Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

Committee Chair
The Hon Natasha Maclaren-Jones MLC
Standing Committee on Law and Justice
Legislative Council, Parliament of NSW
Macquarie Street
Sydney NSW 2000

By email: lawandjustice@parliament.nsw.gov.au

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

This submission responds to the invitation by the Standing Committee on Law and Justice to contribute to the inquiry into remedies for the serious invasion of privacy in New South Wales.

The submission is made by the Australian Privacy Foundation, the nation's leading civil society body regarding privacy.

Summary

In summary –

- the New South Wales Parliament has the power to effectively address serious invasions of privacy that occur in the state.
- Parliament both can and should enact a law that specifically deals with serious invasions of privacy.
- such a law has been strongly recommended by a range of NSW, Commonwealth and other law reform bodies over the past decade. It is not precluded by an exclusive power of the Commonwealth.
- those recommendations reflect the inadequacy of the state and national frameworks in protecting all Australians in a range of circumstances, including young people in offline and online environments.
- a state enactment dealing with serious invasions of privacy would not impose inappropriate burdens on business, inhibit effective public administration or chill free speech and journalism.
- that enactment would not involve extraordinary difficulty in drafting or interpretation by courts.
- it involves matters dear to all Australians and should be adopted by the state Government without delay.
- The Government can also set an example for the other Australian jurisdictions by strengthening law and encouraging best practice beyond the recommended 'invasions' enactment.

The Foundation accordingly recommends that the Committee should –

- recognise the substantial work by NSW and other law reform commissions and parliamentary inquiries over the past decade.
- also recognise the detailed submissions from across the spectrum that demonstrates the need for law reform to address invasions of privacy.
- embrace the early development of a technologically-neutral statutory cause of action regarding invasions of privacy, with scope for meaningful remedies (in particular compensation on an individual or class basis) to people whose privacy has been invaded
- also embrace statute law reform dealing with specific concerns such as 'revenge porn' and 'sexting', noting models in other jurisdictions such as Victoria
- encourage effective implementation of a principles-based regime through appropriate funding of the NSW Information & Privacy Commissioner and mechanisms such as scope for that agency to act as an amicus curiae
- recognise the importance of cooperation between Commonwealth law enforcement and other agencies, NSW agencies, the agencies of other governments and private sector entities.
- encourage development of a coherent and comprehensive national regime through action by the NSW Government to ensure discussion of privacy law reform in law/justice ministers meetings.

Remedies for the serious invasion of privacy in New South Wales

The submission

The submission is made by the Australian Privacy Foundation, the nation's leading civil society body regarding privacy. The Foundation has an inclusive and non-partisan basis. Its board and membership include barristers, legal academics, technology experts, consumer advocates and non-specialists. Its advice has been recognised by law reform commissions and parliamentary inquiries over several decades. (A brief backgrounder is provided as Attachment A; more information is accessible at privacy.org.au which features copies of Foundation submissions and policy papers over the past decade.)

This submission is structured as –

1 Background
2 Building on past consultation
3 A cooperative approach is valuable
4 Action based on principles, not technologies
5 Establishing a statutory cause of action
6 NSW law can coexist with the Commonwealth statutes
7 Invasion and fault
8 Effect of Apology
9 A reasonable expectation of privacy
10 Identifying what is a serious invasion
11 It is possible to balance privacy with other interests
12 NSW and other forums for litigation
13 Breach of confidence actions
14 Injunctions to prevent further harm
15 Surveillance Devices – principles, not specific technologies
16 Respect for privacy does not chill journalism
17 Compensation and other remedial relief
18 Local Government
19 The NSW Information & Privacy Commissioner
20 Individuation as the basis of effective privacy protection

The Attachments provide background about the Foundation and an extract from the APF *Policy Statement re Privacy and the Media*.

1. Background

Privacy is of deep concern to most Australians. That is evident in submissions by the legal profession, business, community representatives and others to public consultations by a range of law reform bodies at the Commonwealth and state levels. It is evident in surveys under the auspices of business, privacy regulators and law reform bodies at the state/territory, Commonwealth and international levels. It is also evident in a range of common and statute law that deals with information privacy[1] and matters such as trespass and offensive behaviour.

Concern about invasions of privacy by individuals, by businesses and by government bodies is not decreasing. It both should and **can** be effectively addressed through law reform that recognises the patchiness of existing statute law alongside limitations on the courts to develop comprehensive and coherent remedies under common law.

[1] See for example the *Privacy Act 1988* (Cth), the *Crimes Act 1900* (NSW) ss 91K, 91L and 574C, *Workplace Privacy Act 2010* (ACT), *Police Offences Act 1935* (Tas) s 14A, *Privacy & Personal Information Protection Act 1998* (NSW), *Health Records and Information Privacy Act 2002* (NSW) and *Workplace Surveillance Act 2005* (NSW).

