Submission No 25

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

Organisation: NSW Young Lawyers
Communications, Entertainment & Technology Committee

Date received: 23/09/2015

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

Communications, Entertainment & Technology Committee

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

11 September 2015

Submission to the Standing Committee on Law and Justice of the Legislative Council of the Parliament of New South Wales

Mrs Natasha Maclaren-Jones MLC, Committee Chair
Standing Committee on Law and Justice
Parliament House
6 Macquarie Street
Sydney NSW 2000

Contact:

Elias Yamine
President, NSW Young Lawyers

Chris Chow
Chair, NSW Young Lawyers Communications, Entertainment & Technology Law Committee

Editors:

James Skelton and Angela George
Submissions Coordinators, NSW Young Lawyers Communications, Entertainment & Technology Law Committee

Contributors:

Maeve Curry, Jayne Hardy, Saba Amir Goudarzi, Melissa Lui, Mahmoud Mando, Ruthushan Muttasamy, Jessica Norgard, Theodore Souris, Isabella Street, Jessica Wong and Daniel Zwi

NSW Young Lawyers
Communications, Entertainment & Technology Law Committee
170 Phillip Street
Sydney NSW 2000
ylgeneral@lawsociety.com.au
www.younglawyers.com.au

The NSW Young Lawyers Communications, Entertainment & Technology Law Committee (**Committee**) makes the following submission in response to the Inquiry into remedies for the serious invasion of privacy in New South Wales (**Inquiry**).

NSW Young Lawyers

NSW Young Lawyers is a division of the Law Society of New South Wales. NSW Young Lawyers supports practitioners in their professional and career development in numerous ways, including by encouraging active participation in its 16 separate committees, each dedicated to particular areas of practice. Membership is automatic for all NSW lawyers under 36 years and/or in their first five years of practice, as well as law students. NSW Young Lawyers currently has over 15,000 members.

The Committee aims to serve the interests of lawyers, law students and other members of the community concerned with areas of law relating to information and communication technology (including technology affecting legal practice); intellectual property; advertising and consumer protection; confidential information and privacy; entertainment; and the media. As innovation inevitably challenges custom, the Committee promotes forward thinking, particularly about the shape of the law and the legal profession as a whole.

Summary of Recommendations

The Committee has considered the call for submissions from the Inquiry and, noting its previous submission to the Australian Law Reform Commission in 2013, submits that:

1. an equitable action for breach of confidence is not completely effective at addressing serious invasions of privacy due to the great level of uncertainty surrounding the tort;
2. the uncertainty surrounding the role and practical powers of the Office of the Australian Information Commissioner (OAIC), including its long term future, raises concerns in respect of protecting privacy;
3. there would be significant value placing greater emphasis on establishing an effective deterrence against cyber-harassment;
4. the Inquiry should take note of international experiences in the area, including recent advances in case law in New Zealand, that address publicising personal information and the intrusion upon seclusion;
5. consideration should be given to the circumstances in which any statutory cause of action should impose liability;
6. a statutory cause of action only be available to natural and living persons; and
7. proof of damage under a statutory cause of action be extended to include emotional distress and humiliation.

The Committee sets out its discussion of these key issues in the following sections.

1. The adequacy of the equitable action of breach of confidence in respect of serious invasions of privacy

The equitable action of breach of confidence has developed in a way that means it has been used to protect against some instances of serious invasions of privacy. Despite this, the Committee submits that there remain three key factors which render the equitable action of breach of confidence inadequate to protect against serious invasions of privacy:

1. uncertainty surrounding the necessary obligation of confidence;
2. the limited remedies available to victims of serious invasions of privacy; and
3. the gaps that may exist due to the distinction between the concepts of confidence and privacy.

While breach of confidence may, in some circumstances, be effective in addressing serious invasions of privacy there is still a great level of uncertainty as to its successful application to all serious invasions of privacy, and the adequacy of the remedies available.

1.1 Uncertainty surrounding the necessary obligation of confidence

The equitable action of breach of confidence requires that:[1]

1. the information must have the necessary quality of confidence about it;
2. the information must have been imparted in circumstances importing an obligation of confidence; and
3. there must be an unauthorised use of that information to the detriment of the party communicating it.

While typically thought of as a means of protecting commercial information or trade secrets, breach of confidence has been used successfully to protect the personal information of individuals. Rather than a commercial or contractual relationship, the courts have found that an obligation of confidence (the second element of the cause of action) can be owed by individuals in a marital or de facto relationship.[2]

In the United Kingdom, judges have gone further, opining that a 'duty of confidence' can be owed whenever a person 'receives information he knows or ought to know is fairly and

---

[1] *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41, 47.

