Submission No 29

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

Organisation: Department of Justice, NSW Government

Date received: 24/09/2015

Legislative Council Law and Justice Standing Committee

Inquiry into remedies for the serious invasion of privacy

NSW Government submission

25 September 2015

Contents

Introduction

The NSW Government provides the following information to the Legislative Council Law and Justice Standing Committee (Committee) for the purposes of informing its inquiry into remedies for the serious invasion of privacy.

The terms of reference for the inquiry are:

> That the Standing Committee on Law and Justice inquire into and report on remedies for the serious invasion of privacy in New South Wales, and in particular:
>
> (a) the adequacy of existing remedies for serious invasions of privacy, including the equitable action of breach of confidence
>
> (b) whether a statutory cause of action for serious invasions of privacy should be introduced, and
>
> (c) any other related matter.

The Government welcomes the opportunity to provide a submission to this inquiry and notes that the Committee has indicated that it is particularly interested in examining the impacts of the recent trend of people experiencing serious privacy invasions facilitated by technology such as the use of revenge pornography and the use of drones (remote piloted aircraft).

In considering the issues, the Government asks that the Committee consider all perspectives including the findings of previous reviews of the law in this area. It is important to ensure a balanced approach to this issue, and consider the context of the operation of laws applying to privacy generally and concerns for the protection of individual privacy. The Government asks that the Committee consider that a range of solutions may be necessary to properly respond to the issues of privacy invasion that are raised by modern technology. The introduction of a statutory cause of action may be contentious if implemented without careful consideration of the potential ramifications, including the potential for forum shopping.

This submission is structured in line with the terms of reference. The intent of this submission is to provide the Committee with an outline of the relevant laws and NSW Government policies currently in place as well as to provide insight into some of the issues that would need to be considered in connection with a statutory cause of action for invasion of privacy.

The Government is aware of community concern and a range of circumstances in which technology may be facilitating increased privacy concerns and where the existing law faces challenges in dealing with the issues raised,

Terms of reference

(a) the adequacy of existing remedies for serious invasions of privacy, including the equitable action of breach of confidence

Current privacy laws and remedies for invasions of privacy in Australia and in NSW

Details of the laws and remedies for invasions of privacy in Australian and in NSW have been exhaustively examined and set out in recent reports by a number of law reform commissions including the ALRC, NSW Law Reform Commission (NSWLRC) and the Victorian Law Reform Commission (VLRC). In addition, in the context of the current inquiry, a paper has recently been published by the NSW Parliamentary Research Service: *Revenge pornography, privacy and the law*, outlining the role of the criminal law in respect to revenge pornography and commenting on the adequacy of existing civil law remedies for serious invasions of privacy by means of revenge pornography, including the equitable action of breach of confidence. The Commonwealth Government also recently published a report on privacy and technology in 2014: *Eyes in the sky*, as a result of a Commonwealth parliamentary inquiry into drones and the regulation of air safety and privacy.

For the purpose of this submission, a brief summary of the current privacy laws and remedies available at common law, the remedies available under the *Privacy and Personal Information Protection Act 1998*, and the relevant criminal offences provisions, is outlined in the sections below.

Remedies for invasions of privacy at common law

A common law tort for invasion of privacy has not yet developed in Australia, despite the High Court leaving open the possibility of such a development in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199[1]. Since this time, as the ALRC noted in 2014, a tort of invasion of privacy has been recognised only in two lower court decisions - *Grosse v Purvis* [2003] QDC 151 in the District Court of Queensland and *Doe v Australian Broadcasting Corporation* [2007] VCC 281 in the County Court of Victoria. Both these cases were settled before appeals by the respective defendants were heard.[2].

