Act, and, allows complaints to be made against relevant employees. This avoids the loss of rights that resulted from the approach the Court took in *MT* regarding the privacy legislation.

In order to improve the coverage of privacy rights in NSW, the most appropriate way is to amend the privacy legislation, so that in cases where the agency or private organisation claims its data protection safeguards were adequate, the legislation allows the complainant to join the relevant employee as second respondent.

The difference in the complaint resolution mechanisms between the PPIP Act and HRIP Act is set out in Annexure 2.

Because of these procedural differences between the two privacy Acts, joining employees as second respondents should be allowed as follows:

- If a public agency's Internal Review investigation of a complaint claims that its systems were reasonable and the complainant applies to the Tribunal for review, the PPIP Act allows the complainant to request that the relevant employee be joined as second respondent; and
- If, during an investigation by the Privacy Commissioner under the HRIP Act regarding "health information," a private organisation claims its systems were reasonable, the HRIP Act allows the complainant to request that the relevant employee be joined as a second respondent.

The mechanism of also making relevant employees answerable has proved effective in better securing the rights of victims of discrimination in complaints under the *Anti-Discrimination Act, 1977*. The relevant section of this Act is Section 53. Annexure 3 considers section 53 in more detail and provides some examples of decided cases.

Section 53 of the *Anti-Discrimination Act, 1977* provides:

53 Liability of principals and employers

(1) An act done by a person as the agent or employee of the person's principal or employer which if done by the principal or employer would be a contravention of this Act is taken to have been done by the principal or employer also unless the principal or employer did not, either before or after the doing of the act, authorise the agent or employee, either expressly or by implication, to do the act.

(2) If both the principal or employer and the agent or employee who did the act are subject to any liability arising under this Act in respect of the doing of the act, they are jointly and severally subject to that liability.

(3) Despite subsection (1), a principal or an employer is not liable under that subsection if the principal or employer took all reasonable steps to prevent the agent or employee from contravening the Act.

(4) For the purposes of subsection (1), the principal or employer of a volunteer or unpaid trainee who contravenes Part 2A is the person or body on whose behalf the volunteer or unpaid trainee provides services.

Due to the different processes between the PPIP Act and the HRIPA Act, there is a need to establish different mechanisms for those who have a privacy complaint to access an independent reviewer. These mechanisms, which join employee(s), need to occur at the first opportunity the complaint is independently reviewed.

For those going through the Internal Review process, the first opportunity for an independent determination is when the complaint is considered by the Tribunal.

For complainants under the private sector complaints management scheme in the HRIP Act, the first independent reviewer is the Privacy Commissioner. Therefore, it is important to ensure that the complainants can request the Privacy Commissioner to make the relevant employees a party to the matter – something that is currently not available to them.

This ability (if adopted) would mean that the complainant would see both the employer and the employee as respondents before the Tribunal.

Recommendation 1:

Amend the PPIP Act and the HRIP Act to allow victims of privacy breaches to have a right to complain against both a public sector agency and relevant employees. That is, to request that the Tribunal make employees second respondents in cases where a public sector agency claims that its data security safeguards were adequate and that the agency should not be liable for the alleged conduct of its employees who contravened privacy law.

Recommendation 2:

Amend the HRIPA Act to allow victims of privacy breaches to have a right to complain against both a private sector organisation and relevant employees. That is, to request that the Privacy Commissioner make employees second respondents in cases where a private sector organisation claims that its data security safeguards were adequate and that the organisation should not be liable for the alleged conduct of its employees who contravened privacy law.

B. Responsibilities of agents (contractors)

When a public sector agency engages an agent (contractor) to whom it will give personal information, the agency must ensure that it does everything reasonably within its power to prevent unauthorised use or disclosure of the information [section 12(d) PPIP Act].

As a line of authority from Tribunal decisions does not exist on the question of what are the privacy obligations of the public sector when contracting-out, there is uncertainty as to how public sector agencies must ensure that they comply with section 12(d). The situation becomes more complex again when the contracted agent uses sub-contractors.

Additionally, the obligations under section 12(d) do not require the public sector agency to do everything within its power to prevent contraventions of the privacy principles by the contractor regarding personal information that the contractor will collect or create while performing the contract. Instead the agency is held accountable for doing anything reasonably within power to prevent unauthorised use or disclosure of the information provided.

Earlier guidance from the Office of the NSW Privacy Commissioner (1999) is that the obligations of agencies continue after they contracted work out to others. It stated that *"the idea behind this principle is that a person who has dealings with an agency should not lose their protection under the Act simply because their personal information is held by an organisation acting in a contractual or agency capacity to the public sector agency*."[40]

The Guidance considered that the obligations may include:

- Contractual provisions minimising opportunities for misuse of personal information;
- Conduct audits or monitor the performance of the service provider;
- Control of the disposal of the information or demand the return of all personal information once the service is completed;
- Indemnity clauses to ensure that the agency is able to pass on the costs of any compensation paid out due to the actions of the contractor.

[40] Privacy NSW (1999) *A guide to the information protection principles*, 18

In 2015 the Privacy Commissioner released a statutory report into the operation of the PPIP Act. It raised, amongst other matters, the issue of the outsourcing of services traditionally provided by the government sector to the non-government sector where the workforce can include both employees and volunteers.[41] The issue was the continuity of protection for personal and health information and the privacy of service users and third parties such as family carers.

Questions were raised also with the Privacy Commissioner about the coverage of contracted service providers who do not provide "data services" but who provide services involving personal information.[42]

Contractors, who could be "*organisations*" under the Federal *Privacy Act 1988*, are exempt from regulatory reach.

The recommendations made in the 2015 statutory report included:

1) *The PPIP Act to be amended to clearly cover contracted service providers and contractors who may be involved in services other than 'data services'.*

2) *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.*

   The Privacy Commissioner to assist agencies 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.

Submissions from the public sector agencies to the Privacy Commissioner, in the context of consultation for the 2015 report, raised the benefit of amending the PPIP Act in line with other jurisdictions to ensure contractors do not engage in privacy breaches.[43]

Since the release of this 2015 report an increasing number of questions have been posed regarding the PPIP Act's capacity to extend enforceable privacy rights against entities that perform work for public sector agencies. This increase has accompanied the NSW Government's ongoing transfer of human and social service provision to the welfare sector.

The 2014 survey of non-government organisations (NGOs) undertaken for the 2015 report, indicated the need to strengthen the privacy framework for service users and to address uncertainty as to the nature of the obligations upon NGOs. There was a strong identified need for targeted training and resources outlining their obligations under PPIP Act, the HRIP Act and the Federal *Privacy Act 1998.* The need for privacy training and support by the NSW Privacy Commissioner has been identified also by a recent Parliamentary Inquiry into service co-ordination for communities of high social need.[44]

The uncertainty around the privacy obligations of NGOs is not a new issue. The 2004 statutory review of the PPIP Act undertaken by the then Attorney General's Department recommended that the PPIP Act provide a structure for binding non-government organisations contracted by public sector agencies (Recommendation 13).[45]

The NSW Law Reform Commission also discussed this gap and recommended that privacy protections be expanded where government outsources services under contract.[46]

While the NSW Parliament foresaw the need to create mechanisms for the direct liability of contractors under the PPIP Act, in practice, these have been made available in a limited range of contracted services. Moreover, the inconsistencies between the two pieces of the NSW privacy legislation produce different frameworks applicable to different service users or even the same service client.

While the PPIP Act does not directly regulate contractors to government regarding dealings with "personal information," the HRIP Act regulates some contractors. This is because it regulates some private organisations that deal with "health information," which includes organisations contracting to government. This

41 Report of the Privacy Commissioner under section 61B of the *Privacy and Personal Information Protection Act 1998* (February 2015). Summarised in Attachment 3

42 Ibid, 20

43 Ibid, p.63

44 NSW Parliament, Standing Committee on Social Issues, (2015) *Service co-ordination into communities of high social need.*

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

46 NSW Law Reform Commission (2010) "*Report 127 – Protecting privacy in NSW*," 30 - 36

creates an uneven regulatory coverage for no discernible and valid reason.

The following approaches are available in NSW to maintain privacy protections when non-government service providers provide services on behalf of the NSW Government:

1. Assigning public sector agency status through the PPIP Act;
2. Assigning public sector agency status through agency specific legislation;
3. Assigning public sector status to affiliates;
4. Assuming the responsibilities for contractors;
5. Deeming an agency as the 'service provider' when it has engaged non-employees to provide a service (to an individual).

Annexure 4 discusses in greater detail these industry specific examples.

The Queensland Parliament has taken a more holistic approach to the issue of direct contractor liability. Sections 36 and 37of the *Information Privacy Act 2009 provide*:

36 Bound contracted service provider to comply with privacy principles

(1) A bound contracted service provider under a service arrangement must comply with part 1 or 2 and part 3 in relation to the discharge of its obligations under the arrangement as if it were the entity that is the contracting agency.

(2) The requirement to comply under subsection (1) continues to apply to the bound contracted service provider in relation to personal information it continues to hold after its obligations under the service arrangement otherwise end.

(3) A bound contracted service provider's compliance with part 1 or 2 and part 3 may be enforced under this Act as if it were an agency.