[2] Argyll v Argyll [1967] Ch 302; *Giller v Procopets* (2008) 24 VR 1; [2008] VSCA 236.

reasonably to be regarded as confidential'.[3] This relaxes the second element of the cause of action, meaning that a pre-existing relationship is no longer necessary to found an action for breach of confidence.

The position in Australia is less clear. There remains uncertainty around how strictly the second element of the cause of action would be applied. Although Gleeson CJ in *ABC v Lenah Games Meats* considered that 'equity may impose obligations of confidentiality even though there is no imparting of information in circumstances of trust and confidence',[4] the circumstances in which equity may impose such an obligation are not sufficiently clear. Some of the most serious invasions of privacy, including the taking of intimate photographs, could foreseeably involve no pre-existing relationship. Therefore, this uncertainty around the second element of the cause of action limits the protection available because:

1. it does not give a potential plaintiff sufficient clarity that they could seek to use the cause of action to protect their privacy; and
2. it does not signal to potential perpetrators of invasions of privacy that their behaviour may give rise to action against them.

A clear standard is desirable in this respect to resolve potential uncertainty for victims and to set standards of behaviour for all individuals.

1.2 Limited remedies available to victims of serious invasions of privacy

As an equitable cause of action, equitable remedies are available for breach of confidence including: injunctions (e.g. to prevent publication); an account of profits; and equitable compensation.

An injunction is likely to be most useful to a potential plaintiff for an anticipated invasion of privacy. The key limitation of breach of confidence is the remedies which will be available to deal with invasions of privacy after they have occurred. An account of profits focuses on the profits the defendant has made as a result of their breach of confidence, and compensation for breach of confidence has usually been limited to economic loss. It is only relatively recently that courts in Australia have recognised that distress and embarrassment caused by a breach of confidence can be compensated in equity.

For example, in *Wilson v Ferguson* [2015] WASC 15 the Supreme Court of Western Australia considered a case that involved:

1. intimate and explicit photos and videos which had the necessary quality of confidence about them;

---

[3] *Campbell v Mirror Group Newspapers Ltd* [2004] 2 AC 457 at 464-5.

[4] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 at [34].

2. the plaintiff and defendant were in a romantic relationship and such a relationship generally carries with it some obligation of confidence as to private matters;
3. the defendant obtained some of the images and videos of the plaintiff by using her phone and emailing copies to himself without her knowledge or consent;
4. the plaintiff then later expressly informed the defendant of their confidential nature; and
5. the defendant deliberately shared these photos on Facebook to cause embarrassment and distress to her in response to the ending of their relationship.

Justice Mitchell agreed with the Victorian Court of Appeal in *Giller v Procopets* that the equitable doctrine of breach of confidence should be developed by providing monetary compensation for embarrassment and distress caused by the disclosure of private and personal information. Justice Mitchell awarded the plaintiff equitable compensation for the significant embarrassment, anxiety and distress she had suffered as a result of the dissemination of intimate images.[5] The award of $35,000 in equitable compensation took into account that the plaintiff had not suffered a psychiatric injury, and also that the amount should not be disproportionate to amounts commonly awarded for pain, suffering and loss of amenity in personal injury cases.

In New South Wales, it would seem unlikely that a victim of a serious invasion of privacy could seek exemplary damages for a breach of confidence. The NSW Court of Appeal has found that a common law remedy, such as exemplary damages, is unlikely to be granted for an equitable cause of action, such as breach of confidence.[6] Exemplary damages are awarded as punishment to the guilty, as a deterrent and as proof of detestation of their actions. In cases such as *Wilson v Ferguson*, where the invasion of privacy was in retribution for the ending of a relationship, an award of exemplary damages could be appropriate to show the court's disapproval of such conduct, and to prevent similar future invasions of privacy. However, as discussed, this remedy is unlikely to be available if the equitable action of breach of confidence is to be used to protect against serious invasions of privacy.

1.3 The distinction between the concepts of confidence and privacy

'Confidence' and 'privacy' are not identical concepts. While there may be some overlap, there are gaps, such that the equitable cause of action of breach of confidence may not be suited to a potential plaintiff who wishes to protect against a serious invasion of privacy. One such gap is that confidential information loses its quality of confidence when

[5] *Wilson v Ferguson* [2015] WASC at [85].
[6] *Harris v Digital Pulse Pty Ltd* (2003) 56 NSWLR 298.

it enters the public domain. However, something considered to be private will still be considered private by an individual, even if it has already entered the public domain. These differences therefore render the use of an action for breach of confidence inadequate to protect all occurrences of serious invasions of privacy.