The ALRC has outlined other existing causes of action in Australian law that may cover some circumstances of invasions of privacy:

- The torts of trespass to the person and trespass to land provide some protection against unauthorised interference with a person's body or intrusions into property.[3] Intrusions into airspace may amount to trespass to land if the intrusion

[1] Page 23, ALRC report *Serious Invasions of Privacy in the Digital Era* (2014): https://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_123_whole_report.pdf

[2] Ibid, page 53-54

[3] Ibid, page 48

is at a height that is potentially necessary for the ordinary use and enjoyment of the occupier.[4]

- The tort of nuisance may cover surveillance from outside a property where there is an unreasonable interference with an occupier's use and enjoyment of their land.[5]

- The tort of defamation covers defamatory publications to a third party. However, the truth of a defamatory statement is now a complete defence, limiting its use as a protection of privacy.[6]

- The tort of breach of confidence can be used to prevent the misuse or disclosure of confidential information, including in some cases personal details imparted in a close personal relationship.[7] However, the ALRC noted in its report there is some uncertainty about whether compensation for emotional distress, which does not qualify as a psychiatric illness, would be available.[8]

The privacy protections under the *Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act)*

The PPIP Act applies to NSW public sector agencies. Under section 36 of the PPIP Act the Privacy Commissioner has a general power to receive, investigate and conciliate complaints about privacy related matters. However, any complaint must be resolved by conciliation. In relation to action for monetary compensation, the PPIP Act provides for the power of the Civil and Administrative Tribunal to review the conduct of agencies under Part 5 of that Act (contravening a privacy protection principle, code of practice or disclosure of information kept in a public register) and to pay to the applicant damages up to $40,000 by way of compensation for any loss or damage suffered because of the agency's conduct. The application for damages can only be made after the conduct has been internally reviewed by the agency.[9]

Civil liability exemptions are set out in section 66A(2) of the PPIP Act, which provides that if a public sector agency provides an individual with access to personal information under the Act, and the access was required by section 14 (Access to personal information held by agencies), or an employee, officer or agent of the public sector agency believed in good faith that the access was required by that section, no action for defamation or breach of confidence lies against the public sector agency or employee or agent, and that no action lies against the person who provided the information to the agency in respect of any publication involved in or resulting from access being given.

The PPIP Act also sets out certain exemptions from compliance with information protection principles by law enforcement agencies and other public sector agencies for law enforcement purposes in section 23, and exemptions relating to investigative agencies in section 24.

---

[4] Ibid, page 49

[5] Ibid, page 48

[6] Ibid, page 50

[7] Ibid, page 50

[8] Ibid, pages 26 and 51

[9] Part 5 *Privacy and Personal Information Protection Act 1998*; page 16, NSW LRC report *Invasion of Privacy* (2009): http://www.lawreform.justice.nsw.gov.au/Documents/report_120.pdf

The PPIP Act also provides in section 62 that a public sector official must not, otherwise than in connection with the lawful exercise of his or her official functions, intentionally disclose or use any personal information about another person to which they have had access via their official functions. The penalty for breaching this is up to 100 penalty units or imprisonment for 2 years or both.

Commonwealth privacy laws

The *Privacy Act 1988* (Cth) sets out privacy protections for the collection, use, disclosure and other handling of personal information by certain entities, including Australian Government agencies, large private sector organisations with a turnover of more than $3 million and some small businesses such as health service providers[10]. Individuals, however, are not bound by the *Privacy Act 1988* (Cth).

Invasions of privacy that are also criminal offences

In addition to a person affected seeking compensatory relief for the harm caused by an invasion of privacy, some invasions of privacy including those facilitated by technology could also be prosecuted as criminal offences. Summaries of the relevant criminal offences in NSW and the adequacy of criminal laws generally to deal with technology-facilitated invasions of privacy.

Existing criminal offences in NSW that relate to technology-facilitated abuse

Crimes (Domestic and Personal Violence) Act 2007

The *Crimes (Domestic and Personal Violence) Act 2007* (the CDPV Act) is a stand-alone Act for apprehended violence orders (AVO). There are two types of AVO: an apprehended domestic violence order (ADVO) and an apprehended personal violence order (APVO). A court may make an ADVO where it is satisfied that a person who has, or has had, a domestic relationship with another person, has reasonable grounds to fear and does in fact fear the commission of a personal violence offence, or intimidating conduct. A court may make an APVO where it is satisfied a person has reasonable grounds to fear, and does in fact fear, the commission of a personal violence offence or intimidating conduct and the people involved are not related and do not have a domestic relationship. AVOs prohibit defendants from engaging in certain kinds of behaviour, including that which would constitute technology-facilitated stalking and abuse. AVOs contain mandatory conditions not to assault, molest, harass, intimidate, stalk or otherwise interfere with a person in need of protection (or 'PINOP'). The court may include additional conditions, including that the defendant not contact or approach the PINOP. While an AVO application itself is not a criminal proceeding, it is a criminal offence to breach any of the conditions of an AVO pursuant to section 14 of the CDPV Act.