A salient example of efficacious reform – which reflects deep community concerns, addresses abuses involving minors and adults, and does not crimp the mass media or otherwise inhibit the implied freedom of communication under the national Constitution – is Victoria's recent enactment dealing with sexting.[2] That Act demonstrates that state governments have the capacity to deal with invasions of privacy and that their initiative in responding to community needs will gain community support. Law reform is not a matter that should be solely a Commonwealth responsibility.

The need for reform and the shape of the corresponding enactments has been recurrently identified by law reform bodies in New South Wales and the other Australian jurisdictions, for example successive reports by the Australian Law Reform Commission (notably its 2013 *Serious Invasions of Privacy in the Digital Era* and 2008 *For Your Information: Australian Privacy Law and Practice*), the 2009 *Invasion of Privacy* report by the NSW Law Reform Commission and the Victorian Law Reform Commission's 2010 *Surveillance in Public Places* report. Submissions by the Australian Privacy Foundation to those law reform commission inquiries and parliamentary committee inquiries are available on the Foundation's web site.

The following paragraphs address specific matters of relevance to the Committee's inquiry. As background it is pertinent to highlight the guiding principles articulated by the Australian Law Reform Commission in its inquiry into serious invasions of privacy.[3]

These principles are –

- 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; and
- privacy protection is an issue of shared responsibility.

2. Building on past consultation

As the preceding section of this submission noted, there have been a succession of reports by law reform commissions, parliamentary committees and other entities that have identified the need for law reform to address invasions of privacy by business, government and individuals.

In essence, there is a consensus that law reform is necessary. There is a consensus that law reform is achievable.

The reports have been informed by a large body of detailed submissions by government agencies, individuals, legal practitioners, commercial entities and civil society advocates. They reflect findings in Australian courts and in the courts of the United Kingdom, New Zealand and Canada.

The Foundation suggests that the Committee recognise the substantial body of work over the past decade (for example by the NSW Law Reform Commission and Australian Law Reform Commission). The Committee is in a position to build on that work. It is also in a position to build on past consultation about privacy law reform. It does not have to 'start from scratch' in considering effective responses to invasions of privacy. Past consultation demonstrates that responses are neither radical nor inappropriate. Instead those responses are likely to gain strong community support.

---

[2] *Crimes Amendment (Sexual Offences & Other Matters) Act 2014* (Vic). Privacy aspects are highlighted in the May 2013 *Inquiry Into Sexting* Final Report by the Victorian Parliament's Law Reform Committee.

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

The Foundation draws attention to the detailed submissions it has provided to the various law reform commissions (typically cited by those commissions) and parliamentary committees, for example to the Australian Law Reform Commission inquiry into *Serious Invasions of Privacy in the Digital Era*. Those submissions are available on the Foundation's web site at privacy.org.au.

3. A cooperative approach is valuable

The Foundation notes that much invasive activity occurs across jurisdictional boundaries and involves digital networks. New South Wales can be instrumental in fostering coherent law and practice though –

- advice to the Commonwealth regarding imperative changes to Commonwealth law (e.g. regarding telecommunications, broadcasting and aviation) and
- encouragement of a cooperative approach involving actors such as the Office of the Australian Information Commissioner, the Australian Communications & Media Authority, the Commonwealth Attorney-General's Department, the Australian Federal Police and state police forces, and private sector entities such as Facebook and Telstra
- statute law reform specific to New South Wales (e.g. on the model of the Victorian sexting statute noted above).

In the first instance that cooperation can be fostered by ensuring that –

- privacy protection is a matter on the agenda of the law ministers' meetings
- the NSW Government strongly urges the Commonwealth to embrace the Australian Law Reform Commission's findings regarding the inadequacy of the Commonwealth, state and territory privacy law (e.g. through adoption of recommendations regarding establishment of a statutory cause of action for serious invasion of privacy)
- the NSW Government strongly urges the Commonwealth to provide adequate resourcing for the Office of the Australian Information Commissioner and resile from the commitment to formally abolish that body, a commitment that has drawn strong condemnation from senior judges and other observers.

4. Action based on principles, not technologies

Privacy protection in Australia have been bedevilled by an emphasis on particular technologies/practices rather than principles. That emphasis has resulted in confusion on the part of business, journalists, the police and individuals. It has also resulted in inconsistency across the jurisdictions (with some states having to play 'catch up' in updating 'listening devices' statutes to accommodate video or other digital devices), uncertainty on the part of regulators, and abuses where there has been opportunistic use of holes in the law or indifference to inadequate penalties.