2. An examination of the efficacy of the current federal privacy regime (including the Australian Privacy Principles)

2.1 Overview of the current privacy regime in Australia

There are a number of protections currently in place at a Federal level in the privacy sphere. The protection of an individual's privacy interests can be found in regulatory schemes, criminal laws, and civil or private law which provide various mechanisms for individuals to make complaints and seek redress. The primary piece of legislation in Australia is the *Privacy Act 1988 (Cth)*, which regulates the handling of personal information about individuals by government agencies and some private sector organisations, and the associated Australian Privacy Principles (APPs) which cover the use, collection, storage and disclosure of this information.

These provisions are complemented by the *Surveillance Devices Act 2004 (Cth)* which regulates the use, communication and publication of information obtained by law enforcement through the use of surveillance devices (and protects individuals from some intrusions into private conversations and activities). These Federal regimes are further supported by surveillance device legislation at a state level (and further, in some states and territories like NSW,[7] ACT,[8] and (to some extent) Victoria[9] which have specific workplace surveillance legislation).

As for communications privacy, the *Telecommunications Act 1997 (Cth)* prohibits the disclosure of certain information by telecommunications providers. On a state level, we have the *Privacy and Personal Information Protection Act 1998 (NSW)* which provides powers to the NSW Privacy Commissioner that are primarily conciliatory as well as

[7] *Workplace Surveillance Act 2005* (NSW).
[8] *Workplace Privacy Act 2011* (ACT).
[9] *Surveillance Devices Act 1999* (Vic) Pt 2A.

criminal sanctions for the corrupt use of or disclosure of personal information by a public official.[10]

The torts of defamation (which protects individuals and corporations with less than ten employees) and injurious falsehood (available to corporations with more than 10 employees) also provide relief by seeking to protect reputation.

2.2 Relief under the *Privacy Act 1988 (Cth)*

'Personal information' is defined under s 6(1) of the *Privacy Act 1988 (Cth)* as information or an opinion about an identified individual, or a reasonably identifiable individual, whether true or not and whether or not recorded in material form.

A breach of an APP in respect of personal information is an 'interference with the privacy of the individual'. Serious or repeated infringements may give rise to civil a penalty order.[11]

Individuals have a number of remedies if an APP entity has or (is suspected to have) invaded their privacy. They may issue a complaint to the Office of the Australian Information Commissioner (**OAIC**) if there has been (or suspected to have been) a breach of an APP which then initiates an investigation by the Privacy Commissioner.[12] The Commissioner may determine in the investigation that there may have been a breach of privacy, a warning may be issued to the respondent to cease conduct, or the complainant may be awarded compensation.[13] The Federal Court or the Federal Circuit Court may also enforce determinations.[14]

2.3 Gaps and Deficiencies in the Federal Privacy Regime

Even though the existing law provides some protection for serious invasions of privacy for individuals certain gaps and deficiencies in the law should be assessed. The *Privacy Act 1988 (Cth)* and other state and territory equivalents only deal with information privacy. The Act does not cover the scope of 'invasions of privacy'. It does not apply to intrusions to personal privacy or to the behaviour of individuals or media entities and does not apply to businesses with an annual turnover of less than $3 million.[15]

It should also be noted that the Privacy Commissioner's role under the revised *Privacy Act 1998 (Cth)* (having been amended in March 2014) is developing. Under the March

[10] *Privacy and Personal Information Protection Act 1998* (NSW) s 62.
[11] *Privacy Act 1988* (Cth) s 13G.
[12] *Privacy Act 1988* (Cth) ss 36, 40
[13] *Privacy Act 1988* (Cth) s 52(1).
[14] *Privacy Act 1988* (Cth) s 55A
[15] Small business exemption.

2014 amendments, the OAIC was given enhanced powers which included conducting assessments of privacy compliance for the Australian Government and some private sector organisations ("own motion investigations"), accepting enforceable undertakings, and seeking civil penalties in the case of serious or repeated breaches of privacy. However, there continues to be some uncertainty surrounding the discretionary use of these broader powers (for example when the Commissioner will instigate an investigation by its "own motion"), and whether this role will be constrained by budgetary or resourcing issues.