37 Contracting agency to comply with privacy principles if contracted service provider not bound

(1) This section applies if a contracted service provider under a service arrangement is not a bound contracted service provider because the contracting agency under the service arrangement did not take the steps required of it under section 35.

(2) The obligations that would attach to the contracted service provider if it were a bound contracted service provider attach instead to the contracting agency under the arrangement.

This model promotes the adoption of privacy responsibilities by contractors engaged by the Queensland public sector. It enables the Queensland public sector to choose to retain responsibility for the privacy contraventions of its contractors, or alternatively, to make contracts that make contractors directly liable as if they are public agencies. Either way, under this model, contracting-out does not result in reduction of the community's privacy rights.

The model also provides more flexibility than the industry specific approaches that have been made available in NSW. It enables the NSW public sector agencies that engage contractors to assess the strengths and weaknesses of the specific situation and decide which will better reflect the intended design of the partnership and make the appropriate contractual arrangement.

A shortcoming with this model is that it does not provide for the binding of subcontractors.

On the other hand, section 95B of the Federal Privacy Act expressly provides for the binding of sub-contractors. Section 95B provides:

Requirements for Commonwealth contracts

1) This section requires an agency entering into a Commonwealth contract to take contractual measures to ensure that a contracted service provider for the contract does not do an act, or engage in a practice, that would breach an Australian Privacy Principle if done or engaged in by the agency.

2) *The agency must ensure that the Commonwealth contract does not authorise a contracted service provider for the contract to do or engage in such an act or practice.*

3) *The agency must also ensure that the Commonwealth contract contains provisions to ensure that such an act or practice is not authorised by a subcontract.*

4) *For the purposes of subsection (3), a **subcontract** is a contract under which a contracted service provider for the Commonwealth contract is engaged to provide services to:*

   (a) another contracted service provider for the Commonwealth contract; or

   (b) any agency;

   (c) for the purposes (whether direct or indirect) of the Commonwealth contract.

5) *This section applies whether the agency is entering into the Commonwealth contract on behalf of the Commonwealth or in the agency's own right.*

The NSW legislation could be amended to adopt the flexibility of the Queensland model with the extension of the Commonwealth provision, so as to require NSW public sector agencies entering into partnerships with the private sector:

› to ensure they make contractual arrangements capable of binding contractors and any subcontractors; and

› where they do not so, to be responsible for their privacy contraventions in the discharge of their obligations under the service provision arrangements.

The combination of these two models ensures that the community's privacy rights are not diminished solely because of the creation of partnerships with the private sector.

Recommendation 3:

Base amendments of both NSW privacy statutes (PPIP Act and HRIP Act) upon sections 36 and 37 of the Queensland *Information Privacy Act 2009* and section 95B of the Federal *Privacy Act 1988* to enable the public sector to choose to retain responsibility for any privacy contravening conduct of its contractors and subcontractors, or alternatively, to enter into contracts that make contractors and any subcontractors directly liable as if they are public sector agencies.

Part 6: Critical employer responsibilities: organisational culture, ethics governance and strong data security systems

While having comprehensive remedies for privacy violations is imperative, prevention remains our primary goal:

> "*Privacy is an intangible interest that, once lost, cannot be restored through a remedy at trial.*
> *…..*
> *This intangible interest is most effectively protected by preserving privacy, not by allowing its invasion, and subsequently awarding damages."*[47]

Organisations need to be aware that ethics and corruption have a social aspect. The definition of corruption includes the aspect of abuse of power for personal gain[48] and as a creator of inequality.[49]

The same considerations arise when employees of organisations intentionally violate the privacy right of others. A privacy violation may degrade a person's physical and psychological integrity, the right to their identity and obstruct the development of their personality according to their own choices. These are not just adverse impacts on the victim. Just like corruption, they have a social impact, because they degrade the trust necessary for effective social relationships and the trust people need to have in their dealings with public and private organisations to which they give their personal and health information.

Implementing and enforcing safeguards in order to maximise trust need not examine solely the cause or motivation of corrupt conduct. The Deputy NSW Ombudsman states it only needs to look at outcomes.[50] Another critical element is to adopt a 'Privacy by Design' approach which is a proactive and preventive approach to preventing and managing risks to privacy.[51]

The first principle of Privacy-by-Design is that data security systems must be proactive not reactive, and preventative not remedial.[52]

To encourage and embed ethical conduct the governance system must include the following aspects:

- Standard setting;
- Expectation setting;
- Prevention strategies;
- Enforcement mechanisms; and
- Deterrence mechanisms.

The NSW Deputy Ombudsman has observed that organisational approaches tend to focus most effort on the first two and that this may not be sufficient if the system is to address intentionally unethical conduct.[53]

It has been argued that the Australian Federal *Criminal Code Act 1995* embodies the concept of "*corporate culture*" in regulating corporations. It takes a holistic approach to blameworthiness. Culpability may be established when the entity's culture directed, encouraged, tolerated or led to non-compliance. Failures at an organisational level may be established when evidence shows corporate practices failed to create a culture of compliance.[54]

In Canada reactive measures, such as disciplinary action, are also suggested as a disincentive to data breaches following the principle of general deterrence.[55]

The benefits of e-records come with increased risk of unauthorised access and disclosure, which increases the risk to individuals and reputational damage for organisations. In discussing research that showed 85% of data breaches involved electronic rather than paper records, the Ontario Information and Privacy

47 Normann Witzleb, "Interim injunctions for invasions of privacy: Challenging the rule in Bonnard v Perryman," In: Normann Witzleb, David Lindsay, Moira Paterson & Sharon Rodrick (eds) *Emerging challenges in privacy law: Comparative perspectives*, 2014, Cambridge University Press, UK, 416

48 Susan Rose-Ackerman & Bonnie J Palifka, *Corruption and Government* (2nd Ed), 2016, Cambridge University Press, New York, 9

49 Yasmin Dawood "Classifying corruption" (2014) 9(1) *Duke Journal of Constitutional Law & Public Policy* 103, 123 – 127

50 "Ethics in the public sector – Clearly important, But …" (2014) 77 *AIAL Forum* 19, 22 - 23

51 Ann Cavoukian (2009) "Privacy by Design: The 7 foundational principles," at: www.iab.org/wp-content/IAB-uploads/2011/fred_carter.pdf

52 Ann Cavoukian (2009) "Privacy by Design: The 7 foundational principles," at: www.iab.org/wp-content/IAB-uploads/2011/fred_carter.pdf

53 C. Wheeler "Ethics in the public sector – Clearly important, But …" (2014) 77 *AIAL Forum* 19, 22 - 23

54 Anthony Nwafor "Corporate criminal responsibility: a comparative analysis (2013) *Journal of African Law* 81, 97; Celia Wells "Criminal responsibility of legal persons in common law jurisdictions," Paper prepared for the OECD Anti-Corruption Unit, 4/10/2000, at: www.coe.int-t-dght.monitoring.greco.evaluations.seminar.Wells_revised.pdf

55 Omar Ha-Redeye "*Class action intrusions: A development in privacy rights or an indeterminate liability?" (2015) 6(1) Western Journal of Legal Studies* 1, 11

Commissioner noted the term "*insider and privilege misuse*." The report concluded:

> *"A strong message should be sent that unauthorized access to personal health information by custodians and their agents is not acceptable and will not be tolerated and those who do so may face serious consequences."*[56]

There is general agreement that a holistic anti-corruption framework must include an element of deterrence achieved through reactive measures, such as administrative and criminal sanctions.[57] Prevention however remains the preferred approach as slated elsewhere in this report.

Systemic organisational failure can lead to extreme violations of privacy by employees over a sustained period. Such a case concerns a Canadian appeal case of the dismissal of a nurse from her hospital employment. It came to the hospital's attention that 15 employees had improperly accessed the e-record of a patient who was also a hospital employee. Audits that the hospital conducted showed that one nurse had been accessing patients' e-records for seven years.

The nurse had made 12,000 enquiries into the records of 5,804 patients. After the patients became aware of the matter, many were critical of the hospital not discovering the breaches earlier and they said "*that their trust was broken and that they felt violated*."

The nurse said that "*She was fascinated that she could access this information, and she began doing so – first with patients in ER and then other patient information*." The Arbitrator who heard the dismissal case described the extent of accesses as "*truly breathtaking – almost mind boggling*" and was troubled by the fact the nurse "*continued to do this for so long – seven years – without being questioned or detected*" causing harm to patients, the hospital and herself.[58]

Another high profile example is the hacking of the website of the Ashley Madison global dating service. This was jointly investigated by the Canadian and Australian Privacy Commissioners.[59] It was concluded that an organisation's data security framework requires:

- Documented privacy and security practices as part of their compliance program;
- Consideration of the personal information collected must be considered when determining and developing an organisation's information and security program;
- regular and documented audits and risk assessments;
- Documentation of privacy and security practices to assist organisations identify gaps;
- Training of all employees, including senior management is part of a functional and robust compliance program.[60]

A question arises as to whether a data security framework may be limited to proactive measures or if it should include reactive measures that the employer takes after it becomes aware of the wrongdoing of an employee.

