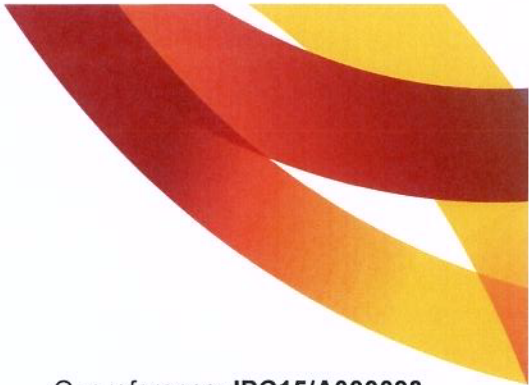


**INQUIRY INTO REMEDIES FOR THE SERIOUS INVASION  
OF PRIVACY IN NEW SOUTH WALES**

**Name:** Dr Elizabeth Coombs, NSW Privacy Commissioner

**Date received:** 29/09/2015

---



Our reference: **IPC15/A000093**

The Director  
Standing Committee on Law and Justice  
Parliament House  
Macquarie Street  
SYDNEY NSW 2000

28 SEP 2015

via e-mail: [lawandjustice@parliament.nsw.gov.au](mailto:lawandjustice@parliament.nsw.gov.au)

Dear Director,

**Submission to Inquiry into remedies for the serious invasion of privacy in New South Wales**

I write to provide you with my submission to the Legislative Council's inquiry into remedies for the serious invasion of privacy in New South Wales.

The purpose of my submission is to highlight and identify:

- the importance of protecting the privacy of individuals;
- key regulatory issues, including possible amendment of NSW privacy legislation;
- major and emerging issues in relation to privacy that pose serious challenges to the privacy of individuals and to the NSW privacy legislative framework;
- factors in favor of developing a statutory cause of action; and
- the possible scope and elements of a cause of action, including the role of the NSW Privacy Commissioner.

I am happy to assist the Standing Committee further with any questions about the NSW privacy regime, any issues or concerns raised by submissions or witnesses in regard to the operation of the regime and how a statutory cause of action would sit within it, and potential reforms to the NSW privacy legislation and the functions of the NSW Privacy Commissioner.

I agree to this submission being published, should the Committee decide to publish submissions. Please ensure that prior to the publication of this letter that my signature is redacted from the version to be published.

Yours sincerely

Dr Elizabeth Coombs  
**NSW Privacy Commissioner**



office of the  
privacy  
commissioner  
new south wales

## **Submission to Inquiry into remedies for the serious invasion of privacy in New South Wales**

## Executive Summary

The purpose of this submission is to highlight and identify:

- the importance of protecting the privacy of individuals
- key regulatory issues, including possible amendment of NSW privacy legislation
- major and emerging issues in relation to privacy that pose serious challenges to the privacy of individuals and to the NSW privacy legislative framework
- factors in favour of developing a statutory cause of action
- the possible scope and elements of a cause of action, including the role of the NSW Privacy Commissioner.

This submission is based on a set of principles originally outlined by the Australian Law Reform Commission (ALRC) in its report 123, *Serious Invasions of Privacy in the Digital Era*, June 2014 (ALRC 2014 report).<sup>1</sup> These principles, outlined below, provide a useful framework for considering both the design of a statutory cause and how it would be set in the broader privacy regime in NSW:

- Privacy is a fundamental value worthy of legal protection.
- There is a public interest in protecting privacy.
- Privacy should be balanced with other important interests.
- Australian privacy laws should meet international standards.
- Privacy laws should be adaptable to technological change.
- Privacy laws should be clear and certain.
- Privacy laws should be coherent and consistent.
- Justice to protect privacy should be accessible.
- Privacy protection is an issue of shared responsibility.

No statutory cause of action currently exists in Australia. No Australian appellate court has recognised a common law tort for invasion of privacy. The ALRC, the NSW Law Reform Commission (NSWLRC) and the Victorian Law Reform Commission (VLRC) have all recommended the introduction of a statutory cause of action for invasions of privacy either as a tort or as a cause of action<sup>2</sup>.

The Commonwealth, Victorian and NSW Governments have not acted on the respective recommendations of the Law Reform Commission reports.

In my 2015 report to Parliament on the operation of the *Privacy and Personal Information Protection Act 1998* (PPIP Act), I supported the development of one privacy regime covering all Australian jurisdictions, through greater alignment between NSW privacy legislation with Commonwealth legislation. Previous NSW Privacy Commissioners have supported the development of a statutory cause of action. I also broadly support the development of a civil law cause of action in statute.

Action is required to address the implementation of a remedy for serious invasion of privacy.

NSW has led the way in privacy protection, providing a catalyst for other jurisdictions to take action. Further leadership could occur in implementing a statutory cause of action. This Inquiry itself is a chance to determine whether it is appropriate for NSW to take leadership on this issue and push ahead with its own approach.

I refer the Committee to NSW's leadership in 1975 in becoming the second jurisdiction in the world to introduce legislation dealing specifically with privacy protection (further background information is at **Attachment A**). An overview of the current legislative framework is at **Attachment B**.

In summary, I support the development of a statutory cause of action to fill the gaps in the NSW privacy legislative framework and to provide an avenue of redress for serious invasions of privacy of individuals which does not currently exist in NSW.

---

<sup>1</sup> Australian Law Reform Commission, Report 123, *'Serious Invasions of Privacy in the Digital Era'*, June 2014 (ALRC 2014 report), pgs 29-40

<sup>2</sup> These reports are the NSW Law Reform Commission, Report 120, *'Invasion of Privacy'*, April 2009 (NSWLRC 2008 report), Victorian Law Reform Commission, Final Report 18, *'Surveillance in Public Places'*, May 2010 (VLRC 2010 report), the Australian Law Reform Commission, Report 108, *'For Your Information: Australian Privacy Law and Practice'*, August 2008 (ALRC 2008 report) and ALRC 2014 report.

## 1. Protecting the privacy of individuals in a changing environment

### *Privacy as a fundamental right*

- 1.1. The protection of an individual's privacy is a critical part of modern democratic values. As the VLRC stated in its Final Report 18, 'Surveillance in Public Places', May 2010 (VLRC 2010 report):

*"privacy is a value of increasing importance to the entire community because it recognises and promotes human dignity" <sup>3</sup>.*

- 1.2. Privacy is enshrined as a human right in the United Nations Universal Declaration of Human Rights 1948. Article 12 of the Declaration states:

*'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'* <sup>4</sup>

- 1.3. Article 17 of the United Nations International Convention on Civil and Political Rights 1976, of which Australia is a signatory, also states:

*1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation'.*

*2. Everyone has the right to the protection of the law against such interference or attacks.'* <sup>5</sup>

- 1.4. NSW has a proud history in privacy protection. It was the second international jurisdiction to legislate in 1975 to protect the privacy of citizens. More detail on the history of privacy legislation is contained in my 2015 report to Parliament, 'Report of the Privacy Commissioner under Section 61B of the Privacy and Personal Information Protection Act' and has been extracted at Attachment A.

### *Challenges to privacy posed by technology and other issues*

- 1.5. All NSW citizens must have their privacy rights respected, whatever their location or circumstances, particularly in an environment where technology is rapidly changing and can be used in a range of ways. The community shares these concerns. Examples of relevant privacy issues identified by the public and included in my report to Parliament are at **Attachment C**.

- 1.6. The ALRC has previously provided some examples of what activities could amount to serious invasions of privacy<sup>6</sup>:

- by physically intruding into the plaintiff's private space or by watching, listening to or recording the plaintiff's private activities or private affairs
- by collecting or disclosing private information about the plaintiff
- serious interference with an individual's home or family life
- an individual has been subjected to unauthorised surveillance
- an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed
- sensitive facts relating to an individual's private life have been disclosed.

- 1.7. There are a number of issues emerging that pose serious challenges, in terms of the adequacy of NSW privacy legislation and its ability to deal with rapid changes to technology. The following sections discuss some notable trends.

### *The coverage of privacy law to metadata*

- 1.8. The internet and access to metadata by public and private sector organisations has become of increasing importance, particularly in a time of growing interest in big data.

<sup>3</sup> VLRC 2010 report, page 147

<sup>4</sup> United Nations Universal Declaration of Human Rights 1948, Article 12

<sup>5</sup> United Nations International Convention on Civil and Political Rights 1976, Article 17

<sup>6</sup> These examples featured in the Australian Law Reform Commission, report 108, 'For Your Information: Australian Privacy Law and Practice', August 2008 (ALRC 2008 report) and the Australian Law Reform Commission, report 123, 'Serious Invasions of Privacy in the Digital Era', June 2014 (ALRC 2014 report).