There is also an uncertainty regarding the continued existence of the OAIC and its constituent bodies[16]. Further, Information Commissioner, Professor John McMillan AO, has recently stepped down (as of 31 July 2015) and Timothy Pilgrim will be the Acting Commissioner in the interim (who is the former Privacy Commissioner). In light of these recent changes, and taking into account budgetary and resourcing difficulties that the OAIC faces, it is unclear what future role OAIC and the Privacy Commissioner will have, and how effective it will be in managing the privacy concerns of Australians.

There are also gaps in other provisions. Legislation dealing with surveillance and with workplace surveillance is not uniform throughout Australia. It is suggested that these surveillance device laws should be replaced with a Commonwealth Act. There is also no tort or civil action for harassment nor is there sufficient deterrence against 'cyber-harassment' in Australian law compared with overseas jurisdictions.[17]

3. The experiences of other jurisdictions that have a statutory breach of privacy regime

Any proposal for an Australian statutory tort for serious invasion of privacy would need to be considered alongside the privacy frameworks of other jurisdictions. Various countries have taken different approaches to their privacy regimes, with some opting for a common law regime, namely the United Kingdom, the United States of America, and certain provinces of Canada and New Zealand. These countries have legislation that address privacy breaches when it comes to personal information held by government and private entities, yet other forms of intrusion into private affairs are still largely governed by case

[16] This is due to Australian Government's budget decision to disband the OAIC on 1 January 2015, however this was since revised and the OIAC remains operational (at the time of writing).

[17] A number of US states have enacted cyber-stalking or cyber-harassment legislation or have laws that explicitly include electronic forms of communication within more traditional stalking or harassment laws. Most of these constitute amendments to State Criminal Codes, updating the meaning of harassment and/or stalking to include electronic communications.

law. This section will briefly discuss the privacy regimes of each of these countries as well as one civil law country's privacy regime, being that of France.

The UK has opted for broader privacy legislation, and is very similar to our APPs in its nature. France, however, has more direct privacy legislation designed to regulate and protect the processing of personal data.[18]

3.1 United Kingdom

While having many common law developments in recent years, largely influenced by the *European Convention on Human Rights* (**ECHR**) and the *Human Rights Act 1998 (UK)*, the UK does not have an explicit statutory scheme for breach of privacy. The closest it has come is through the *Data Protection Act 1998 (UK)* which governs the protection of personal data. Although it does not mention privacy, it was designed to protect the rights of people who have had their personal data processed and held by an organisation. It also contains data protection principles, similar to the APPs, which outline how personal data should be processed and that unauthorised or unlawful processing should be prevented via appropriate technical and organisational measures. It is regulated by the Information Commissioner's Office, which can impose fines of up to £500,000 for breaches. This is similar to Australia's Information Commissioner, which can apply for injunctions to restrain a person from engaging in conduct that would constitute a breach of the *Privacy Act 1998 (Cth)*, or can apply to the courts for an order that an entity pay the Commonwealth a civil penalty.

The UK has extended its equitable breach of confidence action to that of misuse or disclosure of personal information, an action in its own right. However, in practice, both are generally pleaded together. The latter action is based on Article 8 of the ECHR and given effect by UK Courts pursuant to the *Human Rights Act 1998 (UK).*

3.2 France

France adopted its data privacy law in 1978, namely the *Data Protection Act No. 78-17* dated 6 January 1978 (*Loi informatique et libertés*) (**DPA**). This act also created the French Data Protection Authority (Commission Nationale Informatique et Libertés (**CNIL**)), which acts as a dedicated national administration for this legislation. This law applies to any person who is in charge of collecting, processing or storing personal data, and is themselves a data controller (loosely defined to be an individual or entity that determines the purposes and means of the data processing (Article 3 DPA)), or a data processer. It regulates personal data, which is broadly defined in Article 2 of the DPA,

[18] For the privacy regimes of other civil law countries, Scotland and Germany, see Mark Warby QC, Nicole Moreham, Iain Christie (eds), *Tugendaht and Christie: The Law of Privacy and the Media* (Oxford University Press, 2011) ch 3.

and entails the collection of any data that can identify a person, directly or indirectly. This definition allows for many forms of personal data to be included in the scope of this legislation, ranging from automatic processing of personal data to non-automatic processing of personal data that is or may be contained in a personal data filing system.

With regards to enforcement, the CNIL's powers are set out in Article 44 of the DPA. These powers include the ability to conduct on-site inspections (with access to any storage devices), document reviews and conduct hearings. Furthermore, the CNIL can then enforce sanctions by, for example, ordering the lock up of the processed data for a period of three months, and notifying the Prime Minister to take steps to stop the violation. Financial penalties must be proportional to the severity of the breach (Article 47 DPA), and can be a maximum fine of €300,000 (approximately $450,000) and five years' imprisonment for a breach.