The Foundation draws to the Committee's attention the importance of concentrating on principles ... centred on protection from invasions of privacy, irrespective of whether the invasion involves

- a drone,
- spyware surreptitiously installed on a personal computer or mobile phone by a jealous lover,
- dissemination over the net of intimate images as 'revenge porn'
- recording via the 'lapel cams' and 'pen recorders' that are increasingly is use as they become cheaper and easier to obtain
- a disloyal health centre employee using a USB stick to convey a celebrity's medical records to a tabloid publisher
- unauthorised filming of minors or adults in a restroom.

In essence, the time has come to move beyond ‘band-aid’ solutions that are specific to particular devices such as drones and cameras or particular abuses such as illicit recording of personal conversations.

The emphasis should be on the invasion *per se* – discussed below – rather than on *how* the invasion took place.

5. Establishing a statutory cause of action for serious invasion of privacy

The Foundation strongly supports establishment of a statutory right of privacy and a viable cause of action available to individuals to enforce that right. Although the nomenclature is not a matter of significant moment to the Foundation it is appropriate to describe the action as an action in tort. In recommending a cause of action for breach of privacy each of the Australian Law Reform (ALRC), the Victorian Law Reform Commission (VLRC) and the New South Wales Law Reform Commission (NSWLRC) have proposed different models.

The Foundation encourages the Committee to embrace statutory establishment of such a cause of action, both because the tort would provide a remedy for people in New South Wales whose privacy has been disregarded and because the existence of the tort will foster best practice within the public and private sectors.

Consistent with the principles noted above the overall and overriding objective of the Foundation is that any cause of action must be robust, flexible, adaptable and have broad coverage with only very limited and specific exceptions (by means of defences), and be reasonably accessible to individuals in giving them an enforceable right for breaches of their privacy. The threshold for commencing an action should not be high. The action should be sufficiently flexible to allow the tort to adapt with changes in technology and be responsive to societal mores.

The remedies must be robust, diverse and responsive to the ills caused by breaches, including damages, apologies, correction, declaratory and injunctive relief. There should be scope to award significant damages, both general and special. Courts are not generous in the award of damages overall, and general damages specifically. A court should have the discretion to award both aggravated and exemplary damages where the circumstances justify such an award. The cause of action must permit defences that represent relevant competing interests.

The Foundation believes that the most effective structure of a cause of action is that which is consistent with an intentional tort; consisting of elements that a plaintiff must satisfy with countervailing defences available to any putative defendant. There should be no requirement for the court to undertake a balancing exercise as an essential element in determining whether the plaintiff can, on his or her own case, succeed or not

Care must be taken in drafting the statute that the elements of the tort do not, by their architecture unduly constrict its overall operation; for example constraints that may encompass the operation of the “reasonable expectation” element. If this element of the tort is, overall, so difficult to establish it will rarely be used and thereby risks continuing the current problems whereby many serious intrusions are not effectively remedied by legal means.

As a consequence the perception will be that those responsible will be seen to “get away with it” and to repeat intrusions with impunity. This may have the perverse effect of ratcheting down the level of protection one might “reasonably expect”, thus making use of the tort harder over time. This potential "design flaw" of the tort calls for extra efforts to ensure that other potential obstacles to its use are minimised, so people may “reasonably expect” protection and be able to avail themselves of it.

The existing tort in Canada and New Zealand (and has not inhibited legitimate media or other activity) and in the United States is structured in a manner consistent with common law intentional torts. Defendants are able to avail themselves of specific defences. The United Kingdom ("UK")

privacy jurisprudence, by comparison, is grounded in equity and the court must undertake a balancing exercise between the rights set out in Articles 8 and 10 of the *Human Rights Act 1998* (UK). The underlying principles of each head of action differ in significant ways. It is an important distinction.

The Foundation believes that the most effective structure of a cause of action is that which is consistent with an intentional tort; consisting of elements that a plaintiff must satisfy with countervailing defences available to any putative defendant. There should be no requirement for the court to undertake a balancing exercise as an essential element in determining whether the plaintiff can, on his or her own case, succeed or not

6. NSW law can coexist with the Commonwealth statutes

Commonwealth statute law provides an uneven protection against invasion of privacy through a range of statutes such as the *Privacy Act 1988* (Cth), which the Committee may note is weakened through under-resourcing of the Office of the Australian Information Commissioner, and telecommunications enactments.

The law reform reports noted above recognise that there is scope for the New South Wales and other state/territory legislatures to provide meaningful privacy protection through enactments that coexist with Commonwealth statute law. The Foundation draws the Committee's particular attention to the NSW Law Reform Commission's *Invasions* report and to the Victorian legislature's achievement of privacy protection through law regarding sexting.

Overall, action by the NSW Parliament is not precluded by Commonwealth law and should not be delayed on the basis that the Commonwealth will eventually assert its authority. The Foundation urges the Committee to recognise that not all invasions of privacy are readily addressable in terms of information privacy; some can be efficaciously addressed through changes to the state's crimes regime and through vigorous action by the state's Information Commissioner.