In late 2015 the question arose in the NSW Tribunal whether the respondent agency's obligations extended to taking disciplinary action against a nurse, who had used and disclosed the complainant's health information for private purposes. At the time of writing this question does not appear to have been decided.[61]

The Victorian Tribunal considered a case of an accidental disclosure of personal information by an employee. It took into account evidence that the agency's division as a whole responded to minimise the same risk, the employee had received counselling and training as a result of the incident, the agency attempted to engage the complainant after the incident, and, circulated a document advising

[56] *Information and Privacy Commissioner of Ontario* (January 2015*) "Detecting and deterring unauthorized access to personal health information,"* at 26. The report includes a useful nine points plan of both proactive and reactive measures for a data security framework

[57] Transparency International "Examples of national anti-corruption strategies (23/8/2013) at: www.transparency.org/files/content/corruptionqas/Good_practices_in_anti-corruption_strategy.pdf; Adam Graycar & Russell Smith "Identifying and responding to corporate fraud in the 21st century" and "Identifying and responding to electronic fraud risks" (2002) Australian Institute of Criminology, who suggest that: "*At every available opportunity, a culture of compliance needs to be enforced.*"

[58] *North Bay Health Centre v Ontario Nurses Association* [2012] CanLii 97626 (ONLA), 24

[59] Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and Acting Australian Information Commissioner (23/8/2016)

[60] Karl Schober "*The Ashley Madison breach: Canada – Australia report of investigation and takeaways for all organisations*" at: http://www.privacyandcybersecuritylaw.com (28/8/2016)

[61] *BZX & BZY & BZZ v Western Sydney Local Health District* [2015] NSWCATAD 210, [35]

staff of means to print sensitive documents confidentially. The Tribunal held that the public sector agency had reasonable safeguards in place.[62]

These examples using the issue of reasonable data security safeguards, demonstrate regardless of differing decisions, the obligations upon organisations (employers) to have safeguards in place.

The elements of a comprehensive data security governance framework are set out at Annexure 5.

Section 53 of the *Anti-Discrimination Act* provides a good approach to the general question of what measures an organisation should have in place although the provision is addressing the prevention of discrimination. These obligations do not stop at proactive measures, such as policies and procedures. They include the organisation's responses after an incident is brought to the organisation's attention. This legislative provision provides a useful model for consideration in ensuring there is no diminution in privacy protection through provision of government services by other bodies.

The issue of ensuring due responsibility by contracted service providers has been recognised by the (then) Department of Attorney General and the Department of Premier and Cabinet, amongst others.[63]

Recommendation 4:

Amend section 12 of the PPIP Act and HPP5 in Schedule 1 of the HRIP Act to require public sector agencies and private organisations, as may be applicable, to have in place both proactive and reactive measures to prevent data breaches in line with section 53 of the NSW *Anti-Discrimination Act 1977.*

[62] *TSJ v Department of Health & Human Services* [2016] VCAT 687, [25 – 34]

[63] Submissions to the Privacy Commissioner's 2015 Statutory Report referenced above, see p20 of this report for example

Part 7: Conclusion

To participate effectively in a world of accelerated data flows, individuals need to have trust in those to whom they give their personal, and often sensitive, information.

For Governments, such as the NSW Government, wishing to participate in the global information economy, the confidence of citizens that their privacy and information will be protected, is essential if accurate and complete information is to be provided. Protecting privacy, and being seen to do so, enables the establishment of a relationship based on trust.

Privacy loss is a harm that not only damages individuals, but also damages the trust individuals have in institutions. Trust is essential for effective dealings between individuals, businesses, and government.

Where risks result in harm the NSW privacy legislation provides a right to seek redress, but it does so inadequately in certain regards. This report argues that the legislation's coverage is not as effective as other laws but that with some amendment it could become as effective.

Other laws focus more on the actual wrongdoers, and it is immaterial if they are employees or contractors, as their actions are covered regardless. This way they set everyone on an equal footing of responsibility when dealing with other people's personal information. Sharing this responsibility requires organisations, both public and private, to take privacy seriously at the outset as a 'Privacy by Design' approach at the highest levels of management and implement training and data governance systems that work.

Where this fails, the law must ensure that privacy rights are not lost. This report argues that there is loss of privacy rights in cases when employees put personal interests ahead of their official responsibilities. Furthermore there is also a loss of privacy rights where contractors are engaged to do work that was traditionally done by government and appropriate frameworks for privacy protection are not in place.

The recommendations to improve the coverage of the NSW privacy legislation are not new. What is suggested is already part of the ordinary workings of other similar laws.

It is unclear why privacy laws have not been treated equally and their coverage aligned with these other similar laws. This lack of alignment and absence of coverage is particularly concerning in light of the advances in technology that have increased both the frequency and extent of privacy breaches.

For individuals to participate fully in our networked digital society they must feel that their personal information is respected by being protected. Privacy protection involving both proactive measures and a more comprehensive approach to a victim's ability to seek redress for their privacy right when things go wrong is not only an individual concern. It is also a social concern because it underpins the necessary trust needed for "*willingness to connect with others in ways that produce social value*."[64]

To be able to secure protection for privacy and redress for privacy wrongs, there must be clarity of responsibility for any harm, both in terms of who is responsible (whether they be employers, employees and/or contractors) and the harms for which they are responsible.

The other laws this report discusses achieve a better balance of responsibilities.

The additional protections proposed in this report will help bring our privacy law into alignment with these similar laws, and establish mechanisms that deliver real benefits to those individuals within NSW who experience incursions into their informational privacy rights.

[64] Neil Richards & Woodrow Hartzog (15/1/2017) "*Privacy's trust gap*," 20 – 21, Yale Law Journal, Forthcoming. Available at SSRN: https://ssrn.com/abstract=2899760

Annexures

Annexure 1: How principals may become liable for the conduct of employees or agents

The NSW Supreme Court excluded the application of the common law derived principles of "agency" and "vicarious liability" from the operation of the PPIP Act when the complaint is about an intentional wrongdoing of a public agency employee. The outcome of this interpretation is that assessment of liability does not focus on the actual privacy contravening conduct. Rather, the focus shifts to the agency's data protection systems.

In order to situate the Court's approach under the PPIP Act in comparison to the approach of other laws, it is necessary to examine the ways by which other laws hold principals liable for a harm causing act or negligence by their employees or agents.

In this examination principals can be public agencies, private organisations, or anyone engaging an employee or contractor who causes some harm and is then sued for that harm.

The Full Court of the Australian Federal Court has summarised the two ways by which a principal can become liable for the acts of another:

› First, attributing the breach of duty (or liability) of the other person to the principal. This is vicarious (indirect) liability; and

› Secondly, attributing the conduct of the other person to the principal. This follows the rules of agency and is direct liability of the principal.[65]

A principal becomes liable for a law infringing conduct of employees or agents under different mechanisms. Discussion in texts and judgments tends to move across these rather seamlessly, occasionally creating some terminological uncertainty for the reader. In the following comments an attempt is made to more clearly separate the concepts.

Direct Liability: Non-delegable duty

Claimants may allege that the principal against whom they claim a breach of some duty could not delegate that duty to another person. Therefore, the claimant argues that the principal is liable for the acts of those the principal engaged to do something for the principal's business.

This rests on the proposition that the principal must accept the risk of a contractor, for example, causing damage in the course of performing the contract. Usually such claims are made in cases where an extra hazardous situation exists and/or where the victim has some special vulnerability to physical risks. An element in the relationship is required that "*generates a special responsibility or duty to see that care is taken*."[66]

Such claims are primarily made where negligence claims appear likely to fail, as the common law of tort does not generally assign vicarious liability in tort to a principal for the acts of a contractor.[67]

The argument in such claims is not that the principal must take reasonable steps to prevent the wrong or the resulting injury, but rather the stricter test to ensure that reasonable care is taken by whoever is carrying out the activity that causes the injury.

Such claims are said not to extend to intentional and criminal wrongdoings of employees or agents.[68]

This type of claim is unlikely to be made under the PPIP Act.

65 *Pioneer Mortgage Services Pty Ltd v Columbus Capital Pty Ltd* [2016] FCAFC 78, [48], [51] & [56]

66 *Kondis v State Transport Authority* (1984) 154 CLR 672, 687

67 Jonathan Morgan "Liability for independent contractors in contract and tort: Duties to ensure that care is taken" (2015) 74(1) *Cambridge Law Journal* 109, 118 – 119 & 128. Jonathan Burnett (2007) "Avoiding difficult questions: Vicarious liability and independent contractors in *Sweeney v Boylan Nominees*," (2007) 29 *Sydney Law Review* 163 discusses the two exceptions to the general rule.

68 *Mohareb v Kelso; Mohareb v Booth* [2016] NSWDC 208, [50], referring to *NSW v Lepore* (2003) 212 CLR 511

Direct Liability: Primary rule of attribution of responsibility to the principal

A company's governors manage its affairs and are readily identifiable in the constitutional documents of the company. They are the Board of Directors or a vote of the shareholders. In the case of public sector agencies the official conduct is represented as decisions of a Chief Executive. For example setting policy for particular activities. Those decisions are the agency's decisions. If such acts or decisions are contrary to law, the entity has direct liability.