Consequently, France's approach to data privacy is quite varied when considering the UK's legislation, as it explicitly deals with the protection and privacy of personal data, rather than merely providing guiding principles for individuals and organisations who are involved in processing personal data.

3.3 The United States of America

The USA has four categories of privacy tort as stated in the *Second Restatement of the Law.*[19] Following Prosser's classification, the breadth of privacy torts is as follows:

1. Intrusion: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person";[20]

2. Misappropriation and Right of Publicity: "One who appropriates to his own use or benefit the name or likeness of another"; [21]

3. Public Disclosure of Private Facts: "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of privacy if the matter publicised is of a kind that (a) would be highly

[19] R Prosser, 'Privacy' (1960) 48 *California Law Review* 383, 389.

[20] *Restatement of the Law, Second, Torts* (1977) adopted and promulgated by the American Law Institute, vol 3, 52B, 378.

[21] Ibid, 652C, 383.

offensive to a reasonable person and (b) is not of a legitimate concern to the public";[22]

4. False Light: "One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if:
   a. the false light in which the other was placed would be highly offensive to a reasonable person, and
   b. the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed."[23]

Unlike privacy law in Australia, these privacy torts have been well-established in American law for decades, however the ALRC has pointed out that the protection that they provide is limited given the constitutional protection of freedom of speech in the First Amendment of the US Constitution.[24] The State of California has introduced a statutory tort of invasion of privacy.[25]

3.4 Canada

In Canada, privacy law is protected by the *Canadian Charter of Rights and Freedoms* (which only applies to government),[26] legislation[27] and to a certain extent, common law. The Canadian provinces of British Colombia,[28] Manitoba,[29] Newfoundland and Labrador,[30] Quebec[31] and Saskatchewan[32] have their own statutory torts for invasion of privacy. These are supported by common law.[33] The federal government and a few provinces have enacted legislation that protects personal information held by private

---

[22] Ibid, 652D, 383.

[23] Ibid, 652E, 383.

[24] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Discussion Paper 80 (March 2014) 23 [1.23].

[25] *California Civil Code* §1708.8.

[26] *Canadian Charter of Rights and Freedoms*, Part 1 of the Constitution Act 1982, Sch B to the Canada Act 1982 (UK) 1982, c 11.

[27] *Privacy Act*, RSC 1985, c P-21; *Access to Information Act*, RSC 1985, c A-1; these statutes address collection, use and disclosure of personal information by government agencies and rights of access to personal information held by government organisations.

[28] *Privacy Act*, RSBC 1996, c 373.

[29] *Privacy Act*, RSM 1987, c P125.

[30] *Privacy Act*, RSNL 1990, c P-22.

[31] *Civil Code of Quebec*, SQ 1991, c 64 ss 3, 35-37.

[32] *Privacy Act*, RSS 1978, c P-24.

[33] *Jones v Tsige* (2012) 108 OR (3rd) 241.

entities.[34] Moreover, the Commissioner of Canada investigates complaints of potential breaches of privacy and makes recommendations in relation to Internet privacy.[35]

While the *Canadian Charter of Rights and Freedoms* does not contain an express right to privacy, section 7 ("right to life, liberty, and security of the person") and section 8 ("the right to be secure against unreasonable search or seizure) have been applied to protect "reasonable expectations of privacy".[36] Australia does not have an equivalent to Canada's Charter.

Those provinces which have protection for privacy torts provide that it is a "tort, actionable without proof of damage, for a person to wilfully and without claim of right, to violate the privacy of another person".[37] Conduct included in the tort include using the name or likeness of a person without consent in advertising or promotion and using letters or other personal documents without consent. Remedies include damages, injunctions, account for profits, or delivery of documents. Defences include consent, lawful authority, and in the case of publication, public interest, fair comment or privilege under defamation law.

3.5 New Zealand

Privacy is not directly protected in the New Zealand *Bill of Rights Act 1990*. New Zealand's *Privacy Act 1993* provides protections comparable to those in the *Data Protection Act 1998 (UK)*, but does not apply to "any news medium" engaged in "news activities".[38] Its legislative framework for protection of personal privacy is, like Australia's, piecemeal at best. And like Australia, it does not have a statutory cause of action that specifically addresses invasion of privacy.

However, New Zealand has come a longer way with regard to its common law, with the cases of *Hosking v Runting* [2004] NZCA 34 (publicising personal information) and *C v Holland* [2012] 3 NZLR 277 (intrusion upon seclusion). The latter case involved the

---

[34] Personal Information Protection Act, SBC 2003, c 63; Personal Information Protection Act SA 2003, c P-6.5; Act Respecting the Protection of Personal Information in the Private Sector, RSQ c P-39.1.