- 1.9 A key issue for privacy law is whether 'metadata' is covered under the existing definitions of personal information. For example, under section 4 of the PPIP Act, personal information means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.
- 1.10 The ability to identify an individual was a key issue in the case of Ben Grubb and Telstra Corporation Ltd [2015] AICmr 35 (1 May 2015). This case, pursued under the Commonwealth *Privacy Act 1988*, highlights the creation of new types of personal data that are now being recognised as deserving protection, by focussing on whether an individual's identity could be reasonably ascertained from metadata.
- 1.11 Mr Grubb lodged a complaint with the Office of the Australian Information Commissioner (OAIC) on 8 August 2013, claiming that Telstra Corporation Ltd (Telstra) had breached the Privacy Act by refusing to give him access to all the metadata it held in relation to his mobile phone service. In this case, Telstra eventually conceded that some metadata did constitute personal information. This information included itemised bills, outgoing call data records, subscriber information, personal unlock key number, the SIM number, the handset ID, the mobile network and the colour of the phone.
- 1.12 The Commonwealth Privacy Commissioner found Telstra able to ascertain an individual's identity, and that network data and inbound call numbers therefore constituted personal information. On the latter point, the Commissioner stated that Telstra could refuse access to inbound call information if this would have an unreasonable impact on the privacy of other individuals. The Commissioner determined that Telstra had interfered with the privacy of Mr Grubb by refusing to provide him with access to the metadata and ordered Telstra to provide the metadata to him within 30 days. Telstra has lodged an appeal.
- 1.13 Data prescribed under the new Commonwealth data retention laws (*Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth)), which require telecommunication companies to retain and secure metadata records for two years, are considered personal information for the purposes of the Privacy Act.
- 1.14 My 2015 report to Parliament outlines the general issue of new technologies and its impact on the definition of 'personal information' in the PPIP Act and how such information is captured. I recommend guidelines be developed to assist NSW public sector agencies and the public (recommendation 1).
- 1.15 In the same report, I propose the preparation of a research paper, for the Parliament, on the implications of the increasing convergence and capacity of information communication technology (recommendation 2). This piece of work would require additional resourcing to complete, but would provide the Parliament with valuable insight and information on a critical emerging issue.

### ***The use of technology in privacy invasive ways***

- 1.16 Surveillance technology and digital communication are examples of the kinds of technological platforms that facilitate invasions of privacy. Other technologies that may not be intended for surveillance are also likely to have privacy impacts. This is a particular issue as surveillance and other digital communications technologies are now within reach of individuals.
- 1.17 Technology can be used in different ways to invade the privacy of individuals. The use of the technology could constitute an invasion of privacy where the individual who is the subject of the invasion does not know that it is occurring, has not consented or it is used to survey private activity. This may not necessarily involve the collection of information, and the individual or organisation doing the invasion may not even deliberately intend to invade the privacy of the person. In some cases, the invasion may occur to a group of people, rather than a single individual. In addition, technology may be used not only by public sector agencies, but also by private enterprises and private individuals.
- 1.18 I provide some examples where these technologies and platforms could facilitate invasions of privacy:

- the posting by private individuals of personal information, information about private matters or images (such as revenge pornography) on social media
  - the filming by a private individual of a vehicle accident and posting the footage on social media
  - the use of technology to undertake “up-skirting” in public places
  - the use of technology to intercept telephone calls, listen covertly and/or record private conversations of another person.
  - the use of drones by public sector agencies for law enforcement purposes and in emergency situations
  - the use of drones by private individuals for recreational reasons
  - the use of drones by private businesses for commercial purposes, such as to survey land or agricultural stock
  - the use of surveillance devices in public places and workplaces to film and record, such as the use of drones, CCTV or other camera devices
  - the use of surveillance devices in private spaces, such as homes
  - the use of surveillance devices, such as CCTV, by a business outside of a shopfront that records footage of another premises or within a shop that films clients
  - surveillance technology that tracks and captures locational information, such as Global Positioning Systems, mobile phones and smartcards.
- 1.19 My 2015 report to Parliament addresses several of these issues, particularly in relation to surveillance, cloud computing and information technology security (recommendations 18, 19, 20, 21, 22, and 23 of the report).
- 1.20 Of particular currency is the use of social media, such as Facebook, to engage in conduct that could amount to serious invasions of privacy. This could involve a private individual posting images, videos or other information on social media of another person. The person posting the material may not know the person who is subject to the invasion or may be well known.
- 1.21 The rise of ‘revenge pornography’ as a means of an invasion of privacy is noteworthy, given the seriousness and offensive nature of such acts. This has been the subject of a recent NSW Parliamentary Library e-brief, ‘*Revenge pornography, privacy and the law, 7/2015*’<sup>7</sup>.
- 1.22 Another scenario could involve a public sector agency posting a photo or video of a member of the public on social media without that person’s knowledge or consent.
- 1.23 This is also an area of increasing concern for the general public. My Office has received a number of enquiries from members of the public concerned about what redress is available when personal images, videos and other textual information is posted on social media sites without their knowledge or consent.
- 1.24 These concerns and the examples above demonstrate the challenges that are arising from the increasing availability, pervasiveness, and ease of use of technology in potentially privacy invasive ways.
- 1.25 I would encourage the Committee to adopt a broad approach, rather than focusing on one particular manifestation of serious invasion, however offensive it may be. This would ultimately reduce fragmentation, whereby one form of serious invasion of privacy is covered, but others are not.
- 1.26 There are also examples of potential activities that could amount to invasions of privacy noted in various reports, case law and by the Australian and international media, but are not reliant on any particular technology. These include:
- the accessing of personal information by an individual without the person’s knowledge or consent
  - the selling or publishing of personal information or images by one person to another recipient

<sup>7</sup> NSW Parliamentary Library e-brief, ‘*Revenge pornography, privacy and the law, 7/2015*’ at <http://www.parliament.nsw.gov.au/prod/parliament/publications.nsf/v3listrpsubject>

- the publication by media outlets of personal information or images of public figures in private settings
- situations where sensitive personal records are left in a public place
- the observing or filming of a person in a private space or engaging in a private act
- situations where an individual is stalked and harassed by a photographer
- situations where an individual is strip searched by a public officer who has no authority to do so.

### Data breaches that cross borders

- 1.27 In the digital era, invasions of privacy could increasingly occur over the internet, through applications, or “apps”, and via digital platforms owned by companies based off-shore.
- 1.28 The latest example of this is the hacking of the Ashley Madison website, an extramarital dating website. A hacking group, known as Impact Team, infiltrated the website and downloaded and released personal, financial and identifying information of Ashley Madison’s registered users. Ashley Madison’s parent company is Avid Life Media Inc, based in Canada.
- 1.29 Lawsuits have been filed in the United States against Ashley Madison and its parent company by users of the website claiming negligence and invasion of privacy causing emotional distress<sup>8</sup>. A class action against Avid Life Media has also been filed in Canada<sup>9</sup>.
- 1.30 In contrast, Australian users of the website whose personal information may have been leaked as part of the hack cannot seek redress through the courts as there is no common law tort for invasion of privacy in Australia.
- 1.31 The Commonwealth Privacy Commissioner has commenced a joint investigation with the Canadian Privacy Commissioner into the data breach in Australia, in particular, the obligations of organisations that carry on business in Australia to take reasonable steps to ensure that the personal information they hold is held securely<sup>10</sup>.
- 1.32 The ability of the Commonwealth Privacy Commissioner to investigate such matters provides a limited, indirect avenue of redress for those individuals affected by the data breach. However, the Commissioner’s ability to intervene relies heavily on the interpretation of the scope of the territorial jurisdiction of the Privacy Act. The Privacy Act extends to an act done, or a practice engaged in, outside Australia by an organisation that has an Australian link.
- 1.33 The NSW PPIP Act provides no recourse for NSW citizens affected by this breach. Moreover, the NSW PPIP Act provides no protection to data sent outside NSW (or to a Commonwealth agency within NSW borders). Such protections do exist for health information and the *Health Records and Information Privacy Act 2002* (HRIP Act) regulates the transfer of personal information out of NSW. I raised this issue in my report to Parliament (recommendation 14) and strongly support reform to increase the level of protection for personal information held by NSW public sector agencies that is transferred out of NSW.