Examples of such direct liability in the area of NSW privacy regulation can be:

- When an agency decides to publish personal information on its website in a formal publication and that decision proves to be a contravention of the agency's obligations in section;[18]
- When an agency's database systems produce a data breach because of poor design (data leaks);
- When a medical practice refuses to give a patient access to the patient's health information because of a policy that it will only produce records in response to a subpoena; and
- When a hospital refuses to give a patient access to the patient's psychiatric reports because of a practice of considering that every release of psychiatric reports poses a risk to patients, as opposed to considering each release on its own merits.

Direct Liability: General rule of attribution: Agency

Neither companies nor public sector agencies can function effectively if each activity requires authorisation from the highest organs of governance. Other employees also make decisions and have authority to engage in various activities in the course of their employment. For this reason the common law developed rules to attribute law infringing conduct of employees to the principal.

Rules of agency attribute direct liability to the entity for acts of employees or agents with specific functions and specific authorities. These rules are particularly useful to identify if an entity has bound itself in contracts or promises that various employees make. They are also useful in ascertaining whether the conduct of employees contrary to regulatory or criminal law should render the entity liable.

In the initial stages of the development of the rules of agency the courts looked for the person whose conduct could render the entity liable by being the "*directing mind and will*" of the entity.

As entities became more complex and authorities and responsibilities became more diverse and specialised, the courts moved away from that concept. The courts appreciated that there can be more than one person in an entity with decision making responsibilities. Attribution of responsibility to the entity became answering the question whether the person whose conduct was under review has sufficient authority in the specific transaction, as opposed to general superior authority.[69]

This became known as the "*authorised employee*" approach or "*organic theory*" of attribution.[70] It reflects the fact that entities became multi-centred and functional as opposed to the courts examining the structural power arrangements.

The Courts look for the following factors to ascertain if a person is the entity's agent:

- The agent generally acts with the consent of the principal;
- Their relationship is characterised by a degree of control or direction from the principal;
- Control by itself is not enough. There must be some form of the agent representing the principal; and
- Generally, their relationship came about from an agreement.

How the parties describe their relationship is not determinative. The true nature of their agreement must be found.

The fact that the principal may not have authorised the particular conduct that is law infringing does not necessarily excuse the principal from liability.[71]

---

[69] *Tesco Supermarkets Ltd v Nattrass* [1972] AC 153; Discussion of this shift also in *Australian Competition and Consumer Commission v Prysmian Cavi E Sistemi (No 12)* [2016] FCA 822, [224 – 226]

[70] *Meridian Global Funds Management Asia Ltd v Securities Commission* [1995] 2 AC 500

[71] *Mouawad v The Hills Shire Council* [2013] NSWLEC 165, [97]

An example is a matter where a manager of a campsite refused to rent the camp to a youth group on discriminatory grounds and was found to be acting under the owner's authority. The Victorian Court of Appeal said that the organic theory extends the range of people who can bind the principal. This is direct liability and does not have a defence of taking reasonable precautions.[72]

As the above example indicates, agency rules are better suited to transactional disputes as opposed to conduct issues.[73]

Examples in a privacy context may be the following processes implemented by managers of local units without reference to senior management for the specific decision:

- When a branch of a health service provider communicates with clients of that branch by broadcast emails without blind copying the client addresses. A broadcast may reveal both the personal information in the email address and the health information of each recipient, being that each is receiving a health service from that branch.
- When an organisation's branch uses a web-based platform to invite survey answers from clients that are said to be anonymous, but without informing that the settings of the survey are such that the survey will also collect personal information from recipients of the invitation. Such information may be outside the answers participants will provide, or, that the survey will know which one of the recipients responded and who did not.
- An organisation does not have a formal policy describing the volume of personal information it will collect when a client attends to obtain a service. Local branches may decide to collect different amounts of personal information depending on their own understanding of what is reasonably necessary for the service. If a local decision over-burdens the collection of personal information for the transaction, the organisation will be responsible for that decision.

In a matter determined by the NSW Tribunal, an Acting General Counsel of a NSW public agency had made a decision to disclose the complainant's personal information to the NSW Supreme Court. This was found to be contrary to the protections in section 18 PPIP Act. In finding the agency liable for the employee's conduct the NSW Tribunal considered this senior officer's wide delegations and authorities. It found that, although the agency had not given permission to make the particular disclosure, the agency was bound by it, as the conduct was within the ambit of that officer's scope of authority.[74]

Indirect Liability: General rule of attribution. Vicarious liability

The UK Supreme Court defined vicarious liability as follows:

> "*Vicarious liability does not involve any attribution of wrongdoing to the principal. It is merely a rule of law under which the principal may be held strictly liable for the wrongdoing of someone else.*"[75]

It is established when the employee breaches a duty that the employee owes himself or herself and the employer is additionally liable.[76]

Vicarious liability has been explained on different grounds, with none having special primacy over the other:

1. The employer is more likely to be able to compensate the victim than the employee (the deep pockets reason);
2. The wrong was committed as a result of the employee doing something for the employer (the delegation of task reason);
3. The employee's act is likely to be part of the business activity (the enterprise liability reason);
4. By employing the employee, the employer created the risk of the wrongdoing (the risk creation reason); and
5. The employee would have been under the control of the employer (the control reason).[77]

The Australian High Court stated:

---

72 *Christian Youth Camps Ltd & Ors v Cobaw Community Health Services Ltd & Ors* [2014] VSCA 75, [122]

73 Charles Zhen Gu "How statutory civil liability is attributed to a company: An Australian perspective focusing on civil liability for insider trading by companies" (2006) 32(1) *Monash University Law Review* 177, 181

74 *MH V NSW Maritime* [2011] NSWADT 248, [153]

75 *Jetivia SA & Anor v Bilta (UK) Ltd (in liq) & Ors* [2015] UKSC 23, [70]; *Prince Alfred College Inc v ADC* [2016] HCA 37, [39] (Australian High Court)

76 *Jetivia*, [186]

77 *The Catholic Child Welfare Society v Various Claimants & the Institute of the Brothers of Christian Schools* [2012] UKSC 56, [35], Lord Phillips

> *"Common law courts have struggled to identify a coherent basis for identifying the circumstances in which an employer should be held vicariously liable for negligent acts of an employee, let alone for intentional, criminal acts."*[78]

Under the principles of vicarious liability the law looks at everyone who interacts with others, be it on the roads or at the workplace. For this reason it is more compatible with modern service delivery models.[79]

The touchstone to vicarious liability is that the employee's act should be committed within the course or scope of employment.

This issue has three elements:

1. The act was authorised by the employer; or
2. Is an unauthorised mode of doing something authorised; or
3. It may be unauthorised, but it is so connected with authorised acts that it may be regarded as a mode of doing the act, although improper mode of doing it.[80]

The UK Supreme Court has held that there is no need to speak of the relationship being strictly one of employment. Something akin to employment will suffice. For example, when a prison employee was supervising a prisoner who was undertaking work that he was mandated to undertake by prison rules. The prisoner accidentally dropped a sack and injured the prison employee. The UK Supreme Court found there was sufficient likeness to an employment relationship and that the prisoner was sufficiently connected to the prison service.[81]

The UK Supreme Court has applied a wide test of the requirement that the wrongful act be within the scope of employment, described as the "*close connection test*."[82]

This expanded possibility to find the employer liable for unauthorised acts of employees is often described as the enterprise risk theory. Justice McLachlin of the Canadian Supreme Court (and later Chief Justice) explained it as follows:

> "*The employer puts in the community an enterprise which carries with it certain risks. When those risks materialize and cause injury to a member of the public despite the employer's reasonable efforts, it is fair that the person or organisation that creates the enterprise and hence the risk should bear the loss."*[83]

Commentary has described this approach as liberal.[84] It emphasises the control the employer has over the risk itself and not the control over the employee. It recognises that when an enterprise introduces a risk creating business activity and employs individuals to carry on its business, it should bear the external risks that arise from the activity. [85] The explanation is that this approach to liability is to regulate or control employers' risk-taking activities, in particular, their manner of hiring, training, supervising and otherwise dealing with employees.[86]

Justice McLachlin's factors for finding the employer liable were:

1. The opportunity that the enterprise afforded the employee to abuse his or her power;
2. The extent to which the wrongful act may have advanced the employer's aims;
3. The extent to which the act was related to inherent risks of friction, confrontation or intimacy;
4. The extent of power conferred on the employee in relation to the victim; and
5. The vulnerability of potential victims to wrongful exercise of the employee's power.[87]

Although the Australian High Court appears to apply stricter factors, depending on the case,

78 *Prince Alfred College*, [39], [44]

79 Jonathan Morgan "Liability for independent contractors in contract and tort: Duties to ensure that care is taken" (2015) 74(1) *Cambridge Law Journal* 109, 114

80 *Prince Alfred College*, [42]; Referring to the textbook of John Salmond *The Law of Torts* (1st Ed) Stevens & Haynes, London, 1907, at 83 - 84; Also discussed in David Nield "Vicarious liability and the employment rationale" (2013) 44 *Victoria University Wellington Law Review* 707, 716

81 *Cox v Ministry of Justice* [2016] UKSC 10, [35]

82 *Mohamud v WM Morrison Supermarkets plc* [2016] UKSC 11, [36]

83 *Bazley v Curry* [1999] 2 SCR 534, 548

84 James Plunkett " Taking stock of vicarious liability" (2016) 132 *Law Quarterly Review* 556, 561. The Singapore Supreme Court has adopted the same position: *Skandinaviska Enskilda Banken AB (Publ), Singapore Branch v Asia Pacific Breweries (Singapore) Pte Ltd & Anor* [2011] SGCA 22

85 David Tan "Internalising externalities" (2015) 27 *Singapore Academy of Law Journal* 822, 841

86 Attila Ataner "How strict is vicarious liability? Reassessing the enterprise risk theory" (2006) 64(2) *University of Toronto Faculty of Law Review* 63, 81. But this liberal approach may not be adopted by the Australian High Court, which prefers to assess the issue on a case by case basis, noting that the enterprise risk theory has not attracted significant support: *Prince Alfred College*, [74]

87 *Bazley*, 560

the factors pointing towards liability are authority, power, trust, control, intimacy. Mere opportunity to commit the wrongdoing is not enough. But, if "*the employee takes advantage of his or her position with respect to the victim, that may suffice to determine that the wrongful act should be regarded as committed in the course or scope of employment and as such render the employer vicariously liable*."[88]

One may readily find sufficient factors in this scheme to argue that a hospital should absorb liability when, for example, a nurse:

› who is otherwise authorised to access patient computer records unsupervised for the health care of patients;

› uses this special power to access patient records for personal purposes;

› in circumstances where the patients are vulnerable because they trusted their data to the hospital and they have no control of who accesses it.