[35] For example, see Privacy Commissioner of Canada, 'Letter to Google Inc., regarding the company's proposed retention plan for images collected for its Streetview application' (August 21, 2009); Privacy Commissioner of Canada, 'Report of findings into the complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act (2009), <http:///www.priv.gc.ca>

[36] *R v O'Connor* [1995] 4 SCR 411, (1995) DLR (4th) 235, *Hunter v Southam Inc* [1984] 2 SCR 145.

[37] Privacy Act , RSBC 1996, c 373, s 1(1); Privacy Act , RSS 1978, c P-24, s 2; Privacy Act, RSNL 1990, c P-22, s 3(1). Manitoba's statute uses the language of "substantially, unreasonably and without claim of right": Privacy Act, CCSM, c P125, s 2(1).

[38] *Privacy Act 1993*, s 2(1).

surreptitious filming and disclosure of footage of a fellow housemate in the shower. Whata J noted at [6]-[7] that the defendant had 1) intruded into the plaintiff's solitude and seclusion, 2) infringed a reasonable expectation of privacy and 3) his act was highly offensive to a reasonable person. This is largely reasoning drawn from American law.[39]

3.5 Applying international experiences to Australia

The Committee submits that Australia still has further to go in regards to protection of personal privacy. It has not yet reached a level of protection that is as developed as other jurisdictions discussed in this section. Indeed, the lack of human rights legislation is one factor that state and federal governments might consider more closely. Tomlinson QC alludes to the fact that Australia's trajectory of privacy law should be steered towards that of the UK or NZ, both of which draw upon the human rights jurisprudence on personal privacy (Strasbourg case law).[40] The Committee agrees with this general approach (however, it is noted that the Australian Capital Territory and Victoria are the only States in Australia that currently have human rights legislation).[41]

The Committee also submits that Australia would need to be careful to separate a privacy tort from the pre-existing common law actions of defamation, trespass, action on the case for intention infliction of harm and breach of confidence,[42] as these causes of action do not directly protect the right to privacy, but were originally developed to address different interests.

In particular, the Committee is of the view that to expand the breach of confidence cause of action to invasions of privacy (in the same way that the UK has) would conflate the original equitable action. Moreover, it would not necessarily be appropriate to address intrusions upon seclusion or private affairs or a person's solitude, as a breach of confidence usually involves published matter, so intrusions without publication would not be best addressed by this cause of action.

The Committee submits that a separate cause of action, as previously proposed by the ALRC in DP80[43] would be most appropriate. Breach of confidence could shed light on

---

[39] American Law Institute, *Restatement of the Law Second, Torts* (1977) § 652B.

[40] Hugh Tomlinson QC, *How to Create a Privacy Law* (5 May 2011) The Guardian <http://www.theguardian.com/law/2011/may/05/privacy-privacy>

[41] *New Zealand Bill of Rights Act 1990*; *Human Rights Act 2004* (ACT); *Charter of Human Rights and Responsibilities Act 2006* (Vic).

[42] The UK has extended its equitable breach of confidence action to that of misuse or disclosure of personal information, an action in its own right. See section 3.1 of this Submission.

[43] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Discussion Paper 80 (March 2014)

misuse or disclosure of personal information, just as a means of legal reasoning, and not a foundation of the new tort.

The Committee has looked with interest at the ALRC's proposals for a new Commonwealth Act, separate from the *Privacy Act 1988 (Cth)*, which would provide for a new statutory cause of action for serious invasions of privacy. The proposed legislation would cover misuse and disclosure of private information of the plaintiff as well as intrusion upon the plaintiff's seclusion (intrusion upon seclusion). These two types of tortious activity should be treated as separate, but related elements of the same cause of action, due to the difficulty in defining privacy.[44]

4. Considerations as to the scope and application of a statutory cause of action

There are various ways in which to circumscribe the application of a statutory cause of action for serious invasion of privacy. Based on the above analysis of Australian privacy law, and the examination of the approaches to privacy of different jurisdictions, the Committee suggests that the cause of action should be split into two broad types, namely misuse of personal information and intrusion upon seclusion. It is submitted that this approach is preferable to overcome existing gaps in privacy protection while maintaining a balance with competing public interests, such as freedom of expression. It is also submitted that this approach can be achieved by leaving the defining of "serious invasions of privacy" to the judiciary on a case by case basis, and by supplementing each limb of the cause of action with a non-exhaustive list of examples of the types of invasions.