7. Invasion and Fault

In responding to the ALRC inquiry the Foundation broadly supported the scope of the first element of the ALRC's proposed cause of action (i.e. regarding intrusion upon seclusion or private affairs, misuse or disclosure of private information). The focus of the tort should be upon the intrusion into a plaintiff's seclusion or private affairs (including by unlawful surveillance) and/or the misuse or disclosure of private information about the plaintiff. Consistent with the principles the Foundation considers that there is no sound legal or policy basis for limiting the scope of the action to either intentional or reckless acts rather than incorporating negligent acts.

The Foundation notes the ALRC's acknowledgement that restricting the action to intentional or reckless acts will mean there are cases where individuals will have no remedy. For those who suffer harm as a result of privacy invasions, it is little consolation that the tort will reduce rather than remove a recognised gap in the law. It is inappropriate that if a plaintiff in NSW suffers loss as a consequence of negligent acts which breach his or her privacy that the appropriate recourse should be to make a claim in negligence or contract. This would represent a cumbersome and unnecessary segmentation of what should be a seamless and broad protection, aimed at redressing a recognised gap in the law. More importantly, breaches of privacy involve discrete issues which are not suited to a claim in negligence or contract.

The Foundation submits that the parameters of the proposed tort should be based on the question of what elements of the cause of action are best adapted to address the harms arising from serious invasions of privacy. There is no persuasive legal argument that damages in a statutory cause of action must be confined to general damages for emotional distress, rather than special damages including economic loss. That emotional distress may be a "key type of harm", which is beyond dispute, does not mean it is the only type of harm suffered. Nor does it mean that it should be the

only type of harm that should be compensated by a statute aimed at redressing serious harms to privacy.

Establishment by the NSW Parliament of a statutory right for an individual to recover general damages for negligent acts arising out of a privacy breach will not, as a matter of law, alter the common law position regarding other forms of negligence.[4] The nature of the breach is distinct and the facts are commonly, if not invariably, different from those involving other forms of negligence. A statutory cause of action involving breach of privacy is discrete and stands alone, being designed to address specific forms of harm.

The Foundation encourages the Committee to disregard speculation and critique claims that extending liability to negligence may crimp legitimate media activity, lead to excessive self censorship and result in a chilling effect on every day activities. Such claims are empirically unsustainable and are typically advanced by media organisations whose self-regulation is contestable, evident for example in large-scale hacking by News group personnel in the UK that has not been disowned by that group's controlling shareholder. Concerns that negligent actions may inhibit expression, chill free speech and expose those to liability for unintentionally invading someone's privacy should be obviated by a robust public interest defence that adequately protects freedom of expression. Having a broader scope for actionable conduct with a proper, carefully defined, robust defence would avoid the need for arcane and overly-complex arguments as to whether conduct is reckless rather than negligent.

8. Effect of an apology relating to invasion of privacy

The Foundation agrees with the ALRC that an apology or correction of published material by a defendant should not be treated in evidence as an admission of fault. The Foundation further submits that it is unnecessary to provide for the elimination of causes of action already in existence. The existence of the tort is to address the specific goal of filling a gap in the law in this particular area. The concern about an overlap is, in any case, more abstract than real and a matter that does not require legislative action.

9. A Reasonable Expectation of Privacy

As a general principle the Foundation supports having a non exhaustive, non binding, list of factors relevant in the consideration of a reasonable expectation of privacy, provided its operation does not extend, in law or practice, to limiting

- the factors parties may rely upon,
- those factors which the courts should consider and
- the weight that must be given to each, all or none of the factors in any particular case.

Courts should have the broadest discretion as to what they should or should not consider. In this respect, the law should be allowed to develop incrementally and not within rigid structures.

The Foundation notes that it is poor public policy for a person to need to express a desire not to be the subject of a tortious wrong. Even as merely one factor, amongst many, in a non exhaustive list does not seem to be appropriate. At a practical level how should such desire be manifested? Such a factor is likely to be used by defendants who may use the lack of a demonstrated, overt desire as being a factor to be taken into account against a plaintiff.

Similarly great care should be given in taking into account the age and occupation of a party as being any part of a relevant factor. Such an approach has the potential to arbitrarily segment the

[4] The ALRC's conclusion, in its *Serious Invasions* discussion paper, that having both intentional/reckless and negligent acts encompassed as elements in a statutory cause of action would undermine the coherence in the law, is not persuasive. Moreover, the ALRC does not rely upon evidence to demonstrate that recognising a cause of action for negligent invasions of privacy would influence, undermine or detract from the operation and development of other discrete common law causes of action.

operation of the law. Even the slightest possibility that the law may apply differently depending on age, educational standards, profession of the plaintiff should generally be avoided.