Examples of international privacy cases that took this approach are:

An employee of the UK Department of Defence sold to the press information regarding disciplinary action against a senior naval officer. It did not matter that it was done without permission and knowledge of the Department. Justice Nicol said:

> "*There is always an inherent risk that those entrusted with such information will abuse the trust reposed in them, but rather than this being a reason why vicarious liability should not be imposed, I think, on the contrary, it is a reason in its favour."*[89]

The Indiana Court of Appeals confirmed the lower court's award of damages in favour of the complainant for the improper disclosure of health information by the employee of a pharmacy. The judgment started as follows:

> *"In this case, a pharmacist breached one of her most sacred duties by viewing the prescription records of a customer and divulging the information she learned from those records to the client's ex-boyfriend."*[90]

A bank employee accessed customer records and provided the information to his girlfriend, who then disseminated them to others who committed identity fraud on the customers. The Ontario Supreme Court applied the five factors from Justice McLachlin's judgment in *Bazley* and certified the claim to proceed under the Court's procedural rules.[91]

The same court made a similar procedural decision regarding employees who accessed the e-records of 280 patients.[92]

A special rule of attribution arising from the statute under consideration

Under the applicable New Zealand corporations law that required companies to declare shareholdings they had obtained, a middle manager with authority to buy shares failed to make the relevant declarations after he purchased shares without the knowledge of the company's Board of Directors. The New Zealand Court found that the statutory scheme did not impose vicarious liability on the company for the failure of the manager. On appeal to the Privy Council Lord Hoffmann devised the scheme of attribution discussed in this report. In relation to the need for a separate rule in some circumstances, he said:

> "*The company's primary rules of attribution together with the general principles of agency, vicarious liability and so forth are usually sufficient to enable one to determine its rights and obligations. In exceptional cases, however, they will not provide an answer. This will be the case when a rule of law, either expressly or by implication, excludes attribution on the basis of the general principles of agency or vicarious liability*." [93]

Lord Hoffmann then said that in those cases the Court must fashion a special rule that is a matter of statutory interpretation that depends on the facts of the case and the relevant statutory law. Lord Hoffmann is thought to

88 *Prince Alfred College*, [81 – 82]

89 *Axon v Ministry of Defence & NGN Ltd* [2016] EWHC 787, [35]. The complainant was not granted a remedy on grounds that he did not have an expectation of privacy on the facts of the case because of his high seniority in Defence.

90 Walgreen Co v Abigail Hinchy, No 49A02-131-CT-950, 14/11/2014

91 *Evans & Evans v Bank of Nova Scotia & Wilson* (2014) ONSC 2135

92 *Hesse & Ors v Petersborough Regional Health Centre & Ors* (2015) ONCA 112

93 *Meridian Global Foods Management Asia Ltd v Securities Commission* [1995] 2 AC 500, 507

have expanded, as opposed to have restricted, the liability bases for wrongs of employees.[94]

The special rule of attribution arising from the PPIP Act: The *MT* case

A NSW teacher, who was at the same time a soccer team coach, accessed information that the government school held about a health condition affecting a student and disclosed it to the soccer club for purposes unrelated to the school's functions. The reason to disclose it to the club was to decide whether or not the student should be allowed to participate in a soccer game. The student requested an Internal Review of the privacy complaint by the agency under Part 5 of the PPIP Act.

The Department argued that it was not liable under section 17 for any use of the information and under section 18 for the disclosure, because the teacher's disclosure to the club was not for the Department's official functions.

The NSW Court of Appeal's decision in *MT* appears to have relied on the following points:[95]

- The PPIP Act enforces rules regarding the conduct of agencies acting for their public purposes;
- It has no specific provision as to when the conduct of employees or agents will be attributed to the agency;
- Without words in the statute that specifically attribute liability to the agency for the conduct of employees or agents, whether the agency will be found liable, must be determined by interpreting the statute, giving weight to its scope and purpose;
- If obligations in the relevant IPPs are to bind the agency, the personal information must have come into the possession or control of the agency's employee in the course of employment for the agency, not for personal reasons, such as in this case. That is, the agency must be found to "hold" the relevant information before the employee used or disclosed it contrary to the IPPs;
- When use or disclosure is for purposes extraneous to the purposes of the agency, it should not be characterised as use or disclosure by the agency;
- The PPIP Act makes separate provision to regulate employee conduct. This is the criminal offence in section 61(2) of using and/or disclosing information obtained in the course of official functions for corrupt purposes;
- The more relevant IPP in such cases is section 12(c). This is because to hold that the agency has strict vicarious liability would be inconsistent with the obligation in section 12(c) to have only reasonable safeguards in place.

As discussed above the reasoning turns the focus on the agency's obligations, as opposed to focusing on the acts of the agency employee.

Outcomes of the current state of the NSW privacy legislation are that:

1. A remedy cannot be obtained from an employee of a public sector agency under the PPIP Act for unauthorised use or disclosure of personal information obtained in their employment with the agency;
2. By analogy to the provisions in the HRIP Act, a remedy cannot be obtained from employees of a private sector health service provider;
3. The complainant will not be able to join employees as second respondents to a complaint first lodged against the employer organisation.

[94] Eilis Ferran "Corporate attribution and the directing mind and will" (2011) 127 *Law Quarterly Review* 239, 245

[95] *Director General, Department of Education and Training v MT* [2006] NSWCA 270

A different interpretive approach in the House of Lords

The UK *Protection from Harassment Act 1997* creates an anti-harassment framework with statutory obligations. A clinical auditor co-ordinator complained that the section manager was a bully. Lord Nicholls approached the liability of the employer under the statute differently to the NSW approach in *MT*:

> [16] *… The question can be framed this way. Does employers' vicarious liability arise unless the statutory provision expressly or impliedly excludes such liability? Or does employers' liability arise only if the statutory provision expressly or impliedly envisages such liability may arise? As I already indicated, I prefer the first alternative. It is more consistent with the general rule that employers are liable for wrongs committed by employees in the course of their employment. The general rule should apply in respect of wrongs that have a statutory source unless the statute displaces the ordinary rule. …*
>
> [18] *I turn to the material provisions of the 1997 Act. The purpose of this statute is to protect victims of harassment, whatever form the harassment takes, wherever it occurs and whatever its motivation. …*
>
> [26] *Nor does imposition of criminal liability only on the perpetrator of the wrong, and on a person who aids, abets, counsels or procures the harassing conduct, point to a different conclusion. …*
>
> [30] *… To exclude liability on these grounds would be, to use the hackneyed phrase, to throw the baby out with the bath water. It would mean that where serious harassment by an employee in the course of his employment has occurred, the victim – who may not be a fellow employee – would not have the right normally provided by law to persons who suffer a wrong in that circumstance, namely, the right to have recourse to the wrongdoer's employer*."[96]

Liability attribution in Australian Anti-Discrimination laws

In recent years, Federal anti-discrimination laws include specific provisions attributing liability to an employer for acts or employees and agents, titled "*vicarious liability*."

But even before such provisions were included in the Federal statutes, the interpretive approach was to apply the usual common law rules of agency and vicarious liability. This approach was adopted by the Human Rights and Equal Opportunity Commission (as the Australian Human Rights Commission was then titled)[97] and Federal Magistrates.[98]

In a case involving sexual harassment and racial discrimination by a middle ranking prison manager against a prison officer the NSW Tribunal considered that liability of the government agency arose not only from section 53 of the *Anti-Discrimination Act* but also from the common law.[99]

Australian Federal anti-discrimination law has not limited itself to the narrow concept of "*course of employment"* when considering liability of the employer for discriminatory conduct of employees. A test arising from the concept "*in some way related to or associated with the employment"*[100] prevails, providing wider protections to victims of discrimination on the grounds that human rights laws are given a generous interpretation. Examples are conduct that has no connection with the discharge of duties, but nevertheless takes place in employment related activities or merely at the workplace.