### Big data and data analytics

- 1.34 The evolution of information communication technologies has given rise to new challenges in ensuring the protection of privacy and personal information by public sector agencies, private sector organisations and individuals and to new forms and expressions of governance – one of which is information governance.
- 1.35 In the past, some of the chief protections for privacy were that it was just so difficult to collate and link personal information. In 1996 the Hon. Michael Kirby observed:

<sup>8</sup> Examples of media reports of the US lawsuit are <http://www.theguardian.com/technology/2015/aug/25/man-sues-ashley-madison-for-emotional-distress-in-potential-class-action-lawsuit> and <http://www.reuters.com/article/2015/08/25/us-ashleymadison-cybersecurity-lawsuit-idUSKCN0QU05L20150825>

<sup>9</sup> Examples of media reports of Canadian lawsuits are <http://www.bbc.com/news/business-34032760> and <http://www.independent.co.uk/news/world/americas/ashley-madison-hack-canadian-lawyers-launch-368m-lawsuit-against-adultery-website-10467633.html>

<sup>10</sup> <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/ashley-madison-data-breach/ashley-madison-data-breach-investigation-commenced>

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

- 1.36 The advent of ‘big data’ holding vast amounts of information for a digital eternity has removed these ad hoc safeguards. Highly personal ‘big data sets’ are a prime target for hackers and criminals. But more regularly, data breaches arise from within an organisation – either from human or computer error, or from human action. The growth of interest in collecting, holding, using and sharing data has expanded not only the amount of data available but the associated risks for data breaches to occur. This is particularly relevant where the proliferation of data is accompanied by poor management practices, a lack of security safeguards or inconsistent approaches to sharing information.
- 1.37 These risks are compounded in situations where the same datasets are being accessed, shared and held by multiple users in multiple locations or where different datasets are linked, leading to the identification and re-identification of individuals, even in situations where the data in each separate dataset had been intentionally de-identified. New and novel data is also being gathered, such as biometric data for law enforcement, intelligence or other identification purposes. Some additional examples where the increasing interest in big data can facilitate invasions of privacy include:
- the digitisation of services and proliferation of digital footprints, such as the use of cloud computing services for storage and communication, and digital licences
  - increased use data analytics, including data mining
  - the use of government data in commercial ways or sharing with commercial entities.

## **2. Factors in favour of a statutory cause of action**

### ***Limitations of current legislative regime***

- 2.1. The PPIP Act and HRIP Act provide important privacy protections for NSW citizens in certain circumstances, but these protections are by no means comprehensive. They are not sufficient to address many of the challenges identified in the previous section.
- 2.2. For example, the PPIP Act does not apply to the activities of non-government organisations and private sector businesses who are not contracted service providers to NSW public sector agencies, NSW State Owned Corporations, and private individuals acting in their private, family or household capacity. The PPIP Act would also not cover the actions of employees of public sector agencies who are not acting in their official capacity.
- 2.3. The PPIP Act also contains exemptions from the NSW privacy regime for specific functions carried out by agencies, such as law enforcement and related matters (section 23, PPIP Act) and exemptions for investigative agencies (section 24, PPIP Act). Exemptions exist for NSW public sector agencies and organisations in specific circumstances, such as for people who have been reported as missing and for public health and safety.
- 2.4. Specific agencies and official roles are generally exempted from complying with all the privacy principles in the PPIP Act except in relation to the exercise of their administrative and educative functions (section 27). These are the NSW Police Force (NSWPF), the Independent Commission Against Corruption (ICAC), the Inspector of ICAC, the Police Integrity Commission (PIC), the Inspector of the PIC, the staff of the PIC and the NSW Crime Commission.
- 2.5. The NSWLRC has stated that NSW privacy legislation should recognise the unique and important role of these agencies in society but that privacy legislation should not be used as a ‘secrecy shield’ for agencies to hide behind. The NSWLRC further stated that in relation to the NSWPF<sup>11</sup>:

*“...we are of the view that there is no justification for the current level of exemption for the NSW Police Force. It will often be appropriate in circumstances to subject personal information held by the NSW Police Force to privacy principles. While it is important to*

---

<sup>11</sup> NSW Law Reform Commission, ‘Report 127: Protecting Privacy in New South Wales’, May 2010, page 118.

*recognise that their investigative and law enforcement functions are immune from privacy protection, other functions should otherwise remain subject to privacy principles.”*

- 2.6. Finally, the PPIP Act only regulates the handling of personal information (section 6) and does not cover explicitly physical, spatial or territorial privacy. The PPIP Act provides the Privacy Commissioner with broad powers to investigate physical privacy matters, but there are difficulties in exercising this statutory function.
- 2.7. The HRIP Act has similar issues. It is focused on NSW public and private health service providers and organisations above a certain size that hold health information, only covers health information and provides similar exemptions as the PPIP Act. Privacy law of the Commonwealth and other jurisdictions in Australia is also similarly limited.
- 2.8. The HRIP Act does regulate, however, the transfer of personal information out of NSW. This is in contrast to other privacy regimes in Victoria, Queensland and the Commonwealth.
- 2.9. Many of the examples outlined above in the section '*Challenges to privacy posed by technology and other issues*', would not be covered by the PPIP Act or HRIP Act except in situations involving personal information and health information and a NSW public sector agency that could not rely on an exemption.
- 2.10. A range of other legislation also exists in NSW which place restrictions or controls on the use, collection and disclosure of personal information. These range from surveillance laws, criminal law, child protection laws and health regulation, through to laws relating to the release of images under road transport legislation.
- 2.11. Certain issues relevant to privacy are appropriately addressed through other legislation, such as behaviour that is grossly offensive or criminal in nature. While some protections and remedies may be in place already, it is difficult to know with certainty whether these laws will address every specific situation when an invasion of privacy could occur or the gaps in this complex patchwork of law.

### **Restricted avenues for personal redress**

- 2.12. Without a tort for invasion of privacy in either common law or statute, aggrieved individuals have limited avenues to seek financial compensation for damages suffered.
- 2.13. Under the PPIP Act, an individual is entitled to an internal review by a NSW public sector agency if they are aggrieved about the agency's conduct in relation to their personal information. If an individual is not satisfied by the findings of the internal review or the action taken by the agency as a result of the review, they have the right to seek an external review by the NSW Civil and Administrative Tribunal (NCAT). NCAT has the authority to make an order of compensation for a maximum amount of \$40,000.
- 2.14. In the last financial year, the Tribunal has not made an award of the maximum amount available (\$40,000) for a breach of privacy. The last time NCAT awarded the maximum amount was in 2011. The average amount of compensation generally awarded by NCAT where a breach is found and compensation awarded has been between \$5,000 and \$8,000.
- 2.15. Public sector agencies may negotiate amounts in settlement of claims by aggrieved persons and would not be limited by the maximum amount set by NCAT. Any settlements made by agencies are likely to be confidential and subject to a deed of release by the parties. Settlement would more than likely take into consideration factors such as the nature of the breach, any loss or damages, any other costs incurred by the aggrieved person such as counselling, legal fees, and any other relevant issues.
- 2.16. Under the PPIP Act the Privacy Commissioner may investigate, inquire, conciliate and hold hearings with the parties to the complaint as part of the conciliation process. The PPIP also states the Privacy Commissioner must endeavour to resolve all complaints by conciliation. However, the Privacy Commissioner cannot make orders or award damages at the conclusion of conciliation. The Privacy Commissioner also cannot take further action after the conclusion of proceedings, whether or not the parties have reached an agreement. In addition, there is no

right of review to NCAT if the Privacy Commissioner conducts an investigation into a complaint and makes a decision.

- 2.17. Further background information on avenues for redress under the PPIP Act and HRIP Act is at **Attachment B**.

### Shortcomings of current common law options

- 2.18. Civil causes of action for serious invasions of privacy exist in New Zealand, the United Kingdom, the United States and some Canadian provinces<sup>12</sup>.
- 2.19. The New Zealand Law Commission (NZLC) in its 2009 report, *'Invasions of Privacy: Penalties and Remedies, Review of the Law of Privacy Stage 3'*, did not support the development of a statutory cause of action but instead, recommended that a tort continue to be developed through common law<sup>13</sup>. While the NZLC acknowledged that a statutory cause of action would make the law more accessible and certain, there was an absence of evidence that the current state of law was "causing practical difficulties to anyone"<sup>14</sup>. Other arguments against a statutory cause of action raised in the past include that it would alter the balance between privacy and other competing public interests/rights disproportionately, and that it would be an excessive response to issues that could be addressed through other mechanisms.
- 2.20. While I acknowledge international developments and the arguments against a statutory cause of action, there are limitations to leaving the development of a cause of action to the common law.
- 2.21. The ALRC, NSWLRC and VLRC provide very useful information about the development of a tort for invasion of privacy in common law in Australian jurisdictions including NSW, as well as the United Kingdom, New Zealand, Canada and the United States. The Commissions' commentary demonstrates that while some movement is occurring in common law, this is limited and likely to evolve slowly over time with the ALRC describing the movement as, at best, uncertain<sup>15</sup>.
- 2.22. For example, in Australia, though the High Court of Australia has left open the possibility of the development of a common law tort in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, only a limited number of trial courts have recognised a tort of invasion of privacy (for example, in *Grosse v Purvis* [2003] QDC 151 and *Doe v Australian Broadcasting Corporation* [2007] VCC 281<sup>16</sup>).
- 2.23. Other general common law causes of action, such as torts of trespass, nuisance and the equitable action for breach of confidence, which could be used to seek redress for a serious invasion of privacy, are also largely untested. For example, the equitable action for breach of confidence is often raised as a potential alternative to developing a cause of action for serious invasions of privacy. The cases of *Giller v Procopet* [2008] VSCA 236 and *Wilson v Ferguson* [2015] WASC 15 provide some evidence that NSW citizens may be able to seek remedies in equity for breach of confidence that relate to privacy, but these are only two instances<sup>17</sup>. Moreover, there are important differences between the concepts of privacy and confidence, and the circumstances of the relationships between the parties. Questions also remain about whether an equitable action could address all instances of invasions of privacy and how effective the action would be after a wrongful disclosure has occurred<sup>18</sup>.
- 2.24. As the ALRC stated in its 2008 report, there are problems inherent with trying to fit all the circumstances that may give rise to an invasion of privacy into a pre-existing cause of action or by waiting for a common law tort to emerge on a case by case basis<sup>19</sup>.