The Foundation cautions against establishing some form of "public figure" consideration which may warrant less protection being afforded to certain individuals. (That consideration is overly broad; other factors are more reasonable, such as where the intrusion occurred, the sensitivity of the information involved, and the purpose of the misuse.)

10. Identifying seriousness in an invasion of privacy

There has been disagreement about whether the cause of action should only be available where the invasion of privacy is 'serious' and what constitutes 'serious'.

The Foundation considers that the Victorian Law Reform Commission's approach is better equipped than that of the NSW Law Reform Commission in dealing with what invasions should be addressed under the tort.

If the cause of action is structured as an intentional tort damage should be presumed. The remedy, whether in the form of injunctive relief, damages or other relief, will (or should) reflect the seriousness of the breach. To that extent establishing a threshold of 'serious in all the circumstances' is unnecessary. Similarly, delineating conduct as highly offensive rather than merely offensive is also unnecessary. Offensive conduct is a sufficiently high threshold if there is to be one. Furthermore, the distinction between "highly offensive" and "offensive" at law and in practice is not entirely clear. Clearly the former behaviour is worse than the latter.

The egregiousness of the conduct, if found to constitute a breach, should be reflected in the scope and, where appropriate, quantum of damages.

11. It is possible to balance privacy with other interests

The Foundation submits that there is little utility in incorporating a balancing exercise of the plaintiff's privacy interest against freedom of expression or other broader public interest. The Foundation does not accept the assertion that it is widely accepted that the public interest must be considered at some stage in an action for breach of privacy. That presupposes that public interest considerations apply as a matter of course and all privacy actions follow a similar pattern and will continue to do so.

Ideally the issues of freedom of expression and other legitimate defences should be discrete defences. In that respect the balancing of interests proposed by the ALRC is more consistent with the approach taken by the UK courts when considering Articles 8 and 10 of the *Human Rights Act 1998* (UK) as they are required to do. That exercise is done as part of an equitable cause of action, the misuse of private information. That is a separate and distinct cause of action to that of the statutory tort proposed by the ALRC, which incorporates an action against intrusion.

In practice, in tortious claims it is more appropriate and efficacious for a defendant to plead defences of his/her/its own choice, facts and law permitting. Defendants may not necessarily wish to agitate any form of 'public interest' defences, as should be their right. There may be good legal, tactical and practical reasons to avoid agitating some defences, which may include public interest related defences even if the facts permit it.

If a defendant does not wish to rely upon a public interest defence, for example, simply alleging the act did not take place and nothing further, and the plaintiff claims there is no public interest issue, then the mandated exercise of taking public interest into account as part of the cause of action will be artificial, unnecessarily time consuming and costly. Having the two reluctant parties having to address an issue neither believes applies is the antithesis of modern civil procedure and case management.

The Foundation acknowledges that there may be some potential dangers with a broadly-framed 'public interest' defence, associated in part with the terminology. In particular, the Foundation believes that the protection of privacy is a public interest as well as a private interest, so use of "public interest" (in opposition to the interest in protecting privacy) can potentially be misleading. Moreover, the protection of privacy (and related rights and interests, such as confidentiality and information security) may support other public interests including, on occasion, the right to freedom of expression. Any reference to the "broader public interest" in the context of this tort should therefore include some acknowledgement of privacy's key role in support of other public interests, and not imply automatic incompatibility with or hostility to privacy and related values. This could, for example, be achieved through appropriate use of interpretative material, such as an objects clause in the proposed legislation, or appropriate qualifications in the explanatory memorandum.

On the broader point, the Foundation submits that there is no evidence for concluding that having public interest as a defence, rather than an element of the cause of action, would prolong the length of time of an unmeritorious claim. There are fact situations where public interest defences are not relevant. For example it does not follow that a privacy action will necessarily, or even often, involve freedom of expression issues. Breaches of privacy, much like defamation proceedings, do not invariably involve the media. The facts can, and often are, more prosaic and do not throw up significant public interest issues even if they involve an invasion of privacy.

12. NSW and other forums for litigation

The Foundation notes and endorses the ALRC proposal that state, territory and federal courts should have jurisdiction to hear an action for serious invasion of privacy under the proposed Commonwealth legislation regarding an invasion of privacy.

The inclusion of lower levels of State and Territory courts is, in particular, supported because, as PIAC and others have submitted, '[a]ccessibility is a key factor in considering which forum is appropriate ...'.

Complainants/plaintiffs should have the option to take actions for interferences with privacy to the Courts, not only to the Privacy Commissioner, a fortiori in the case of a 'serious invasion of privacy'.

13. Breach of Confidence Actions for Misuse of Private Information

There is a case for clarifying the availability of compensation for emotional distress in actions for breach of confidence. Although the Victorian Court of Appeal *in Giller v Procopets* (2008) 24 VR 1 held that equitable compensation could be recovered for emotional distress in an action for breach of confidence, the position remains unnecessarily complex and uncertain. As emotional distress is often the main harm arising from a breach of confidence relating to personal or private confidential information, the availability of compensation for this harm is necessary to ensure that complainants are entitled to a suitable remedy.