---

96 *Majrowski v Guy's & St Thomas' NHS Trust* [2006] UKHL 34

97 For example: *Kordos v Plumrose (Aust)* (1989) EOC 92-256. Discussed in Australian Human Rights Commission (2016) *Federal Discrimination law*, 166. Available at: https://www.humanrights.gov.au/our-work/legal/publications/federal-discrimination-law-2016

98 For example: *Taylor v Morrison & Ors* [2003] FMCA 79, [23]. *Lee v Smith & Ors* [2007] FMCA 59, [213

99 *Borg v Commissioner, Department of Corrective Services & Anor* [2002] NSWADT 42, 101, 154

100 *Lee v Smith* [2007] FMCA 59, [213]

Liability attribution in other privacy statutes

If one accepts the reasoning in *MT* that the rules of agency and vicarious liability deriving from the common law are not present, describing liability as vicarious in statutory schemes that specifically provide for it and provide various defences is incorrect. For this reason the better way is to describe the employer's liability as "*attributed,*"[101] with specific defences as provided in each statute.

Section 68(1) of the *Information Privacy Act 2000* (Victoria) provides:

> *"Any act done or practice engaged in by or on behalf of an organisation by an employee or agent of the organisation acting within the scope of his or her actual or apparent authority is to be taken…to have been done or engaged in by the organisation and not by the employee or agent unless the organisation establishes that it took reasonable precautions and exercised due diligence to avoid the act being done or the practice being engaged by its employee or agent."*

Section 8 of the Australian Federal *Privacy Act 1988* is to similar effect, because it treats acts or practices of employees in the performance of duties as acts of the organisation.

It also provides a reasonable precautions defence in section 99A(2) regarding the conduct of employees or agents acting within the scope of their actual or ostensible authority.

Examples from the determinations of the Federal Privacy Commissioner are:

› Comcare, an Australian Federal agency responsible for managing workers compensation claims, decided to trial new electronic communications with other departments and private insurance companies to manage claims. These communications disclosed a person's health information when the person's file was already closed and it could not be part of the trial. The Australian Privacy Commissioner held that organisations are obliged to test the processes they use to aggregate data they intend to disclose externally in bulk.[102]

› A telecommunications retailer held identification information, such as copies of driver licences. After deciding to dispose a volume of information it held, it stored in a locked container on an open piece of land that was unfenced, awaiting contractors to destroy the documents. Trespassers broke the lock and discarded the documents in bushland. A television channel informed the complainant that it found the documents. The Australian Privacy Commissioner found against the company on the basis that its data security system was inadequate for not storing the container on fenced land, where the public would not have ready access.

The South African *Protection of Personal Information Act 2013* makes responsible parties liable for acts of employees. Whilst it contains provisions obliging employers as responsible parties to take safeguards to protect personal information, the defences to a claim are limited and listed in section 99(2). The relevant defence applies when section 99(2) (d) comes into play: *Compliance was not reasonably practicable in the circumstances of the particular case*.

It has been argued that the South African defence is narrower than the general defence of reasonable safeguards being assessed as a systems issue, which is the NSW approach. Also, that evidence of a system of reasonable safeguards may only be taken into account "*as mitigating circumstances when determining a just and equitable amount as damages*."[103] A decision testing this argument does not appear available.

Section 13(3) of the UK *Data Protection Act 1998* provides a defence where the employer had taken such care as in all the circumstances was reasonably required to comply with the Act.

[101] See discussion in *Christian Youth Camps Limited & Ors v Cobaw Community Health Services Limited & Ors [2014] VSCA 75*, [385 – 391], where it was said that the term vicarious liability is loosely used, even in headings in statutes that actually impose liability on employers on the basis of the general agency rule and allow for defences of taking reasonable measures. Referring to Neil Rees, Katherine Lindsay & Simon Rice, *Australian Anti-Discrimination Law*, 2008, Federation Press, Sydney, 514

[102] *JO v Comcare* [2016] AICmr 64, [43 – 45]

[103] D Millard & E G Basceranco "Employers' statutory vicarious liability in terms of the Protection of Personal Information Act" (2016) 19 *Potchefstroom Electronic Law Journal* 1, 11 – 12

Similarly, the New Zealand *Privacy Act 1993* provides an analogous defence in section 126(4).

Recent United Kingdom examples are:

› Police obtained immigration records about the complainant police officer that proved she had flown to Barbados with her daughter when she was on sick leave and had not informed her supervisor. This was a minor disciplinary infraction. The relevant power to request immigration information was available only in relation to law enforcement functions, which does not include disciplinary enquiries. It was reported that the relevant Detective Inspector also requested information from Virgin Atlantic, citing the non-existent Police Act 2007.[104] The error by police staff in interpreting their powers led the County Court to find the Police Force committed the tort of misuse of private information, as well as a breach of the *Data Protection Act* (UK). The Court commented:

> "*True it is that all the witnesses for the Defendants displayed a troubling lack of insight, contrition or, indeed, any understanding that they or their Force had done anything wrong in 'data protection' terms*."[105]

› As part of open government initiatives the Home Office publishes monthly statistics of processes to repatriate families who have no right to remain in the United Kingdom. The document published is a spread sheet. Due to human error, the Office also published a link to a second sheet that contained personal information, such as names, nationality, age and the regional office handling the asylum claim. In the High Court the Home Office conceded the tort of misuse of private information and a breach of the *Data Protection Act*.[106]

[104] BBC News online (24/8/16)
[105] *Brown v Commissioner of Police for the Metropolis & Chief Constable of Police of Greater Manchester Police,* claim No 3YM09078 (7/10/16)
[106] *TLT & Ors v Secretary of State for the Home Department & Home Office* [2016] EWHC 2217

Annexure 2: Complaints resolution mechanisms – Roles and responsibilities

NSW privacy legislation allows citizens to make complaints about alleged breaches of privacy or informational rights either to the Privacy Commissioner or to the organisation involved in the alleged breach. Each mechanism confers different responsibilities upon the Privacy Commissioner and the respondent public sector agency or private organisation which in turn, become a responsibility of the 'employer'.

There is a requirement upon the employer however to ensure that the internal review application must be dealt with by an individual who must be as far as practicable, someone who was not substantially involved in any matter relating to the conduct involved in the application and who is an employee or officer of the agency and suitably qualified to deal with the matters raised in the application (section 53(4) PPIP Act).

The NSW public sector privacy complaints scheme

A: Complaints to the Privacy Commissioner

The PPIP Act provides for complaints to be made to the Privacy Commissioner about the alleged violation of, or interference with, the privacy of an individual (Part 4, Division 3 - complaints relating to privacy).

Role of the Privacy Commissioner:

The Privacy Commissioner may conduct a preliminary assessment of the complaint in order to decide whether to deal with the complaint [section 46(1)].

If the subject matter of the complaint relates to conduct about which an Internal Review request can be made directly to a public sector agency, the Privacy Commissioner must inform the complainant of the Internal Review process available under Part 5 of the PPIP Act and the remedial action that may be available, if the complainant decides to make an application for review of the conduct [section 46(2)].

The Privacy Commissioner may refer a complaint for investigation or other action to another person or body (section 47).
If the Privacy Commissioner decides to deal with a complaint, the Privacy Commissioner may:

- deal with the complaint; and
- make such inquiries and investigations in relation to the complaint as the Privacy Commissioner thinks appropriate (section 48).

In dealing with the complaint the Privacy Commissioner must endeavour to resolve the complaint by conciliation (section 49).

The Privacy Commissioner may by written notice request the complainant, and the person or body against whom the complaint is made, to appear before the Privacy Commissioner in conciliation proceedings [section 49(2)]. A public sector agency, which receives such notice, must comply with the terms of the notice [section 49(3)].

The Privacy Commissioner may make a written report as to any findings or recommendations by the Privacy Commissioner in relation to the complaint and give a copy of the report to the complainant, and other persons or bodies as appear to be materially involved in matters concerning the complaint (section 50).

Even though the Privacy Commissioner declines to deal with a complaint, or decides to refer the complaint to a relevant authority, the Privacy Commissioner may conduct an inquiry or investigation into any general issues or matters raised in connection with the complaint (section 51).

The Privacy Commissioner may make recommendations but these are not enforceable.

Requirements of public agencies:

These primarily relate to the requirement to give information to the Privacy Commissioner as the Privacy Commissioner may require any person or public sector agency to:

› give the Privacy Commissioner a statement of information, or

› produce to the Privacy Commissioner any document or other thing, or

› give the Privacy Commissioner a copy of any document [section 37(1)].

The Privacy Commissioner is not to make any such requirement if it appears to the Privacy Commissioner that:

› the person or public sector agency concerned does not consent to compliance with the requirement, and

› the person or public sector agency would not, in court proceedings, be required to comply with a similar requirement on the grounds of public interest, privilege against self-incrimination or legal professional privilege [section 37(2)].

Also any request received by the entity must be in writing and specify or describe the information, document or thing required, and must specify the time and manner for complying with the requirement [section 37(3)].

B: Applications for Internal Review of complaints to the agency concerned

A person who is aggrieved by the conduct of a public sector agency concerning "personal information" can make an application to the agency for an Internal Review of the conduct (Part 5 of the PPIP Act – Review of certain conduct). The conduct could be a contravention of an IPP or privacy code of practice that applies to the agency or disclosure of personal information kept in a public register (sections 52 and 53).