The Committee recommends that the Standing Committee considers the following issues in relation to the scope of the statutory cause of action:

1. whether liability should only be imposed where the plaintiff had a reasonable expectation of privacy in all circumstances;
2. whether the cause of action should be limited to intentional or reckless acts;
3. whether the cause of action should only be available to natural and living persons; and
4. whether proof of damage should be extended to include emotional distress and humiliation.

Further, the defences of consent, absolute privilege, authorisation or requirement due to existing law, or the need to defend property or persons, should be applicable.

---

[44] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Discussion Paper 80 (March 2014) 76-77 [5.53] – [5.58].

4.1 Types of activities caught by the Act

The Committee notes that most invasions of privacy fall under one or both of the following categories:

1. misuse of private information; and
2. intrusion upon seclusion.

Misuse of private information involves the collection and/or disclosure of a person's personal information without their express consent. Examples of such disclosure may range from the sharing of a person's mobile number and residential address to a third party to the publication of a person's sexually explicit photographs on social media.

Intrusion upon seclusion usually involves the surreptitious observation of a person's private life, whether or not any information is published, and indeed regardless of whether any information is gathered at all.

The Committee considers that framing the statutory cause of action in terms of two types of invasions of privacy has the advantage of adding a degree of specificity to what is a notoriously nebulous concept.[45] At the same time, the two limbs are not so specific as to unduly confine the application of the tort.

Adopting these categories also has the added benefit of aligning with proposals for reform in other jurisdictions. Both the 2010 VLRC inquiry and the 2014 ALRC inquiry recommended the splitting of the concept of invasion of privacy into the misuse of personal information and intrusion upon seclusion, although the former submitted that each limb should constitute a separate cause of action[46] whereas the latter suggested that they form two branches of the same tort[47.]

On this issue, the Committee notes the implication of its submission to the 2013 ALRC inquiry[48] (**ALRC Submission**), that there are merits to both arguments regarding whether two separate causes of action should be enacted. In any case, it is submitted that the division of invasion of privacy into misuse of information and intrusion upon seclusion achieves the correct balance between specificity and flexibility, and should be preferred to a statute creating a general cause of action for invasion of privacy.

---

[45] Gummow and Hayne JJ noted 'the difficulties in obtaining in this field something approaching definition rather than abstracted generalisation' in *Australian Broadcasting Corporation v Lenah Game Meats* (2001) 208 CLR 199 [116].

[46] Victorian Law Reform Commission, Surveillance in Public Places, Final Report 18, 147.

[47] ALRC, 74.

[48] Submission to the Australian Law Reform Commission by the NSW Young Lawyers Communications, Entertainment & Technology Law Committee and Human Rights Committee in relation to Serious Invasions of Privacy in the Digital Era – Issues Paper dated 29 November 2013

4.2 Non-exhaustive lists

The Committee supports the inclusion of a non-exhaustive list of examples of invasion of privacy in the legislative provisions which impose the cause of action. Such a list will provide a point of reference for decision makers, while at the same time allowing for the tort's application to new or unforeseen examples of privacy invasion (which will help to ensure that the tort remains adaptable to new and emerging technologies).

The Committee recommends that the following examples could be used to illustrate the misuse of private information:

1. assuming the identity of another person; and
2. unauthorised access to services or accounts used to communicate privately or to store private information;

and that intrusion upon seclusion could be illustrated by the following examples:

3. intrusion into home or family life; and
4. physically intruding into the plaintiff's private space or by watching, listening to or recording the plaintiff's private activities or private affairs[49].

4.3 Intentional or reckless invasion of privacy

A tort that too readily confers liability for invasion of privacy runs the risk of compromising the right to freedom of speech and political communication, as well as the ability of the media to investigate matters of public concern.

The Committee therefore suggests that the Standing Committee strongly considers the implications of a statutory cause of action that goes beyond intentional or reckless behaviour. While the Committee acknowledges that negligent or accidental acts of invasion of privacy can be just as damaging to an individual as deliberate or reckless invasions, it is submitted that negligence lacks the moral culpability or fault element associated with deliberate, wilful or reckless conduct.

4.4 Cause of action restricted to natural persons and living persons

Another way of ensuring that a statutory cause of action does not unduly restrict the right to freedom of speech or the ability to scrutinise institutions of power is to confine the application of the cause of action to breaches of privacy of natural persons.