It is desirable to clarify the law even if a NSW or Commonwealth statutory tort is introduced. The Foundation is not disquieted by the potential availability of more than one cause of action arising from the same set of facts. It may be, for example, that a breach of confidence involves both a misuse of personal information and an unauthorised use or disclosure of other information, such as commercial information. If a statutory tort were introduced, a complainant seeking compensation would still need to bring an action for breach of confidence in relation to the non-personal information. Although there may be an overlap between the statutory tort and the action for breach of confidence in relation to the misuse of personal information, the courts have well-established mechanisms for preventing double compensation.

The ALRC proposed that the desired statutory clarification should be confined to actions for breach of confidence that concern a serious invasion of privacy by the misuse, publication or disclosure of personal information.

The Foundation considers that distinguishing actions for breach of confidence that involve personal information from those which do not risks introducing unnecessary complexity. The introduction of a statutory clarification ensuring the availability of compensation for emotional distress in actions for breach of confidence would seem sufficient to achieve the desired objectives, given that courts can, in their discretion, be trusted to confine such awards to appropriate cases.

14. Injunctions to prevent further harm

The Foundation considers agrees that courts hearing interlocutory applications must exercise caution where the application seeks prior restraint of publication, a position endorsed by Gleeson CJ and Crennan J in *ABC v O'Neill* (2006) 227 CLR 57. It notes that privacy and related rights are, in many cases, the foundation of other rights. For instance, freedom of expression, freedom of association and freedom of religion may all require protection of privacy, personal information security and confidentiality for their full exercise.

Consequently, proposals for expressly recognising public interest considerations in the context of actions for breach of confidence must also incorporate explicit recognition of the essential public interest character of privacy and related rights, including their central role in supporting other rights and freedoms,

The Foundation does not consider that different considerations should be applied to actions for breach of confidence aimed at protecting private information than apply to actions for protecting other confidential information, as the public interest in protecting privacy is not a lesser interest than the public interest in protecting confidentiality. Privileging 'commercial' information over 'personal' information that does not have a readily discernable commercial value (e.g. doesn't relate to a celebrity) also seems to be antithetical to introducing a cause of action regarding invasion of privacy. It would, for example, perpetuate the problems evident in the *Douglas v Hello!* Litigation, where public figures are able to assert that information about themselves has a commercial value and thus can use confidentiality law to gain protection that may be unavailable to complainants who are not public figures or celebrities. Moreover, those who are not public figures or celebrities may find disregard of their privacy more distressing, as they are not inured to life under the spotlight.

The public interest considerations taken into account by courts exercising the balance of convenience in applications for interlocutory injunctions are conceptually distinct from the availability of, and the scope of, a public interest defence to actions for breach of confidence. The Foundation considers that Australian courts have adopted an unduly narrow approach to the public interest defence in the context of actions for breach of confidence, effectively ruling out considerations relating to the broader public interest in freedom of expression. Just as there is a case for a public interest defence to a statutory action for serious invasion of privacy, there is a case for a public interest defence to actions for breach of confidence. There is no case, however, for specifically confining the defence to actions for protecting private information, as the public interest in freedom of expression also applies to other forms of confidential information, including government and commercial information.

15. Surveillance devices – principle, not specific technologies

The Foundation considers that the current State and Territory surveillance device and workplace surveillance laws are inadequate for protecting the privacy of Australians, and should be reformed as a matter of priority. The lack of uniformity in the laws between the States and Territories has created considerable uncertainty about what is legally permissible and what is impermissible surveillance. This has been compounded by an apparent reluctance to inform the public about the laws and the allocation of limited resources to enforce the laws.

The lack of consistency in State and Territory laws poses difficulties both for victims of unjustified surveillance and for those lawfully able to use surveillance devices. While it is important to remove inconsistencies and promote uniformity, this must not be at the expense of reducing the level of protection of Australians against unjustified surveillance.

Given the proliferation of existing and emerging surveillance technologies and practices, it is more important than ever for Australians to have a high level of protection against surveillance unless there is a compelling public interest that justifies surveillance. In other words, uniformity should not be achieved at the expense of watering down Australians' rights to be free from unauthorised surveillance and any standardisation should be based on 'best practice' protection of privacy and not on 'lowest common denominator' protection.