<sup>12</sup> ALRC 2014 report, pages 22-23.

<sup>13</sup> New Zealand Law Commission, *'Report 113, Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy: Stage 3'*, January 2010, recommendation 28 at page 91.

<sup>14</sup> *Ibid*, page 90.

<sup>15</sup> ALRC 2014 report, page 55.

<sup>16</sup> NSWLRC 2008 report, pages 11-12.

<sup>17</sup> ALRC 2014 report, page 183 and NSW Parliamentary Library e-brief, pages 12-15.

<sup>18</sup> ALRC 2014 report, page 52.

<sup>19</sup> ALRC 2008 report, page 2564.

## General conclusions

- 2.25. Few activities currently could give rise directly to a common law tort for invasion of privacy. Difficulties also arise in trying to seek to pursue privacy matters through other common law torts or the equitable action for breach of confidence. The NSWLRC has stated that tampering with existing causes of action or developing specific torts would be an unsatisfactory basis for the ongoing development of privacy law in a climate of dynamic societal and technological change<sup>20</sup>.
- 2.26. There are several advantages to using a statutory approach in relation to the cause of action. A statutory cause of action could provide consistency, in terms of the development of the law (as courts would only address the matter on a case by case basis and on the facts at hand), and a basis to address those unique or intermittent circumstances which are not covered by other regulation. It could help overcome differences between equitable and tort-based causes of actions, and the defences and remedies unique to each<sup>21</sup>. A statutory approach could provide a broader range of remedies and a more flexible approach, in contrast to courts that are limited to the existing remedies available to them<sup>22</sup>.
- 2.27. A statutory approach could provide individuals with a simple, clear way to seek a remedy. It would provide certainty to individuals that are currently experiencing or have experienced invasions of their privacy, but do not have access to a direct remedy.

## 3. Possible elements of a cause of action

- 3.1. The Committee is no doubt aware of the substantial analysis of the possible approaches to establishing a statutory cause of action for serious invasions of privacy by the NSWLRC, ALRC and VLRC. While the NSWLRC, ALRC and VLRC all supported the development of a statutory cause of action, the Commissions proposed slightly different models. The differences between the models proposed by the ALRC, NSWLRC and VLRC further suggest national harmonisation may be a longer term goal.
- 3.2. The main elements of the NSWLRC, ALRC and VLRC models are provided in a table at **Attachment D** to assist the Committee in identifying the differences between the proposals. The table focuses on the following aspects of a potential statutory cause of action:

### Scope

- 3.3. Two alternative options have been proposed – a broad cause of action that could cover any circumstances; a narrow cause of action that is limited to intrusion upon seclusion and misuse of private information.
- 3.4. One model proposed that the cause of action should be considered a tort while other models proposed a statutory cause of action. The main reasons why a tort was not considered appropriate by the latter models were:
- to enable a public interest balancing test to be included as an element of the cause of action
  - to ensure that the cause of action was not constrained by existing rules and principles applicable in the law of torts
  - to avoid the need for proof of damage to be an element of the cause of action.
- 3.5. The ALRC and NSWLRC supported the development of a nationally-consistent statutory cause of action based on the goal of national consistency for privacy regulation.

### Application

- 3.6. There is consistent support across the models for the cause of action to only be actionable by natural persons, not corporations and other organisations. There are differences in views between whether an action can survive the death of an aggrieved party and whether an action

---

<sup>20</sup> NSWLRC 2008 report, page 17.

<sup>21</sup> ALRC 2008 report, page 2565.

<sup>22</sup> ALRC 2008 report, page 2564.

can be taken against an estate of a deceased person. Varying approaches have been proposed on whether exemptions should apply.

### *Threshold*

- 3.7. There is consistent support across the models for an objective test of a person having reasonable expectations of privacy in all the circumstances, though variation in what the threshold should cover. For example, some models included the concept of seriousness and a fault element, while others did not. Proof of damage was generally considered to be relevant only when considering remedies.

### *Consideration of other relevant matters in determining actionability*

- 3.8. Some models suggested the inclusion of a non-exhaustive list of relevant matters for courts to consider when determining whether an action was made out. Others did not support the inclusion of a list.

### *The listing of activities that are privacy invasive*

- 3.9. Some models suggested that there should be examples of activities that could be considered as privacy invasive, to provide some guidance. As noted above, the ALRC has provided some examples of what could constitute privacy invasive activities.

### *The approach taken to balancing competing public interests and to consent*

- 3.10. Most models built the consideration of competing public interests into the threshold of actionability. This took the form of a balancing test in which the claimant's privacy was weighed against other relevant public interests. Other models considered that the public interest should be considered as a defence, rather than a component of the threshold.
- 3.11. Consent was considered as a part of the elements of a cause of action in some models, while other models suggested that consent should be considered a defence.
- 3.12. These issues are relevant in determining where the burden of proof should lie.

### *Defences*

- 3.13. Defences that have been proposed across all the models are:
- required or authorised by law
  - lawful defence of person or property
  - publication of information could be subject to privilege under defamation law.
- 3.14. A range of other defences have been canvassed by the different models.

### *Remedies*

- 3.15. Remedies that have been proposed across all the models are:
- compensatory damages
  - injunctions
  - declarations.
- 3.16. A number of other remedies have been proposed by the different models.

### *Limitation period*

- 3.17. The models proposed varying limitation periods of between one to three years from the date of the defendant's conduct.

### *Regulatory mechanisms*

- 3.18. The models proposed a variety of different regulatory mechanisms for administering the cause of action. These ranged from the Commonwealth Privacy Commissioner, to administrative

tribunals and State, Territory and Commonwealth courts. I discuss the possible application in NSW below.

### ***The NSW Privacy Commissioner's role in a statutory cause of action***

- 3.19. I note the ALRC's 2014 report recommended that the Commonwealth Privacy Commissioner's existing power to investigate complaints be extended to encapsulate complaints about serious invasions of privacy more generally<sup>23</sup>. The rationale was that this would provide a low-cost option for individuals to make complaints about serious invasions of privacy<sup>24</sup>.
- 3.20. The OAIC submission to the ALRC's report asserted that under the complaints model, the OAIC would act as the first entry point for initial complaints to be made<sup>25</sup>. The courts would have two roles – first, where the OAIC refers a question of law to the courts; second, where the OAIC is satisfied the complaint involves an issue of public importance requiring the consideration of the Federal Court or Federal Circuit Court.
- 3.21. This would have the benefit of encouraging fast, informal and low-cost resolution of disputes through conciliation, and building on the existing model of the Privacy Act<sup>26</sup>. Individuals would also have access to the OAIC's existing complaints and conciliation processes and expertise<sup>27</sup>. The OAIC's submission also emphasised that the model would only be successful if it was adequately funded<sup>28</sup>.
- 3.22. This is a sensible rationale and I support a similar extension of the complaints functions of the NSW Privacy Commissioner. Consideration could be given to amending the PPIP Act to enable this extension to occur, and which tribunal or court in NSW could serve a similar function as that proposed for the Federal Court or Federal Circuit Court.
- 3.23. For this model to be effective in NSW, this extension should be accompanied with further determinative powers for the NSW Privacy Commissioner.
- 3.24. Any extension of the functions of the Privacy Commissioner would require appropriate structural and organisational arrangements and additional resources. Discussion of reforms should be accompanied by careful consideration by the Committee of how best to resource these privacy functions.

### ***Potential criteria for assessing a model***

- 3.25. The elements of a model for a statutory cause of action could be combined in various ways, as demonstrated above. To assist the Committee in its assessment of what would work best in NSW, the following criteria are proposed:
- The need to complement the existing NSW privacy legal framework and add to the coherence of that legal framework.
  - The need to recognise the importance of protecting the information privacy and physical privacy of individuals, including from surveillance.
  - The need for any mechanism to be technology and forum neutral, flexible enough to accommodate a broad range of circumstances and be adaptable to changing technologies and practices<sup>29</sup>.
  - The capability of a statutory cause of action to take into account changing community expectations, values, norms and concerns<sup>30</sup>.
  - The importance of balancing the interest of individuals in their own privacy against other important public interests. For example, any proposal should seek to strike an appropriate

<sup>23</sup> ALRC 2014 report, recommendation 16 at page 310.