The CDPV Act nominates 55 'personal violence offences' and provides that a personal violence offence is a 'domestic violence offence' for the purposes of the CDPV Act. NSW is the only jurisdiction that prescribes domestic violence-related offences in this way. These personal violence offences carry maximum penalties of up to life imprisonment and standard non-parole periods of up to 20 years. On conviction they will be recorded as domestic violence offences (with a 'DV' annotation). This ensures that courts know of

[10] Page 23, ALRC report *Serious Invasions of Privacy in the Digital Era* (2014): https://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_123_whole_report.pdf

all prior DV offending when considering ADVO applications, bail or sentencing offenders for breaches of orders or relevant offences.

Section 14 of the CDPV Act creates the offence of knowingly contravening an AVO. It provides that a breach committed through an act of violence must result in a sentence of imprisonment unless the court otherwise orders (although this does not apply to juveniles). The maximum penalty is two years imprisonment and/or a fine of $5,000.

The CDPV Act also has a separate offence of stalking/intimidation with the intention of, or being reckless to, causing fear of physical or mental harm. The offence carries a maximum penalty of five years imprisonment or 50 penalty units or both (s 13(1)). The prosecution does not need to prove the victim actually felt fear and courts are specifically directed to consider patterns of conduct. The offence of stalking applies to technology-facilitated abuse insofar as it relates to the following of a person about, or the watching or frequenting the vicinity of, or an approach to, a person's place of residence, business or work or any other place the person frequents for the purposes of any social or leisure activity. The offence of intimidation more widely applies to technology-facilitated abuse and includes:

- Conduct amounting to harassment or molestation of a person.
- Publishing or threatening to publish revenge pornography.
- An approach made to the person by any means (including by telephone, telephone text messaging, e-mailing and other technologically assisted means) that causes the person to fear for his or her safety.
- Any conduct that causes a reasonable apprehension of injury to a person or to a person with whom he or she has a domestic relationship, or of violence or damage to any person or property.

The offence of intimidation is the most common offence used in relation to technology-facilitated abuse, due to its wide application to a range of offender behaviours. Its flexibility stems from the fact that it is directed towards what the accused intended, or was reckless to, rather than any particular act or impact on the victim so that the use of technology, or any tool, to achieve this aim will be covered.

Surveillance Devices Act 2007

The use of surveillance devices in NSW is governed by the *Surveillance Devices Act 2007* (the SD Act). The principal objective of the SD Act is to regulate the installation, use, maintenance and retrieval of surveillance devices. Surveillance devices may be used in the context of domestic and personal violence, including listening, optical surveillance and GPS tracking devices to spy on and stalk the victim.

The devices currently regulated by the SD Act are listening devices, optical surveillance devices, data surveillance devices and tracking devices. The SD Act prohibits, subject to limited exceptions, the use of devices without a warrant or authorisation issued to a law enforcement officer or otherwise in accordance with Commonwealth law. The use of a device by any person in contravention of the SD Act is a criminal offence. The relevant offences in the SD Act are the prohibition on installation, use and maintenance of listening devices (s7); and prohibition on installation, use and maintenance of tracking devices (s9).

Crimes Act 1900

The *Crimes Act 1900* (Crimes Act) contains a number of offences that target specific behaviours relating to technology-facilitated stalking and abuse. These include:

- Sending documents containing threats (s31)
- Sexting (s91H(2))
- Voyeurism (s91J)
- Filming a person engaged in a private act (s91K)
- Filming a person's private parts (s91L)
- Installing a device to facilitate observation or filming (s91M)
- Publishing indecent articles (s578C).

The NSW legislation takes a flexible approach. For example, 'filming' could include the dissemination of moving or still images to a third party without the victim's consent.