Part 5 of the PPIP Act is also the mechanism for aggrieved persons to request Internal Reviews regarding contraventions in the HRIP Act concerning "health information."

Role of the Privacy Commissioner:
The Privacy Commissioner has an oversight role and is empowered to make submissions to the agency in relation to the subject matter of the application (section 54).

Requirements of public agencies:
The Privacy Commissioner must be informed of an application for Internal Review and kept informed of the progress of the internal review. As stated previously, the Privacy Commissioner is empowered to make submissions to the agency in relation to the subject matter of the application (section 54). Typically, public sector agencies send draft investigation reports to the Privacy Commissioner to review the thoroughness of the investigation and enable the Privacy Commissioner to make submissions.[107]

Following completion of the internal review the public sector agency may do any one or more of the following:

› take no further action on the matter;

› make a formal apology to the applicant;

› take such remedial action as it thinks appropriate (e.g. the payment of monetary compensation to the applicant);

› provide undertakings that the conduct will not occur again;

› implement administrative measures to ensure that the conduct will not occur again [section 53(7)].

If a person is not satisfied with the findings of the internal review or the action taken by the public sector agency in relation to the matter, he/she can apply to the Tribunal for review of the conduct (section 55).

On reviewing the conduct of the public sector agency, the Tribunal may decide not to take any action on the matter, or it may make orders including requiring the public sector agency to:

› pay the applicant damages not exceeding $40,000 by way of compensation for any loss or damage suffered because of the conduct;

› refrain from any conduct or action in contravention of an information protection principle or a privacy code of practice;

[107] See for more details Office of the NSW Privacy Commissioner (2016) "*Guidance: The Privacy Commissioner's oversight role in internal reviews of privacy complaints.*" Available at: www.ipc.nsw.gov.au

- comply with an information protection principle or a privacy code of practice;
- correct personal information that has been disclosed,
- take specified steps to remedy any loss or damage suffered by the applicant,
- not disclose personal information contained in a public register.

The Tribunal can make also ancillary orders as it thinks appropriate.

If in the course of a review the Tribunal is of the opinion that the chief executive officer or an employee of the public sector agency concerned has failed to exercise in good faith a function conferred or imposed on the officer or employee by or under this Act (including by or under a privacy code of practice), the Tribunal may take such measures as it considers appropriate to bring the matter to the attention of the responsible Minister (if any) for the public sector agency.

Decisions of the Tribunal may be reviewed by the Appeal Panel of the Tribunal (Part 6 of the *Civil and Administrative Tribunal Act 2013*). Decisions of the Tribunal Appeal Panel may be subject to appeal in the Supreme Court of NSW (section 32(3) of the *Civil and Administrative Tribunal Act 2013*).

Requirements of the Employee(s)
There are no additional provisions relating directly to the employee(s) who may have been involved in the complaint other than those already outlined.

The NSW health privacy complaints scheme regarding private organisations

Part 4 of the HRIP Act extends the Privacy Commissioner's investigative powers to private sector organisations, which are:

- Health service providers and hold health information irrespective of the size of their enterprise, and
- Organisations, which do not provide a health service, but hold health information and they are over a certain size.[108]

The definition of health service is wide and captures a variety of professionals, such as hospitals, medical and pharmaceutical services, community health centres, and, ambulance, Chinese medicine, chiropractic, optical, psychology and alternative therapy services that provide health care.[109]

Role of the Privacy Commissioner:
The HRIP Act empowers the Privacy Commissioner to receive and investigate complaints regarding alleged contraventions of the HPPs by private organisations and the special provisions in the HRIP Act that apply only to the private sector regarding access to and amendment of health information.[110]

The Privacy Commissioner has powers to assess a complaint and if accepted to be dealt with under the scheme, to conciliate or investigate the complaint.[111] The Privacy Commissioner's reports are not enforceable.

Where the Privacy Commissioner prepares a report under section 47 and the complainant remains dissatisfied with the outcomes, the complainant may request review of their complaint in the Tribunal. The Tribunal has powers to issue binding decisions.

Responsibilities of private organisations:
The requirements to provide information and to assist in any investigation are consistent with those in the PPIP Act with the addition of a requirement that a person must not by intimidation, threat or harassment influence an individual to essentially prevent them from exercising their rights under the HRIP Act.[112]

[108] The HRIP Act describes private organisations as "private sector persons." With an annual turnover of more than AU$3 million: see definition of small business operator in section 6D of the federal *Privacy Act 1988*.
[109] Section 4 HRIP Act
[110] Sections 26 to 37
[111] Sections 41 to 47
[112] section 70

Annexure 3: 'Liability and reasonable measures' defence in anti-discrimination and anti-harassment laws

The controlling provision in the NSW *Anti-Discrimination Act 1977* is section 53, which relevantly says:

> *53 Liability of principals and employers*
>
> *(1) An act done by a person as the agent or employee of the person's principal or employer which if done by the principal or employer would be a contravention of this Act is taken to have been done by the principal or employer also unless the principal or employer did not, either before or after the doing of the act, authorise the agent or employee, either expressly or by implication, to do the act.*
>
> *(2) If both the principal or employer and the agent or employee who did the act are subject to any liability arising under this Act in respect of the doing of the act, they are jointly and severally subject to that liability.*
>
> *(3) Despite subsection (1), a principal or an employer is not liable under that subsection if the principal or employer took all reasonable steps to prevent the agent or employee from contravening the Act.*

There are two notable issues:

First, both employer and employee or agent may be made liable for discriminatory acts: for example, at the workplace, for conduct towards colleagues, or, in the provision of services, for conduct towards clients.

Remedies are available where the employee's or agent's conduct is contrary to the employer's policies and practices, is unknown to the employer and is by definition prohibited, as it is a breach of the *Anti-Discrimination Act*.

The phenomenon of "*moral hazard*" has been used in industries such as regulation of organisations to design responsibility allocations. It arises in situations where the interests of the principal are not aligned with those of the agent, leaving the agent with incentive to act contrary to the principal's intentions or obligations.

A tool to manage "*moral hazard*" is to make sure that all those who have some control of a risk and the ability to cause harm know that they may be held responsible.[113]

Section 53 provides incentives for everyone with power and opportunity to breach the statute not to do so, due to the prospect of becoming subject to complaints and financial liability.

In discussing the work that section 53 does, the NSW Court of Appeal said:

> *"…..The purposes of the Anti-Discrimination Act are better served by focusing that burden on the actual perpetrator or perpetrators of the unlawful conduct."* [114]

Secondly, the requirement for discrimination prevention measures extends after the event that triggered the complaint in question.

Examples from decided cases illustrate the need for a thorough approach to good governance:

- The NSW Police had dismissed an employee. In the unfair dismissal litigation, in the NSW Industrial Relations Commission, the Police submissions included reference to a report of inquiry Barrister Chris Ronalds SC had prepared for the Police in 2006. It identified that an important aspect of satisfying the requirement to take reasonable steps to prevent sexual harassment, is to take "*appropriate action against perpetrators including dismissing police officers for serious acts of sexual harassment*."[115]
- In a sexual harassment case the NSW Tribunal found sufficiency in relevant policies, but held the agency liable for not having a training programme on the policies in place and communicating them to staff, including how to handle complaints. The Tribunal found both the

[113] See discussion of the concept in: Tom Baker & David Moss "*Government as risk manager*" in David Moss & John Cisternino, *New perspectives on regulation*, 2009, The Tobin Project, Cambridge, MA, 93. Robert Baldwin, Martin Cave & Martin Lodge *Understanding Regulation – Theory, Strategy & Practice* (2nd Ed), 2012, Oxford University Press, Oxford, 20

[114] *Commissioner of Police v The Estate of Edward John Russell & Ors* [2002] NSWCA 272, [76]

[115] *Parfrey v Commissioner of Police* [2010] NSWIRComm 19, [116]

agency and the perpetrator employee liable.[116]

› In a case of sexual harassment of a club clerk by the club's President, the Supreme Court upheld the Tribunal's finding that the club had not taken reasonable anti-harassment measures because it did not appear that it had made any real attempt "… *to communicate to the directors the existence of the sexual harassment circular and the importance of not engaging in conduct which might contravene the relevant provisions of the Act*."[117]

› When considering the conduct of an assistant manager, the Appeal Panel of the NSW Tribunal upheld the primary Tribunal's finding that there was a policy and some training, but "*there is little evidence that this policy was enforced and consequently it was ineffective in preventing Mr Matic's conduct.*"[118]

› In relation to training programs, the Tribunal held that it is not sufficient to hold briefing sessions with attendance being discretionary. Unless training is compulsory, it may be that those least aware of their obligations were able to avoid attending.[119]

› In another NSW Tribunal decision, the NSW public sector agency presented evidence that it had taken reasonable steps to protect employees from sexual harassment, including the reactive step of disciplining the perpetrator. The Tribunal agreed and it found only the perpetrator employee liable.[120]

The NSW approach is similar to that of the Federal and Victorian systems:

› In order to absolve an employer of liability, the Federal Court required that a policy must clearly state that conduct is against the policy, and identify the law that wrongdoings breach. This way an employer shows a lively interest that it will have in "*scrupulous adherence to its warnings*." Omission of such things resulted in a finding that the company did not have sufficient measures in place to prevent the wrongdoing.[121]