<sup>24</sup> Ibid, page 310.

<sup>25</sup> Submission by the Office of the Australian Information Commissioner (OAIC) to the ALRC, Serious Invasions of Privacy in the Digital Era, November 2013, which can be accessed at [http://www.oaic.gov.au/images/documents/news-and-events/submissions/privacy-submissions/OAIC\\_submission\\_to\\_ALRC\\_Serious\\_invasions\\_of\\_privacy\\_in\\_the\\_digital\\_era.pdf](http://www.oaic.gov.au/images/documents/news-and-events/submissions/privacy-submissions/OAIC_submission_to_ALRC_Serious_invasions_of_privacy_in_the_digital_era.pdf)

<sup>26</sup> Ibid, page 6.

<sup>27</sup> Ibid.

<sup>28</sup> Ibid.

<sup>29</sup> Ibid.

<sup>30</sup> NSWLRC 2008 report, pages 26-29; VLRC 2010 report, page 136.

balance between the use and disclosure of information, protecting personal privacy and freedom of expression<sup>31</sup>.

- The right to seek a remedy, as per the ICCPR, and be able to have access to taking the action. The action should be user-friendly, non-adversarial, and have minimal cost and formality to make the cause of action accessible to the average person<sup>32</sup>. The NCAT is an example of a forum that could meet these criteria.
- The flexibility to deal with varying individual circumstances.
- The ability to limit the making of unmeritorious claims.
- Consideration of whether a cause of action should be limited to natural persons only, consistent with the approach taken under the PPIP Act and HRIP Act. The privacy of a deceased person remains protected under the PPIP Act and HRIP Act, which protects the personal information of a deceased person for up to 30 years<sup>33</sup>.
- Consideration of whether third parties should be able to take an action, for example, in a situation where a group of individuals experience an invasion of privacy.
- Consideration of whether a period should be set after which the statutory cause of action is reviewed to determine how effectively it has been operating.

## 4. Implications for NSW privacy regime

### Addressing gaps in the current regime

4.1. The gaps in the NSW legislative framework and the limitations of common law redress outlined above are relevant for the Committee's assessment of the adequacy of existing remedies for serious invasions of privacy. In particular, a statutory cause of action could address the gaps and limitations outlined above by potentially providing an option for redress:

- for some conduct of NSW public sector agencies that could otherwise rely on an exemption in the PPIP Act or HRIP Act
- against individuals or entities that do not fall under the coverage of the PPIP Act or HRIP Act
- for conduct that involves spatial or physical matters, that is, other than personal information.

4.2. If it is decided that a statutory cause of action should not be pursued, these gaps in existing privacy protections in NSW need to be addressed and I refer the Committee to my report to Parliament.

### Extending the application of current NSW privacy legislation

4.3. An alternative to developing a statutory action is assessing the feasibility of possible amendments to the PPIP Act and HRIP Act to extend their application. The NSWLRC has issued several reports about reforms to the PPIP Act and HRIP Act. Some possible ideas could include:

- Re-considering the coverage of the PPIP Act in terms of entities and types of privacy. While the PPIP Act and HRIP Act have been designed to be technology neutral, there is scope for new areas of privacy protection in NSW. For example, intrusion upon seclusion could be a new area of coverage to address both spatial and physical privacy. This could include intruding on someone's solitude or invading their private space, and would not need to result in the publication of information<sup>34</sup>.
- Evaluating the continued relevance of the broad exemptions that have been provided in the PPIP Act and HRIP Act.
- Evaluating the existing Information Protection Principles (IPPs) in the PPIP Act and Health Privacy Principles (HPPs) in the HRIP Act to see whether these could be strengthened, for example, should an individual be able to request to delete or destroy their personal information which is no longer going to be used.

<sup>31</sup> ALRC 2014 report, chapter 9.

<sup>32</sup> Submission by the Queensland Office of the Information Commissioner to the ALRC Issues Paper, Serious Invasions of Privacy in the Digital Era, November 2013, page 2.

<sup>33</sup> See section 4, PPIP Act and section 5, HRIP Act.

<sup>34</sup> VLRC 2010 report, page 134.

- Assessing whether principles of anonymity and pseudonymity should be included in the PPIP Act, as in the HRIP Act and Commonwealth privacy legislation.
- Assessing the adequacy of the avenues of redress, remedies and penalties associated with breaches of the IPPs and HPPs.
- Considering whether the NSW Privacy Commissioner should be provided with additional powers that are determinative in nature.
- Considering whether agencies should be required to comply with the recommendations of the Privacy Commissioner following a conciliation process, and whether a right of appeal to NCAT should be provided in relation to findings and recommendations by the Privacy Commissioner in relation to conciliations<sup>35</sup>.
- Assessing the role of NCAT as a low cost avenue for dealing with serious invasions of privacy.
- Examining how the PPIP Act and HRIP Act interact with other NSW legislation relevant to privacy.

## 5. Conclusion

5.1 I support the development of a statutory cause of action for serious invasions of privacy, for the following reasons:

- The current NSW legislative framework relevant to privacy has gaps in its coverage.
- The common law may evolve too slowly, while alternative common law causes of action provide limited redress to individuals alleging invasions of privacy. This option may also be cost prohibitive for individuals.
- There are no direct, readily accessible remedies to deal with interferences with spatial or physical privacy, or with interferences with personal information by other individuals.
- A statutory cause of action would create rights that have not been recognised in Australia, including in NSW.
- Using a statutory approach provides the opportunity to carefully target and shape a cause of action, and take into account competing public interests.
- A statutory cause of action would have real benefits for individuals who have or are experiencing serious invasions into their privacy that cannot seek redress under the current regime.
- A statutory cause of action would provide certainty by creating an action in civil law that individuals could pursue to protect their privacy.

5.2 The advantages of a statutory approach to privacy protection were outlined in a submission by the previous NSW Deputy Privacy Commissioner in 2011<sup>36</sup>.

5.3 First, a statutory privacy regime has a deterrent effect and gives a degree of certainty to the expectation of privacy in individuals whose personal information is subject to protection under those laws.

5.4 Second, it could provide a simple, low cost option for individuals to bring complaints to the Privacy Commissioner and to seek damages for proven breaches. Litigation through courts could be costly and limit the ability of a large section of the public from seeking redress. Third, a statutory approach would help ensure consistency of approach in the application of privacy law. Finally, it would lessen the publicising of any interference of privacy.

## 6. Attachments

**Attachment A:**      **Background to the *Privacy and Personal Information Protection Act 1998***  
 Extract from my 2015 report to Parliament, '*Report of the Privacy Commissioner under Section 61B of the Privacy and Personal Information Protection Act*'.

<sup>35</sup> Recommendation 32 of the Privacy Commissioner's 2015 report to Parliament.

<sup>36</sup> The submission can be found on the IPC website at [http://www.ipc.nsw.gov.au/sites/default/files/file\\_manager/submission\\_on\\_the\\_issues\\_paper\\_a\\_commonwealth.pdf](http://www.ipc.nsw.gov.au/sites/default/files/file_manager/submission_on_the_issues_paper_a_commonwealth.pdf)

**Attachment B: Overview of the NSW Privacy Regime**

An overview of the NSW privacy regime, the current opportunities for redress provided by NSW privacy legislation and the consolidated list of recommendations from my 2015 report to Parliament.

**Attachment C: Privacy issues identified by the public**

Examples of privacy issues identified by the public that featured in my 2015 report to Parliament.

**Attachment D: Overview of models proposed by Australian jurisdictions**

Table containing a summary of the key elements and issues of the models proposed by the NSWLRC, ALRC and VLRC for a statutory cause of action.

## Background to the *Privacy and Personal Information Protection Act 1998*

### **The Privacy Committee Act 1975**

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

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

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

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

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

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

### **The Privacy and Personal Information Protection Act 1998**

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

He observed that information technology made records of personal information more vulnerable to abuse as it

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

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

The Attorney noted that government is one of the main collectors and users of personal information and that effective safeguards are a vital part of government’s compact with the community. The Attorney General reminded the Parliament that the need to provide for safeguards in relation to the release of personal information held by NSW government

agencies was highlighted in the ICAC's 1992 "Report into the Unauthorised Release of Government Information". That inquiry revealed an illicit trade in personal information involving government departments, the police, lawyers, financial institutions and private investigators. As well as drawing attention to the corrupt conduct involved in this trade, ICAC was very critical of the lack of any coordinated and consistent government policy dealing with the storage and release of information.

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

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

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

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

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

## Overview of the NSW privacy regime

### The role of the NSW Privacy Commissioner

The role of the NSW Privacy Commissioner recognises the importance of the privacy rights of the people of NSW with respect to both their personal and health information. It is an acknowledgement that NSW citizens need an independent voice to oversee the protection of their privacy.