Laws that apply to "sexting" in NSW

In NSW, people who engage in 'sexting' (sending intimate images or videos by text message) may commit an offence against s 91H(2) of the Crimes Act where the conduct involves producing, disseminating or possessing a sexual image of a person under 16 years. People who 'sext' may also commit an offence under the Commonwealth Criminal Code, where the conduct involves sending or receiving by internet or phone a sexual image of a person under 18 years. However, the consent of the Commonwealth Attorney-General is required to commence proceedings against a person who was under 18 at the time of the offence.[11]

The consequences of being convicted for a child pornography offence (state or Commonwealth) include registration on the Child Protection Register. However, a minor who commits a single offence relating to child abuse material will not be registered for this reason alone.

Powers to investigate and prosecute invasions of privacy via social media

Existing State and Commonwealth laws enable Police to prosecute for a range of offences relating to serious invasions of privacy by a person publishing or posting naked or sexually explicit pictures or videos of another person. The NSW Police Force have a range of challenges when prosecuting for serious invasions of privacy by digital means. Issues with prosecuting privacy invasions include:

[11] Part 10.6 of the *Criminal Code Act 1995* (Cth) deals with offences about telecommunications services. For the purpose of the Inquiry, the relevant sections are section 474.17 Using a carriage service to menace, harass or cause offence which carries a maximum three year sentence, and section 474.19 Using a carriage service for child pornography which carries a maximum 15 year sentence. 'Child pornography material' is about people who are or appear to be under 18 years of age.

- In any matter involving images or videos being published to a social media site (e.g. Facebook), an online bulletin board site such as Reddit, or various ‘revenge porn’ sites, a user may operate under an alias, rendering identification an issue.

- There is also the difficulty in proving that a particular person uploaded the material, for example where the device used may not be in their exclusive control (e.g. a personal computer in a shared household).

Computers and related devices can be seized under a search warrant, and a portable device such as a smartphone or tablet can be seized from a person, provided that in either case the officer has reasonable grounds to suspect that the thing may provide evidence of the commission of a relevant (indictable) offence. However, the power to obtain search warrants is limited to indictable offences. Some of the offences outlined above, such as publishing an indecent article are summary offences so the options of seizing the device via search warrant or from a person are not available.

Further, if a device is password protected, police officers have no power to compel a person to disclose the password. Images and videos may be stored ‘in the cloud’ rather than on the device, and there is no power to compel a person to provide access to the website where the file is stored either.

Terms of reference

(b) whether a statutory cause of action for serious invasions of privacy should be introduced

Recent law reform work on the question of introducing a statutory cause of action for serious invasion of privacy

As there is no recognised cause of action at common law for serious invasion of privacy in Australian law, the proposal to introduce a statutory cause of action for serious invasion of privacy has been canvassed in detail by several law reform commissions in recent years:

- NSWLRC report *Invasion of Privacy* (2009)
- ALRC report *For your information: Australian Privacy Law and Practice* (2010)
- VLRC report *Surveillance in Public Places* (2010)
- ALRC report *Serious Invasions of Privacy in the Digital Era* (2014)

The Commissions in all of the above reports have made recommendations for the introduction of a statutory cause of action for breach of privacy (whether through State or Commonwealth legislation), with some variances in the proposed form and scope (for example, the VLRC recommended the introduction of two statutory causes of action – one regarding misuse of private information and a second regarding intrusion upon seclusion).

Further, the Commonwealth Government released a report on privacy and technology issues in 2014: *Eyes in the sky*, as a result of a Commonwealth parliamentary inquiry into drones and the regulation of air safety and privacy. The report made recommendations about privacy regulation, including that the introduction of a statutory cause of action similar to the one proposed by the ALRC be considered to provide protection against privacy-invasive technologies such as drones.

In 2013 the Law Reform Institute of South Australia initiated an inquiry into whether or not South Australia should enact a statutory cause of action for invasion of privacy. The final report is anticipated at the end of 2015. In 2014, on the introduction of new privacy laws under the *Information Privacy Act 2014* (ACT) it was announced that the ACT Government would consider the ALRC report before making a decision on options for the adoption of a statutory cause of action for serious invasions of privacy in the ACT.