In general, the Foundation considers that what amounts to a 'private activity' should, in general, be determined by reference to whether there is a 'reasonable expectation of privacy' and not, for example, to whether an activity is carried on inside or outside a building (which is the case with the current offence for optical surveillance in Victoria). Nevertheless, the Foundation acknowledges concerns with the 'reasonable expectation of privacy' benchmark. The main concern with adopting this standard is that it raises the possibility of privacy invasive technologies and practices which become entrenched changing what is regarded as 'reasonable', thereby shifting the playing field. While there may not be any one perfect solution to the problem of satisfactorily defining what amounts to a 'private activity', the Foundation urges the Committee to give serious consideration as to how best to deal with the potential for privacy rights to be eroded by changing expectations, possibly instigated by business practices premised on large-scale privacy invasions.

The Foundation emphasises that offences for data surveillance should not be confined to law enforcement officers. Uniform surveillance device laws should adopt a technology-neutral definition of a 'surveillance device'. What amounts to a surveillance device should be determined by reference to the objective purpose of the device. The focus should be on whether or not the device is capable of surveillance and not, for example, on distinctions focused on the capability of technologies – whether hardware or software – for performing surveillance functions, and not on the specific features of particular technologies.

Although flexible, technology-neutral definitions may be thought desirable at the general level, the Foundation has reservations about this, as there may well be particular technologies which give rise to specific concerns. Where this is the case, or where it is necessary to avoid doubt about whether or not a type of device is subject to the law, there may be an inescapable need for definitions to refer to particular technologies. In order to avoid the possibility of surveillance devices escaping regulation as a result of abstract legislative definitions, it may be advisable to include indicative lists of current and emerging technologies that are intended to fall within surveillance device laws.

The Foundation considers that NSW and Commonwealth laws should apply to all existing and emerging technologies that are capable of monitoring and recording the activities of people and their data. For example, the laws should make it clear that they apply to unjustified surveillance by means of drones, wearable devices, data surveillance devices or RFID devices. Where there are gaps in the law, such as the monitoring of communications over wireless local networks, these unintentional exceptions should be removed. Moreover, as multi-functional mobile devices proliferate, it is important that protections against widespread surveillance to be maintained, even if this means that devices formerly thought not to be surveillance devices are caught by the regulatory net.

The Foundation suggests that NSW (and other) surveillance device laws should include a general offence proscribing surveillance or recording of private conversations or activities without consent, provided that what is 'private' and what amounts to 'consent' are adequately defined. As indicated above, the Foundation considers that, in the absence of a more satisfactory test, 'private' conversations and activities should be defined by reference to whether there is a 'reasonable expectation of privacy'. In relation to 'consent', it is important that any consent be freely given and unambiguous, and not unnecessarily implied or inferred from surrounding circumstances. In this respect, the Foundation considers that an overly-lax approach to consent in Australian information privacy law has tended to normalise privacy-invasive practices as, in practice, individuals are often given little option but to agree to data processing.

The Foundation considers that, unless surveillance is subject to specific exceptions, it should not be covert and should only be conducted with the consent of all parties to a conversation or activity. There may be limited circumstances in which there is a public interest in allowing participant monitoring, such as where it is reasonably necessary for the protection of the lawful interests of the principal party to a conversation or activity. The Foundation submits, however, that such exceptions should be carefully circumscribed so as to avoid the possibility of the exceptions swallowing the rule.

16. Respect for privacy does not chill journalism

The Foundation supports the public interest activities of responsible journalists in investigating and reporting on matters of public interest, such as uncovering corruption.

The Foundation does not support a broad or vague exception for journalists, however, on the basis that regular recourse to surveillance technologies may well lead to a 'slippery slope', which has been highlighted by unlawful and unacceptable activities of news organisations in the UK, as detailed in the Leveson Inquiry[5] The real concerns arising from the recent history of widespread unauthorised surveillance by media organisations in the UK suggest that quite different considerations apply in determining the scope of defences to surveillance device laws than apply to defences to actions for defamation.

The Foundation supports the creation of a public interest exception for the activities of journalists, but subject to the vital condition that it is satisfactorily confined, so that it does not act as an open invitation for media organisations to undertake surveillance of private activities and practices. We draw attention to the specific formulation in the APF's *Policy Statement on Privacy and the Media* of March 2009. The relevant segment of that Statement is attached to this document.

In particular, care would need to be exercised in defining who was entitled to an exception, as well as precisely limiting the circumstances in which surveillance might be permissible. While a level of surveillance for the purposes of uncovering corruption may be acceptable, there is obviously considerable room for debate about what might amount to corruption in this context. Given the potential for 'scope creep', there may be a case for limiting the exception to circumstances involving 'serious corruption'. In any event, there is no case for surveillance where the activities are merely of interest to the public or likely to titillate the public interest.

In addition, there are serious questions about the level of information or suspicion about corrupt behavior that might be needed in order for surveillance to be justified, especially given the potential for existing and emerging technologies to allow for widespread surveillance as part of 'fishing expeditions'. For example, it would seem that something more than mere speculation about the possibility of corruption should be required before the exception could be relied upon. It may be that any exception for the media should incorporate a 'reasonable suspicion' test – although, even then, difficult questions arise about the level of evidence required to substantiate a reasonable suspicion of corruption.