Section 36 of the PPIP Act enables me to, for example, promote privacy, publish guidelines, conduct research or inquiries, receive, investigate and conciliate complaints, provide advice on any privacy matters generally, make public statements about any matter relating to the privacy of individuals, and prepare reports recommending legislative, administrative or other action in the interests of privacy. This section also allows me to take up broader privacy issues which may arise in the community outside of the NSW public sector, for example, to examine the issue of drone surveillance. The Privacy Commissioner also has powers equivalent to a Royal Commission to require any person or public sector agency to give information. However, the Privacy Commissioner cannot make determinations.

I report to the NSW Parliament and am oversighted by the Parliamentary Committee on the Ombudsman, the Police Integrity Commission and the Crime Commission.

### The NSW privacy legislative regime

The NSW privacy regime consists of two primary pieces of legislation—the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act). The Acts set out the NSW privacy framework and my role as Privacy Commissioner. As beneficial legislation, the NSW privacy regime places NSW citizens at the centre to ensure that NSW public sector agencies and organisations act lawfully and protect citizen privacy.

The PPIP Act and HRIP Act set out the obligations of NSW public sector agencies and other organisations to protect and manage personal and health information in accordance with the NSW privacy legislative regime. The Acts contain mechanisms that help ensure the appropriate and legitimate collection, use, disclosure and accessibility of personal information by a NSW public sector agency or private health provider. The existence of these Acts is testament to the support that privacy protection has had from both sides of politics, under the Lewis and Willis government in 1975 and the Carr government in 1998.

The objective of the NSW privacy regime is to give citizens confidence that NSW public sector agencies manage their personal and health information appropriately in all circumstances. The structure and approach of this regime is broadly similar to that in other jurisdictions, including the Commonwealth privacy regime.

The PPIP Act regulates the way in which all NSW public sector agencies (NSW government departments and agencies, statutory authorities, universities, local councils and other bodies whose accounts are subject to the Auditor General) collect, use, access, store, dispose of, and disclose personal information of members of the public. These obligations are set out as Information Protection Principles (IPPs) in the PPIP Act. The PPIP Act can also apply to private sector or non-government organisations (NGOs) if they are contractually required to comply with the privacy regime by a NSW public sector agency. As the Standing Committee is no doubt aware, there is a growing role for NGO providers in the provision of human services.

The HRIP Act outlines how NSW public sector agencies, health service providers and certain other organisations should handle the health information of members of the public. Similar to the IPPs, the Health Privacy Principles (HPPs) within the HRIP Act set out how health information must be collected, used, accessed, stored, disposed of and disclosed.

These statutes can be complemented by other instruments, such as Codes of Practice and Public Interest Directions, to enable a flexible, context specific response to the needs of agencies, communities and individuals. One of the benefits of a principles-based and technological neutral privacy regime is that it can be flexibly adapted to the circumstances. This is particularly important given the rapid change in technology which allows the collection, analysis and sharing of information in ways previously unimaginable.

As can be seen, the PPIP Act and the HRIP Act provide a flexible, principles-based regime to protect the privacy of NSW citizens in relation to the conduct of NSW public sector agencies. The privacy principles (and privacy modifications and exemptions allowed in the legislation) can provide a robust privacy framework in which an agency initiative, program or project can operate within.

### Avenues for redress

The PPIP Act and HRIP Act provide individuals with the right to seek a review in situations where they believe that a public sector agency has mishandled their personal information. These review pathways provide avenues of redress to individuals whose privacy has been breached by public sector agencies, and private sector entities under the HRIP Act.

The IPC has issued guidance on how the Privacy Commissioner handles privacy complaints, which I attach for the Committee's information.

#### Public sector agencies under the PPIP Act

Part 5 of the PPIP Act outlines the requirements and process for reviews of public sector agencies' conduct.

An individual is entitled to an internal review by an NSW public sector agency if they are aggrieved about the agency's conduct in relation to their personal information. While the agency must conduct the internal review, the Privacy Commissioner must be notified and may also make submissions to the agency about the matter.

If an individual is not satisfied by the findings of the internal review or the action taken by the agency as a result of the review, they have the right to seek an external review by the NSW Civil and Administrative Tribunal (NCAT). The PPIP Act sets out what orders NCAT may make to remedy the agency's conduct. NCAT may make the following decisions (section 55(2), PPIP Act):

- not to take any action
- award compensation (damages) of up to \$40,000 for any financial loss, or psychological or physical harm, because of the conduct of the agency or body
- require the agency or body to stop any conduct or action which contravenes an IPP or a HPP
- order the performance of an IPP or a HPP by the agency
- order the agency to take specified steps to remedy any loss or damage suffered by the individual
- order the agency to correct personal information that has been disclosed.

The Privacy Commissioner may appear and make submissions at Tribunal hearings.

Individuals also have the right to make complaints to the Privacy Commissioner about alleged violations of or interferences with their own privacy under the PPIP Act. The Privacy Commissioner may investigate, inquire, conciliate and hold hearings with the parties to the complaint as part of the conciliation process. Under the PPIP Act, the Privacy Commissioner must endeavor to resolve all complaints by conciliation. The Privacy Commissioner cannot make orders or award damages at the conclusion of conciliation. The Privacy Commissioner also cannot take further action after the conclusion of proceedings, whether or not the parties have reached an agreement. In addition, there is no right of review to NCAT if the Privacy Commissioner conducts an investigation into a complaint and makes a decision.

Lastly, sections 62 and 63 of the PPIP Act set out penalties for public sector officials that engage in corrupt disclosure and use of personal information or offer to supply personal information that has been disclosed unlawfully.

#### Public sector agencies under the HRIP Act

Under the HRIP Act, an individual is also entitled to an internal review by an NSW public sector agency if they are aggrieved about the agency's conduct in relation to their personal information, and external review by NCAT. The requirements outlined in Part 5 of the PPIP Act also apply to reviews under the HRIP Act (section 21, HRIP Act).

#### Private sector entities under the HRIP Act

Individuals have the right to make a complaint to the Privacy Commissioner about alleged breaches by a private sector person of the HRIP Act. The Commonwealth *Privacy Act 1988* can also apply to private sector health service providers. In situations where this occurs, individuals can choose to make the complaint to the Commonwealth Privacy Commissioner. If the individual elects for the NSW Privacy Commissioner to investigate their complaint, the complaint cannot be subsequently dealt with by Commonwealth Privacy Commissioner, and vice versa.

The process for dealing with complaints against a private sector entity under the HRIP Act varies slightly to that under the PPIP Act. The Privacy Commissioner may investigate, inquire, conciliate and hold hearings with the parties to the complaint as part of the conciliation process. The Privacy Commissioner must endeavor to resolve all complaints by conciliation.

Complainants cannot usually ask NCAT to conduct a further review of the complaint if the person is unhappy with the outcome of the Privacy Commissioner's investigation. However, the HRIP Act provides that the Privacy Commissioner may prepare a report as a result of a complaint about an alleged breach of a HPP by a private sector entity (section 47, HRIP Act). If an individual is dissatisfied by the outcome of the Privacy

Commissioner's report or the actions taken by the entity in response to the findings in the report the Applicant may apply to NCAT for an inquiry.

## **Report of the Privacy Commissioner under Section 61B of the *Privacy and Personal Information Act 1998* - Consolidated list of recommendations**

### **Definition of personal information**

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

### **Coverage of the PPIP Act – State Owned Corporations**

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

### **Contracted services and contractors**

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

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

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

### **Privacy by design**

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

### **Anonymity and pseudonymity**

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

### **Notification of privacy breaches**

- 10) The PPIP Act be amended to provide for mandatory notification of serious breaches of an individual's privacy by a public sector agency similar to that proposed to be provided in the Privacy Act 1988 (Cth).
- 11) The Annual Reports Act and related Regulations be amended to require reporting of serious breaches and actions taken to address the breaches.

### **Accessing personal information**

- 12) Access to and amendment of personal information be governed solely by the PPIP Act and that access to non-personal information (Government information) be governed by the GIPA Act.
- 13) Consideration be given to amending the PPIP Act section 10 (f) to reflect changes in technology for collecting and storing personal information and changes in service provision models.

### **Interjurisdictional or transborder disclosure**

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

### **Exemptions for research purposes**

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

### **Structure of the PPIP Act**

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

### **Public sector capability in privacy and information management**

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

#### Information technology security

- 18) ISO/IEC 27018 standard covering privacy, security and cloud services be considered for inclusion in the NSW Government's Information Security Management Systems Policy.
- 19) The Privacy Commissioner in conjunction with the Office of Finance and Services develop model clauses for inclusion in cloud computing contracts to ensure the protection of privacy and personal information, covering the collection, custody and ownership, use, storage, access to, disclosure and sharing of the information, business continuity, data disposal and exit strategy.
- 20) Agencies include periodic audits of the implementation of the NSW Government Cloud Services Policy in their audit and risk plans.
- 21) The Auditor General conduct a post-implementation review of the NSW Government Cloud Services Policy within two years of the date of commencement of the policy in which privacy management and compliance is a component of the review.