Developments internationally

Many other common law jurisdictions have recognised a right to sue for invasion of privacy and as a result have not sought to introduce a statutory cause of action. For example, in the UK, New Zealand, Canada and the United States there are civil causes of action for serious invasions of privacy. The ALRC's 2014 report notes that 'although committees in the UK and New Zealand have recommended against the introduction of

a statutory cause of action, this must be seen in light of the significant and recent developments in the common law in those two countries'.[12]

The need for consistency in approach across Australian jurisdictions

Were NSW to unilaterally introduce a statutory cause of action this would be likely to give rise to a number of issues. For example, the ALRC and NSWLRC reports noted the issues of:

- the possibility of forum shopping
- the potential for increased costs and other burdens on organisations operating across jurisdictional borders, where different laws apply, and
- the non-jurisdictional nature of invasions of privacy via the use of technology.[13]

To achieve uniformity nationally, it would be necessary to first resolve the issue of the approach to implementation of a statutory cause of action. There are a range of solutions proposed by different Law Reform Commissions. Two different approaches were proposed by the ALRC and the NSWLRC. A comparison is attached at Appendix A. The ALRC recommended (in 2010 and 2014 reports) that a statutory cause of action be introduced through federal legislation, while the NSWLRC advocated an approach where the states and territories each enact a model bill developed by the NSWLRC. The NSWLRC recognised that this approach would require agreement between all the jurisdictions on the terms of the legislation, and then for them to enact 'substantially uniform' legislation. There would also need to be an agreed mechanism to make future amendments in order to maintain uniformity between the jurisdictions.

Differences in statutory causes of action proposed by ALRC and NSWLRC

The ALRC and NSWLRC have proposed slightly different tests for establishing a breach of privacy, with the ALRC arguably setting a slightly higher threshold than the NSWLRC's proposed model.

Both ALRC and NSWLRC models incorporate matters of public interest into the evaluation of whether a person's privacy has been invaded. The NSWLRC stated that that:

> 'legal principle requires that plaintiffs bear the onus of establishing their case. It is appropriate…that, as part of establishing an invasion of privacy, plaintiffs should demonstrate at the outset that their claim to privacy is not outweighed by a competing public interest.[14]

[12] Page 22, *ALRC Invasions of privacy in the digital era* (2014) https://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_123_whole_report.pdf

[13] Page 72, NSW Law Reform Commission report *Invasion of privacy* (2009) http://www.lawreform.justice.nsw.gov.au/Documents/report_120.pdf

[14] Page 33, NSWLRC *Invasion of privacy* (2009) http://www.lawreform.justice.nsw.gov.au/Documents/report_120.pdf

In contrast, the VLRC report in 2010 proposed that public interest be a defence 'where the defendant's conduct was in the public interest, or if involving a publication, the publication was privileged or fair comment'.[15]

Implementing a statutory cause of action in NSW – other issues to be considered

In addition to settling the substance of a statutory cause of action for serious invasion of privacy, it is necessary to consider and resolve how such a cause of action would interact with a variety of existing state and Commonwealth laws.

For example:

- The interaction with defamation law would need to be considered to ensure that there was no inconsistency and that a plaintiff was not prevented from bringing a cause of action that would be more appropriately brought under the other cause of action.

- NSW passed journalist shield laws in 2011 with the *Evidence Amendment (Journalist Privilege) Act 2011*. These amendments protect journalists from being forced to reveal the identity of sources in court, subject to certain exceptions. It will be necessary to consider the intersection between these two laws, given that a journalist's source may be an appropriate defendant for a breach of privacy action. Consideration would therefore need to be given to the appropriate balance to strike between privacy and the freedom and independence of the press.

- It would be necessary to consider which courts should hear such claims and what procedures would apply. For example consideration will be required regarding whether hearings would need to be in closed court and whether non-publication orders would be necessary.

Impact of a statutory cause of action on law enforcement or investigative functions

A statutory cause of action may impact on the ability of law enforcement agencies to operate, as well as affecting other regulatory or investigative functions carried out by government agencies. Consideration should be given to the incorporation of a specific defence of law enforcement purposes in any statutory cause of action, similar in effect to the law enforcement exclusions outlined in section 27 of the PPIP Act. There is concern that Police officers should not be liable for any actions that arise in the course of their official functions, except where actions are connected to their administrative and educative functions. Consideration should also be given to whether a plaintiff should be required to show that their right to privacy outweighs any countervailing rights or public interests. In this respect, the statutory cause of action proposed by both the ALRC and NSWLRC appear to include factors that would take these matters into account e.g. the defence of lawful conduct and the public interest test.