Finally, the exception for responsible journalism should not be used as a Trojan horse for the reporting of private facts uncovered as part of a corruption investigation. For example, surveillance of a public figure may well reveal personal information, such as information about an affair, which is unrelated to the allegations of corruption.

The journalism exception should not be extended to allow for the publication of unrelated private information where there is no clear public interest in the information being published.

17. Compensation and other remedial relief

[5] The ALRC proposed that surveillance device laws should include a defence of responsible journalism, for surveillance in limited circumstances by journalists investigating matters of public concern and importance, such as corruption. This proposed defence appears to have been influenced by the *Reynolds* defence to actions for defamation under English law.

The Foundation considers that surveillance device laws should provide for courts to make orders for compensation or other remedial relief to victims of unlawful surveillance, on an individual or class basis.

The Foundation suggests that the Committee consider to the precise mechanism for providing victims with an effective means for seeking remedial relief. Given Australia's history of inadequate enforcement of surveillance device laws, the Foundation supports the introduction of a civil penalties regime for breaches of surveillance devices laws. The introduction of a civil penalties regime would establish an effective mechanism for ensuring compliance with surveillance device laws.

If a statutory tort is not introduced, there is an even stronger case for establishing a civil penalties regime under uniform surveillance device laws. Even if a statutory tort were to be introduced, the Foundation considers that there are advantages in establishing an additional affordable mechanism for victims of unauthorised surveillance to seek appropriate relief.

18. Local Government

The Foundation considers that surveillance devices, including CCTV cameras installed for security purposes, should be regulated by strong uniform laws.

Any regulation at the local government level must comply with standards established under uniform surveillance device laws. While there may be scope for councils to be involved with resolving disputes about the installation and use of some devices, this must not be at the expense of strong national standards.

The Committee's attention is drawn to the Foundation's *Policy Statement on Visual Surveillance*, including CCTV, revised in January 2010, which identifies the Principles necessary to provide effective control over these activities.[6]

19. The NSW Information & Privacy Commissioner

The Foundation proposes that NSW law provide for the NSW Information & Privacy Commission (the Privacy Commissioner) to assist the court as amicus curiae and to intervene in court proceedings.

It should also provide for the Commissioner to have jurisdiction to investigate and rule on complaints of 'serious invasions of privacy', with resourcing that would allow the Commissioner to give effect to that power.[7]

The Foundation notes the importance of vigorous and appropriately-resourced privacy commissioners at the Commonwealth and state/territory levels. Timely, well-publicised and robust action by the commissioners serves to build community trust in the legitimacy of those entities and – more importantly – encourage best practice across the public and private sectors. Under-resourcing of regulators is not good public policy; ultimately it burdens individuals and business with unnecessary costs.

20. Individuation as the basis of effective privacy protection

The Foundation encourages the Committee to look beyond 'identification' to 'individuation' as the basis of privacy protection.

---

[6] The Statement is at http://www.privacy.org.au/Papers/PS-CCTV.html.

[7] The Committee's attention is drawn to the 2012 amendments to Hong Kong's Personal Data (Privacy) Ordinance, allowing the Commissioner to grant appropriate applications to act on behalf of a plaintiff (or fund representation by counsel) in a compensation claim before a court. The costs of the Commissioner or counsel in such matters are a first charge on any compensation awarded.

The definition of ‘personal information’ in state law and practice should be amended so that it no longer is restricted to information which has the capacity to identify an individual, but also includes information which provides the capacity (whether by itself or in conjunction with other information) for another entity to interact with an individual on an individualised or ‘personal’ basis. If an entity can send a person emails, SMS messages or the like, or configure their experience of a website or other digital facility, on the basis of information that depends upon their individual experience, history, preferences or other individuating factors, then such information should be regarded as personal information, and the interaction with them should be regarded as the use of such personal information. Such individuated/personalised interactions are now the basis of all marketing conducted on the Internet and via mobile telecommunications, and as such constitute one of most significant serious invasions of privacy in the digital era.

Moreover, the Foundation considers that rapidly emerging marketing practices, including online behavioural advertising, psychographic profiling and predictive analytics, mean that this issue requires urgent attention. A change, along the lines suggested here, which is under consideration in current European law reform processes, would involve a major strengthening of privacy protection relevant to this reference.’

Principles are identified in Attachment B to this submission.

Representatives of the Foundation would be pleased to discuss this submission with you and address particular aspects in more detail.

Thank you for your consideration.

Yours sincerely

Australian Privacy Foundation

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, SubCommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby AC CMG and The Hon Elizabeth Evatt AC, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90) http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html

- The Media (2007-) http://www.privacy.org.au/Campaigns/Media/