#### 'Big data'

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

#### Surveillance

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

#### Firearm regulation and risks to individual privacy and public safety

- 24) The NSW Police Force review the processes and systems relating to the register of firearm ammunition purchases to ensure compliance with legislation relating to the register while ensuring the protection of the privacy and personal information of purchasers.
- 25) The Privacy Commissioner to raise with the NSW Auditor General the inclusion of this matter in the forward performance audit program of the Audit Office.

#### Public sector agency accountability for privacy management

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

#### Changing nature of Government and service provision

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

#### Consent

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

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

- 29) The Privacy Commissioner in conjunction with relevant agencies, establish a project to identify and investigate methodologies that enable the safe use of personal information in de-identified, aggregated and linked data sets so as to protect the privacy and personal information of individuals.
- 30) The appropriateness of a Code of Practice to enable information sharing for planning and policy analysis purposes between agencies be examined and developed if such a need is demonstrated.

#### Exchange of information for child protection purposes

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

#### Privacy Commissioner's conciliation of complaints

- 32) The PPIP Act be amended to:
  - a. require agency compliance with the recommendations of the Privacy Commissioner arising from the conciliation of a complaint to the Commissioner
  - b. provide for the right of appeal to NCAT in relation to findings and recommendations of the Privacy Commissioner in respect of the conciliation of a complaint
  - c. remove the restriction in section 46(7) of the HRIP Act on the Privacy Commissioner taking any further action as a result of conciliation proceedings.

#### Internal reviews

- 33) The PPIP Act be amended to:
  - a. clarify that 'representative' claims can be the subject of the internal review process and review by NCAT, and
  - b. allow agencies to be able to outsource their undertaking of the internal review.

**Time frames applying to oversight of internal reviews**

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

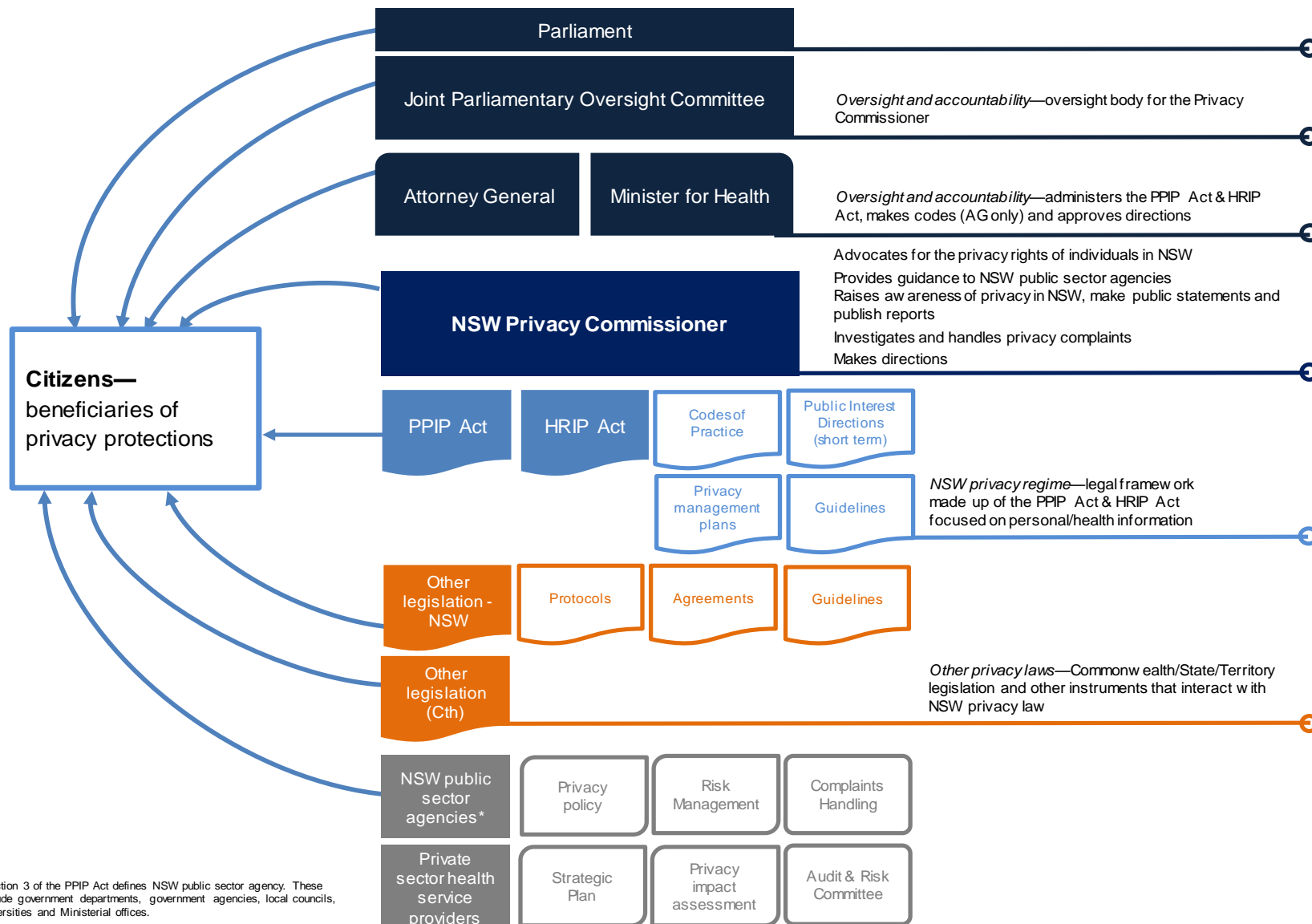
**Treatment of excluded information**

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

**Resourcing support**

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

## Current Privacy Protections in NSW



\*Section 3 of the PPIP Act defines NSW public sector agency. These include government departments, government agencies, local councils, universities and Ministerial offices.

## **Privacy issues identified by the public**

This section provides some examples of privacy issues identified by the public that features in my 2015 report to Parliament, *'Report of the Privacy Commissioner under Section 61B of the Privacy and Personal Information Protection Act'*.

### **Consent for the provision, use and sharing of personal information**

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

### **Specific initiatives and technologies**

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

### **Surveillance**

- "The potential proliferation of drones (in the future) by persons for no good purpose other than to stalk and harass private citizens i.e. invasion of one's personal space."
- "The impact on the psychology of people who are born into a society that surveils all its citizens does not seem like a healthy direction..."

### **Big data and data mining**

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

### **Vulnerability of certain groups**

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

## Overview of models proposed by Australian jurisdictions

The table below contains a summary of the key elements and issues of the models proposed by the NSWLRC, ALRC and VLRC for a statutory cause of action.

	NSWLRC in 2008 report	ALRC in 2008 report	ALRC in 2014 report	VLRC in 2010 report
<b>Scope</b>	<p>Broad – could cover any circumstance.</p> <p>Proposes a statutory cause of action, not a statutory tort.</p> <p>Should be a uniform approach for all jurisdictions and created by each State/Territory legislation; in NSW, a statutory cause of action would be housed in the <i>Civil Liabilities Act 2002</i>.</p>	<p>Broad – could cover any circumstance.</p> <p>Proposes a statutory cause of action, not a statutory tort.</p> <p>Enacted in Commonwealth legislation separate to the Privacy Act.</p>	<p>Narrow – proposes one statutory cause of action covering two broad types:</p> <ul style="list-style-type: none"> <li>• Intrusion upon seclusion</li> <li>• Misuse of private information.</li> </ul> <p>Proposes a statutory cause of action that is a tort.</p> <p>Should be enabled in Commonwealth legislation that is separate to the Privacy Act.</p>	<p>Narrow – proposes two statutory causes of action for misuse of surveillance in a public place, that are actual or threatened:</p> <ul style="list-style-type: none"> <li>• Intrusion upon seclusion</li> <li>• Misuse of private information.</li> </ul> <p>Proposes a statutory cause of action, not a tort.</p> <p>No express view – considered national harmonisation a long term goal; suggested Victoria take leadership on the issue.</p>
<b>Application</b>	<p>Natural persons.</p> <p>Does not allow action to survive death of a person.</p> <p>Allows action to be taken against estates of deceased persons.</p> <p>No exemptions.</p>	<p>Natural persons.</p> <p>Deceased persons – n/a</p> <p>Exemptions – n/a</p>	<p>Natural persons.</p> <p>Does not allow for action to be taken by or against the estate of a deceased person.</p> <p>Provides for one exemption – children and young persons.</p>	<p>Natural persons.</p> <p>Does not allow for action to be taken by deceased persons.</p> <p>No exemptions.</p>
<b>Threshold to make out a cause/elements</b>	<p>Objective test – conduct of another person invaded the privacy that the individual was reasonable entitled to expect in all the circumstances having regard to any relevant public interest (including the interest of the public in being informed about</p>	<p>Objective test – claimant must show a reasonable expectation of privacy in the circumstances, and the act or conduct complained of is highly offensive to a reasonable person of ordinary sensibilities.</p> <p>Fault element – intentional or</p>	<p>Objective test – a person in the position of the claimant would have had a reasonable expectation of privacy in all of the circumstances.</p> <p>Fault element – intentional or reckless invasions of privacy, and not negligence.</p> <p>Seriousness – yes; degree of any</p>	<p>Objective test – Elements of misuse of private information:</p> <ul style="list-style-type: none"> <li>• the defendant misused, by publication or otherwise, information about the plaintiff in respect of which the plaintiff had a reasonable expectation of privacy;</li> </ul>