Similarly, the consideration should be given to whether, if a statutory action was to apply to the use of surveillance drones, there would need to be provision for exclusion of

[15] Page 18, VLRC report *Surveillance in public places* (2014) http://www.lawreform.vic.gov.au/sites/default/files/Surveillance_final_report.pdf

government agencies carrying out investigative and enforcement activities similar to the exclusions in the PPIP Act, to make provision for the use of drones being used to investigate mining activities and the clearing of native vegetation.

It should also be noted that the secrecy provisions in the *Taxation Administration Act 1996* and the *Fines Act 1996*, and the provisions in the PPIP Act, currently permit the Office of State Revenue to use information for the purposes of administering or executing those Acts. The Commissioner of Fines Administration is currently authorised to access data held by other government agencies and credit reference agencies. The Commissioner also has a broad authority to disclose data in connection to the enforcement of fines. Any statutory cause of action could result in limits on government access to data beyond that which is currently permitted in legislation.

Appendix A

Differences between the models proposed by ALRC and NSWLRC for a statutory cause of action are summarised in the table below.

Elements and defences	Proposal by ALRC (2014)	Proposal by NSWLRC (2009)
Nature of cause of action	Action in tort.	Not an action in tort. Not constrained by rules and principles that apply in tort law. To the extent that the general law recognises a specific tort for the invasion of a person's privacy it should be abolished by the statutory cause of action.
Damage caused by defendant	The privacy invasion need not cause actual damage.	Remains silent on the specification of requirement to show damage or fault – leave this to development in case law.
Reasonable expectation of privacy	It must be proved that a person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances.	There are facts in respect of which, in all the circumstances, there is a reasonable expectation of privacy.
Circumstances of invasion of privacy	The invasion of privacy must be either by intrusion into seclusion (intrusion into a person's physical private space) or by misuse of private information.	Generally intended to cover invasions of privacy: - where the defendant has disclosed private information about the plaintiff (information privacy) - the defendant has intruded on the plaintiff's solitude, seclusion, or private affairs (seclusion)
Public interest test	For the plaintiff to have a cause of action, the court must be satisfied that the public interest in privacy outweighs any countervailing public interest.	That the claim to protection of privacy is not outweighed by some other competing public interest.
Seriousness	The invasion must be serious, having regard among other things to: (a) the degree of any offence, distress or harm to dignity that the invasion of privacy was likely to cause to a person of ordinary sensibilities in the position of the plaintiff; and (b) whether the defendant was motivated by malice or knew the invasion of privacy was likely to offend, distress or harm the dignity of the plaintiff	Not confined to 'serious' invasions of privacy - general cause of action for invasions of privacy. Generally intended to cover invasions of privacy: - where the defendant has disclosed private information about the plaintiff (information privacy) - the defendant has intruded on the plaintiff's solitude, seclusion, or private affairs (seclusion)

Intention of the defendant	The invasion of privacy must be intentional or reckless.	Covers unintentional invasions of privacy. As it is not an action in tort, it is unnecessary to specify for the purposes of the cause of action whether or not the conduct of the defendant that invades the plaintiff's privacy must be intentional.
Consent	Consent is a defence (see below).	A plaintiff cannot succeed in an action for invasion of privacy if the plaintiff has consented to the defendant's conduct. Consent may be express or implied.
Defences	Defences are: - lawful authority to protect defendants from liability under the new privacy tort where their conduct was required or authorised by law; - conduct incidental to the exercise of a lawful right of defence of persons or property, where that conduct was proportionate, necessary and reasonable, and where the defendant reasonably believed that the conduct was necessary to protect persons or property; - necessity where a defendant acts in a reasonable belief that they were preventing an imminent and greater harm; and - consent including express and implied consent	Defences are: - required or authorised by or under law; or - done in lawful defence of person or property (not necessarily being "authorised" or "required" by or under law); or - the publication of matter that would attract certain defamation defences; or - the publication of matter where, as between the defendant publisher and the recipient of the information, there is a common interest or duty in giving and receiving information on the subject in question
Cap on compensation payable	The cap on damages for both non-economic loss and any exemplary damages should not exceed the cap on damages for non-economic loss in defamation which is currently $376,500 (section 35 of the *Defamation Act 2005*).	A cap on compensation payable for non-economic loss should be set at $150,000.