The Committee notes that at its core, privacy should be considered a personal right, concerned with the deleterious effect upon an individual of unauthorised access to

[49] This example was posited in ALRC, 85

intimate information or physical space. It is submitted that corporations lack the 'sensibilities, offence and injury… which provide a staple value for any developing law of privacy'.[50]

As such, the Committee is of the view that the cause of action for serious invasion of privacy should not survive the death of the plaintiff. This is consistent with a cause of action for defamation, where generally the action does not survive for the benefit of the defamed person's estate, because a reputation is personal. Similarly, the Committee contends that the cause of action for serious invasion of privacy should not provide for the survival of the cause of action for the benefit of the estate of the person whose privacy was invaded before his or her death, because privacy is personal.

4.5 Reasonableness

The Committee also suggests that the scope of the statute be limited to situations where the plaintiff had a reasonable expectation of privacy in all circumstances.

Such a requirement would ensure that persons who are hypersensitive to observation, or have a higher sense of entitlement to seclusion than society's norms, could not use the statute to unduly restrict the legitimate acts of others.

4.6 Defences

Conduct authorised or required by law or incidental to exercise of a lawful right

The Committee is of the view that a defence to the new statutory cause of action should exist where the impugned conduct was authorised by the person who would otherwise have had their privacy invaded.

The Standing Committee should also consider defences for situations where the conduct was required by or under law, where the conduct arose out of necessity or where it was incidental to the exercise of a lawful right of defence of persons or property.

However, this defence should be qualified to the effect that the conduct must have been proportionate or necessary and reasonable, bearing in mind any flexibility granted by the legal requirement to disclose, or the seriousness of the risk to persons or property.

---

[50] Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 208 CLR 199.

Absolute privilege

The Committee submits that the common law and statutory defamation defence of absolute privilege[51] should be available for serious invasions of privacy. The defence of absolute privilege, which attaches to any statement made on a "privileged occasion", facilitates full and frank debate in Parliament and in court, which is necessary to ensure rigour and transparency in the formation and interpretation of our laws.

5. Consequences for a breach of a statutory cause of action

5.1 Action per se

The Committee is of the view that an invasion of privacy should be actionable per se, with minimum penalties to apply even if actual damage cannot be proven. The penalties applicable should increase according to the extent of damage that can be proven (noting that in the following section, the Committee submits that the types of damages recognised under the cause of action should be widened to include non-financial damage).

This approach is both consistent with the Committee's previous ALRC Submission, and the idea canvassed in section 3.5 above that the cause of action should be approached from a human rights perspective.

5.2 Damage

The Committee recognises that invasions of privacy are often non-financial in consequence, resulting instead in emotional distress, humiliation and insult, and therefore falling short of provable damage. Approaching invasions of privacy in the same way as the intentional torts of trespass and defamation is appropriate, as it would allow the court to award a wider range of remedies to redress the invasion of privacy. This would also address the key gap in the common law's inability to award damages in tort, outside the scope of trespass and defamation, for non-financial consequences of conduct invading privacy.

As such, the Committee suggests that the Standing Committee consider including emotional distress, humiliation or insult within the definition of "damage" for the purposes of the statutory cause of action for serious invasion of privacy. This would be consistent with s 52 of the *Privacy Act 1988 (Cth)*, which includes injury to the plaintiff's feelings or humiliation suffered by them.

---

[51] *Defamation Act 2005* (NSW) s 27

5.3 Civil Penalties

Finally, the Committee submits that a similar regime regarding civil penalties for repeated breaches, as provided for in the Privacy Act 1988 (Cth) (as described in section 2.2 above) should be considered by the Standing Committee for breaches of privacy. It is submitted that this would have a desired deterrent value and would allow redress in situations where plaintiffs are not willing to pursue breaches of their privacy and/or where one person repeatedly breaches the privacy of different people.

Concluding Comments

The Committee is of the view that a cause of action for serious invasions of privacy would be a welcome addition to privacy protection laws in New South Wales, particularly in an era where technological advances are creating additional avenues for invasions of privacy. The Committee submits that such a cause of action has become necessary to protect the privacy interests of individuals. It should be broad enough to adapt to changing social contexts and technologies, but also provide flexibility for legitimate competing interests and defences.

NSW Young Lawyers and the Committee thank you for the opportunity to make this submission. If you have any queries or require further submissions please contact the undersigned at your convenience.

Contact:

Elias Yamine
President
NSW Young Lawyers
Email: president@younglawyers.com.au

Alternate Contact:

Chris Chow
Chair
NSW Young Lawyers Communications, Entertainment & Technology Law Committee
Email: cet.chair@younglawyers.com.au