	NSWLRC in 2008 report	ALRC in 2008 report	ALRC in 2014 report	VLRC in 2010 report
	<p>matters of public concern).</p> <p>Fault element – not required.</p> <p>Seriousness – not required.</p> <p>Proof of damage – not required.</p>	<p>reckless acts and not merely negligent.</p> <p>Seriousness element – yes.</p> <p>Proof of damage – not required.</p>	<p>offence, distress or harm to dignity that the invasion of privacy was likely to cause to a person of ordinary sensibilities in the position of the claimant, and whether the defendant was motivated by malice or knew the invasion of privacy was likely to offend, distress or harm the dignity of the claimant.</p> <p>Proof of damage – not required; considered when looking at remedies (invasion need not cause actual damage but focus on mental or emotional distress).</p>	<p>and</p> <ul style="list-style-type: none"> <li>a reasonable person would consider the defendant's misuse of that information highly offensive.</li> </ul> <p>Objective test – Elements of intrusion upon seclusion:</p> <ul style="list-style-type: none"> <li>the defendant intruded upon the seclusion of the plaintiff when the plaintiff had a reasonable expectation of privacy; and</li> <li>a reasonable person would consider the defendant's intrusion upon the plaintiff's seclusion highly offensive.</li> </ul> <p>Fault element – intentional, reckless or negligent acts.</p> <p>Seriousness – yes.</p> <p>Proof of damage – not required.</p>
<b>Consideration of other relevant matters in determining actionability</b>	Yes – provides a non-exhaustive list that a court must take into account when deciding if an invasion of privacy has occurred.	n/a	Yes – provides a non-exhaustive list that a court may take into account.	n/a
<b>Listing of activities that are privacy invasive</b>	Not required.	Yes – non-exhaustive list.	Yes – non-exhaustive list.	n/a
<b>Consideration of the public interest</b>	Built into the cause of action as an element to be made out – having regard to any relevant public interest (including the	Built into cause of action as an element to be made out – consider whether the public interest in maintaining the claimant's privacy	Built into the cause of action as an element to be made out – the public interest in privacy outweighs any	Considered as a defence.

	NSWLRC in 2008 report	ALRC in 2008 report	ALRC in 2014 report	VLRC in 2010 report
	interest of the public in being informed about matters of public concern).	outweighs other matters of public interest (including the interest of the public to be informed about matters of public concern and the public interest in allowing freedom of expression).	<p>countervailing public interest.</p> <p>Provides a list of countervailing public interest matters which a court may consider, along with any other relevant public interest matter:</p> <ul style="list-style-type: none"> <li>• freedom of expression, including political communication and artistic expression;</li> <li>• freedom of the media, particularly to responsibly investigate and report matters of public concern and importance;</li> <li>• the proper administration of government;</li> <li>• open justice;</li> <li>• public health and safety;</li> <li>• national security; and</li> <li>• the prevention and detection of crime and fraud.</li> </ul>	
<b>Consent</b>	Considered as part of elements of cause of action – an action is not made out if the individual or another person with lawful authority for the individual, expressly or impliedly consented to the conduct.	Considered as part of elements of cause of action.	Considered as a defence.	Considered as a defence.
<b>Defences</b>	Required or authorised by law. Lawful defence of person/property.	Act/conduct is incidental to the exercise of a lawful right of defence of person/property. Act/conduct is required or	Conduct was required or authorised by law. Conduct was incidental to the exercise of a lawful right of defence of	Defences for misuse of private information: <ul style="list-style-type: none"> <li>• Consent to the use of information</li> </ul>

	NSWLRC in 2008 report	ALRC in 2008 report	ALRC in 2014 report	VLRC in 2010 report
	<p>Publication of matter that would attract certain defamation defences.</p> <p>Publication of information as an employee or agent of a subordinate distributor, and the defendant did not or could not reasonably know that publication constituted an invasion of privacy.</p> <p>Publication of information where, as between the defendant and recipient of information, there is a common interest or duty in giving and receiving information on the subject in question; this defence is defeated if the claimant proves that the publication of information was actuated by malice.</p>	<p>authorised by or under law.</p> <p>Publication of information is subject to privilege under the law of defamation.</p>	<p>persons/property where that conduct was proportionate, necessary and reasonable.</p> <p>Defence of necessity.</p> <p>Defence of consent.</p> <p>Defence of absolute privilege.</p> <p>Defence of publication of public documents.</p> <p>Defence of fair report of proceedings of public concern.</p>	<ul style="list-style-type: none"> <li>• Act or conduct is incidental to the exercise of a lawful right of defence of person/property, and was reasonable and proportionate response to the threatened harm</li> <li>• Activity was required or authorised by or under law</li> <li>• Defendant is a police or public officer engaged in duty and their conduct was not disproportionate to the matter being investigated nor committed in the course of a trespass</li> <li>• Publication of private information was privileged or fair comment (can be defeated if malice is proved)</li> <li>• Defendant's conduct was in the public interest, where public interest is a limited concept and not any matter the public may be interested in.</li> </ul> <p>Defences for intrusion upon seclusion:</p> <ul style="list-style-type: none"> <li>• Consent to the conduct</li> <li>• Act or conduct is incidental to the exercise of a lawful right of defence of person/property, and was reasonable and proportionate response to the threatened harm</li> <li>• Activity was required or authorised by or under law</li> <li>• Defendant is a police or public</li> </ul>

	NSWLRC in 2008 report	ALRC in 2008 report	ALRC in 2014 report	VLRC in 2010 report
				<p>officer engaged in duty and their conduct was not disproportionate to the matter being investigated nor committed in the course of a trespass</p> <ul style="list-style-type: none"> <li>Defendant's conduct was in the public interest, where public interest is a limited concept and not any matter the public may be interested in.</li> </ul>
<b>Remedies</b>	<p>Range of statutory remedies, including compensatory damages, injunctive style prohibitory orders, orders of a declaratory nature, and orders for delivery up and destruction of material.</p> <p>Exemplary or punitive damages are excluded.</p> <p>Damages for non-economic loss are limited to a maximum of \$150,000, adjusted annually.</p>	<p>Access to wide range of remedies, including ordinary and aggravated damages, account of profits, injunction, order to apologise, correction order, order for delivery up and destruction of material and a declaration.</p> <p>Exemplary damages are excluded.</p> <p>No limitation to amount of damages.</p>	<p>Damages (including for emotional distress; a non-exhaustive list is provided of aggravating and mitigating factors for courts to consider in determining amount of damages), account of profits, interlocutory order or injunction, delivery up, destruction and removal of material, order for publication of correction, order to apologise, and a declaration.</p> <p>Exemplary damages are allowed in exceptional circumstances.</p> <p>Cap for damages set at a sum of damages for economic loss and any exemplary damages. The cap should not exceed the cap on non-economic loss in defamation law.</p>	<p>Compensatory damages, injunctions and declarations.</p> <p>Exemplary damages are excluded.</p> <p>No statutory cap on amount of damages.</p> <p>Costs administered according to rules set out in VCAT Act.</p>
<b>Limitation period</b>	<p>One year, running from the date of the defendant's conduct, which can be extended for up to three years.</p>	n/a	<p>One year from the date on which the claimant became aware of the invasion of privacy, or three years from the date on which the invasion occurred, whichever is earlier.</p>	<p>Three years running from the date on which the cause of action occurred.</p>
<b>Regulatory</b>	Commonwealth, state or territory	Appropriate court to hear the action	Federal, state and territory courts all	VCAT to have sole jurisdiction.

	NSWLRC in 2008 report	ALRC in 2008 report	ALRC in 2014 report	VLRC in 2010 report
<b>mechanisms</b>	courts ( <i>note: this is implied in the report</i> )	will depend on the circumstance giving rise to the liability. As such, could encompass federal courts, state courts, district and county courts.	<p>retain jurisdiction to hear an action.</p> <p>Consideration to be given to give jurisdiction to appropriate State and Territory tribunals.</p> <p>Commonwealth Privacy Commissioner to be amicus curiae and to intervene in court proceedings, with leave of the court.</p> <p>Consider extending Commonwealth Privacy Commissioner's complaints powers to enable investigation of complaints about serious invasions of privacy and to make appropriate declarations.</p>	