› The Victorian Supreme Court found against the employer, as the company had identified a risk to bullying the employee complainant, but failed to follow up on its own view that a risk assessment was necessary. The Court said: "*The Board did not properly monitor, on an ongoing basis, the behaviour of its employees inter se*."[122]

Federal anti-discrimination judgments stress the need to have in place both proactive measures to combat discrimination, especially training, and reactive measures after the employer becomes aware of the alleged conduct of employees.[123]

116 *Dee v NSW Police & Anor* (No 2) [2004] NSWADT 168, [71 – 79]
117 Shellharbour Golf Club v Wheeler [1999] NSWSC 224, 49
118 *Sharma v QSR Pty Ltd t/as KFC Punchbowl* [2010] NSWADTAP 22, [35]. In *Borg v Commissioner, Department of Corrective Services & Anor* [2002] NSWADT 42, [107] and [158] the Tribunal found both the Department and the employee liable and held that policies regarding harassment were not properly implemented.
119 *Hunt v Rail Corporation of NSW* [2007] NSWADT 152, [204]
120 *Cooper v Western Area Local Health Network* [2012] NSWADT 39, [55]
121 *Richardson v Oracle Corporation Australia Pty Ltd* [2013] FCA 102, 163]
122 *Swan v Monash Law Book Co-operative* [2013] VSC 326, [176]
123 Australian Human Rights Commission (2016) *Federal Discrimination law*, 161 & 259. Also in: (2008) *The Right to a Discrimination-Free Workplace*, available at: https://www.humanrights.gov.au/publications/right-discrimination-free-workplace

Annexure 4: Industry specific extensions of the Internal Review scheme

As this report has discussed, the NSW privacy legislation has gaps in the rights it provides to persons aggrieved by the conduct of government contractors, as enforceable rights may be claimed only against public sector agencies.

The following industry specific mechanisms are useful in NSW to achieve widening of the coverage of the legislation.

The first mechanism: Assigning public sector agency status to contractors through the PPIP Act

The definition of public sector agency in section 3 includes private sector organisations that have been engaged or have been funded by the public sector to provide data services. Data services relate to collection, processing, disclosing or using personal information for some purpose or project. There are no private organisations prescribed under the Regulation as public sector agencies for this purpose. This means that this facility is not being used by the public sector to ensure that its data services contractors are directly regulated under the PPIP Act in their processing of personal information.

The second mechanism: Assigning public sector agency status through agency specific legislation

It is possible to deem private sector entities to be public sector agencies in relation to specific functions, which they have been engaged by a government department to perform. An example of this arrangement is the *Land and Property Information NSW (Authorised Transaction) Act 2016*. Section 39(1) provides:

> *39 Privacy*
>
> *(1) The authorised operator is deemed to be a public sector agency for purposes of the Privacy and Personal Information Protection Act 1998 in relation to titling and registry functions.*

This enables complainants to request an Internal Review of their privacy complaint directly to a company regarding that company's conduct when it contracts to the Department of Finance, Services and Innovation for the services specified in the section.

The third mechanism: Assigning public sector agency status to affiliates

Under the *Health Services Act 1997* a number of statutory health corporations, and, private hospitals and health organisations accept Internal Review applications regarding health privacy complaints. They are listed in Schedules 2 and 3 of that Act. They typically have strong public purposes connections with the purposes of the NSW Health Ministry and are bound by the Ministry's privacy management policies.[124]

One example of a private hospital subject to the Internal Review mechanism was the allegation that St Vincent's Hospital had disclosed without consent, health records to an external medical practitioner and the Health Care Complaints Commission.[125]

The fourth mechanism: Assuming responsibility for conduct of contractors

The NSW workers compensation scheme engages a number of insurance companies, known as scheme agents. They are typically engaged to investigate, assess and manage workers compensation claims. Section 154N of the *Workers Compensation Act 1987* enables Regulations to be made regarding the confidentiality obligations of the scheme agents. Under section 154K the records of scheme agents in the exercise of these functions remain the property of the Nominal Insurer. Following the commencement of the *State Insurance and Care Governance Act 2015*, Workcover NSW was abolished and Insurance and Care NSW (ICARE) assumed its role. ICARE acts for the Nominal Insurer in the same way Workcover previously did.

ICARE assumes responsibilities for issues of information access regarding records of the scheme agents and for privacy complaints. Similarly, ICARE makes voluntary notifications to the Privacy Commissioner for data breaches arising from the work of the scheme agents.

---

[124] NSW Health (2005) "*Privacy Manual (version 2)*," 4; (2015) "*Privacy Management Plan*," 1

[125] *AQB v St Vincent's Hospital Sydney Ltd* [2013] NSWADT 210

The fifth mechanism: Deeming an agency as the 'service provider' when it has engaged non-employees to provide a service (to an individual)

Part 5 of the *Privacy Code of Practice (General) 2003* deals with the provision of certain services to offenders. It provides that the definition of staff member of Corrective Services (now a Division of the Department of Justice) includes a person working under contract.

Clause 12(2) of the Code extends the Department's obligations by deeming the Department to be the service provider. The clause provides:

(2) For the purposes of this Part, the following services or programs provided to an offender are taken to be provided by the Department:

(a) a service or program provided on behalf of the Department,

(b) a service or program provided because of a requirement placed on the offender by a court or any of the following bodies within the meaning of the Crimes (Administration of Sentences) Act 1999:

(i) the Parole Authority,

(ii) the Review Council,

(iii) the Probation and Parole Service.

As a Tribunal decision dealing with this issue has not been identified, the effect of this provision on the Department of Justice's obligations, under the PPIP Act for the conduct of persons who are not departmental employees, is not known.

Annexure 5: The elements of a good data security governance framework

The measures that employers need to put in place in order to ensure that personal and health information they hold is protected from accidental or mischievous uses and disclosures by employees needs to include:

Policy

- A strong, clear and unambiguous policy that reinforces that privacy concerns should be appropriately considered in all aspects of the agency's operations and especially when dealing with personal information. This includes adopting a privacy by design approach and the application of a Privacy Impact Assessment to projects including new and amended policies, systems, legislation and service delivery models.[126]
- The policy is communicated effectively in the workplace.
- Visible support for the policy from senior management.
- Regular review of the policy and related procedures to ensure they are up to date with the law and best practice, and, ensure that any updates are clearly communicated to staff.

Systems

- A clear governance framework for the management of information systems, including policies, procedures and protocols for access to, amendment of, use and disclosure of personal information obtained from information systems.
- Effective and regular communication of the policy, procedures and protocols relating to access to, amendment of, use and disclosure of personal information obtained from information systems in the workplace, including when they access information systems.
- Clear alerts in the sign-in protocols for information systems reminding employees of their obligations under the PPIP Act and making clear that they must not use personal information used in their employment for unauthorised purposes (which includes participation in private community activities).
- Monitoring compliance with the policy, protocols and procedures and be visible in enforcing compliance with them.

Training

- Regular training to staff to ensure they are aware of the entity's policies and procedures to ensure the protection of privacy and personal information held by the agency and that they understand their responsibilities for protection of privacy and personal information, including their obligations to comply with the IPPs and any privacy code of practice applicable to the agency and not to use or disclose information used in their employment for unauthorised purposes.
- Training for employees who are responsible for dealing with privacy complaints and applications for internal review.

Complaints

- Clear responsibilities and procedures to respond to privacy complaints to ensure they are treated seriously and handled fairly, promptly and effectively.
- Clear, unambiguous and visible support from senior management for the agency's privacy complaints procedures, including providing oversight of their implementation, monitoring the number, nature and outcome of complaints and ensuring that any systemic issues identified are rectified.
- Visibly nominated privacy contact officers with whom employees and the community can discuss any questions, concerns or complaints about privacy.

Monitoring and reporting

- Mechanisms to monitor the implementation of the agency's policies and procedures, including regular reporting to senior management on issues such as:
  - privacy risks identified through Privacy Impact Assessments.
  - privacy breaches and risks identified through complaints and applications for internal review.

[126] NSW Privacy Commissioner (2016) "*Guidance: Guide to Privacy Impact Assessments in NSW*"

- internal sanctions applied to employees who have been found to have contravened provisions of the PPIP Act.
- consideration of referrals to professional licencing bodies regarding employees who must be licenced to practice their profession.
- Consideration of referrals to police in cases of conduct that may be a criminal offence.

- Mechanisms to rectify contraventions or shortfall in practice to ensure improvement in order to avoid repeat data breaches.
- Public reporting via Annual Reports or entity websites.

Comments and other feedback is welcome.
Please address to:

OFFICE OF THE PRIVACY COMMISSIONER NSW

Level 3, 47 Bridge Street
Sydney NSW, 2000

PO Box R232
Royal Exchange NSW, 1225

Free call:
1800 IPC NSW
(1800 472 679)
Direct: (02) 9258 0066
Fax: (02) 8114 3756

Email: privacy@ipc.nsw.gov.au

Web: www.ipc.nsw.gov.au/privacy

OFFICE OF THE PRIVACY COMMISSIONER, NSW

ISBN: 78-0-9876237-0-6

OPC: RP2017/001