

Submission by the
Office of the Information Commissioner

SERIOUS INVASIONS OF PRIVACY IN THE DIGITAL ERA
Australian Law Reform Commission Issues Paper

November 2013

The Queensland Office of the Information Commissioner is an independent statutory authority. This submission does not represent the views or opinions of the Queensland Government.

The Office of the Information Commissioner (Queensland) (**OIC**) generally supports measures strengthening protections against abuses of privacy, particularly where inadequacies with the existing regulatory framework are identified. In principle, OIC supports the introduction of a statutory cause of action for privacy.

Queensland has a statutory scheme under which an individual can seek compensation or remedies for a breach of their privacy by a public authority (see detail following). OIC recognises that the rapid growth in the commoditisation of 'personal information' and the ease with which that information can be obtained, used and disseminated has exposed individuals to new privacy risks or exacerbated existing risks to the point where the adequacy of protections needs consideration.

In general terms, OIC considers that the Queensland's statutory regime for privacy grievances works well in practice and that the principles of this regime would translate well to a broader statutory cause of action.

Queensland privacy law

On 1 July 2009 Queensland enacted the *Information Privacy Act 2009 (IP Act)*. The IP Act regulates how 'government agencies' collect, store, use and disclose 'personal information' through obligations to comply with 'privacy principles' consisting of:

- Information Privacy Principles (**IPP**) – for all government agencies other than health agencies; or
- National Privacy Principles – for health agencies including Queensland Health
- provisions dealing with service providers contracted to government agencies; and
- provisions dealing the transfer of personal information outside Australia.

Government agencies include Ministers, Queensland Government departments, local government and public authorities. The IP Act does not apply to Government Owned Corporations (**GOCs**), individuals, the private sector or community organisations. Queensland GOCs, the private and community sector could be covered under the Commonwealth's privacy legislation if these entities have an annual turnover of more than \$3 million per annum. Additionally, there is a measure of privacy protection in Queensland's criminal code¹, through the common laws of nuisance and trespass and for recorded conversation².

If an individual – who need not be a Queensland citizen - considers that a Queensland Government agency has failed to comply with its obligations under the privacy principles, they are able to make a formal complaint concerning the alleged privacy breach. While the IP Act strongly provides the opportunity for the individual and the relevant government agency to settle the subject matter of the complaint between themselves, ultimately the privacy complaint can be referred to the Queensland Civil and Administrative Tribunal (**QCAT**) for its determination and orders. QCAT orders are remedial in nature; there is no capacity for it to order punitive measures.

1. Section 227A of the Criminal Code renders some observations or visual recording 'in circumstances where a reasonable adult would expect to be afforded privacy' a misdemeanour punishable by up to two years imprisonment.

2 *Invasion of Privacy Act 1971* (Qld).

There is the capacity for QCAT to award an individual up to a maximum of \$100,000 in compensatory damages which can include non-economic loss.

In summary, Queensland has a statutory cause of action for privacy breach in respect of Queensland State Government agencies only. This submission will largely put forward OIC's position that Queensland's statutory scheme can be readily adapted to a broader statutory cause of action system.

1. What guiding principles would best inform the ALRC's approach to the Inquiry and, in particular, the design of a statutory cause of action for serious invasion of privacy? What values and interests should be balanced with the protection of privacy?

OIC considers that the right to an effective and enforceable remedy should be a key guiding principle in the design of a statutory cause of action for serious invasion of privacy. The remedy should be able to be achieved in a user-friendly, non-adversarial environment with the minimum of cost and formality.

OIC acknowledges that privacy is not an absolute value which necessarily takes precedence over other values and interests and acknowledges the range of values, freedoms and matters of public interest identified in the Issues paper. Acknowledgement of these other public interests includes acceptance that no single public interest is absolute.

However, as noted in earlier ALRC reports on this issue, a statutory cause of action would provide an opportunity to ensure that the appropriate balance is struck between the public interests in protection of privacy and other public interests.

2. What specific types of activities should a statutory cause of action for serious invasion of privacy prevent or redress? The ALRC is particularly interested in examples of activities that the law may not already adequately prevent or redress.

Privacy is universally defined in its absence rather than its presence. To adapt a familiar adage – 'I don't know what privacy is but I know when I don't have it.' Consistent with this, the IP Act uses the word 'privacy' 425 times but nowhere is the term itself defined.

Under Queensland's IP Act, government agencies have obligations to comply with privacy principles in their dealings with personal information. Individuals have the option of seeking redress if an act or practice in relation to the individual's personal information is a breach of these obligations.

The privacy principles do not impede the legitimate collection, use and disclosure of personal information. Rather, a privacy breach is interpreted as being a misuse or abuse of an individual's personal information.

There are a broad range of flexibilities, exceptions and exemptions which allow these legitimate dealings. Some of these apply to agencies as a whole, some apply to specific classes of information; others apply to specific functions and/or activities of certain agencies – for example, the judicial functions of courts and tribunals.

Many of the exemptions recognise competing public interests such as public health and safety or the efficient administration of law enforcement activities.

OIC considers that a similar approach be taken in respect of statutory cause of action. Rather than defining where and when a statutory cause of action may apply, the starting point is that individuals have the in-principle right to an effective remedy if they experience a serious invasion of privacy but that right is then tempered by exceptions and exemptions which reflect relevant competing public interest considerations.

3. What specific types of activities should the ALRC ensure are not unduly restricted by a statutory cause of action for serious invasion of privacy?

Consistent with the above approach, OIC acknowledges that certain activities or functions of agencies could be excluded from the ambit of any proposed cause of action, for example – courts and tribunals.

While OIC is of the opinion that in general, organisations should not have blanket exemptions, OIC also accepts that a cause of action would not apply to limited specialist bodies such as Commissions of Inquiry.

4. Should an Act that provides for a cause of action for serious invasion of privacy (the Act) include a list of examples of invasions of privacy that may fall within the cause of action. If so, what should the list include?

Yes - however any list should be non- exhaustive.

The examples provided in the Issues Paper appear appropriate; however, OIC suggests that a further example for consideration is appropriation of another person's name or likeness.

Further, OIC suggests that where terms have a distinct use and meaning in privacy law, that those terms be the subject of illustrative examples of the types of invasions that fall within the cause of action.

5. What, if any, benefit would there be in enacting separate causes of action for:

- misuse of private information; and*
- intrusion upon seclusion?*

There are many different types of privacy. The IP Act is concerned with privacy of information only. Misuse or the non-legitimate use of personal information is covered under the IP Act in relation to acts by 'government agencies'³. The right to seclusion or 'the right to be left alone' can involve restraints on collection, use and disclosure of an individual's personal information as covered in the IP Act.

³ Government agencies are defined as Ministers, Department, local government and public authorities (including the Office of the Information Commissioner).

If this concept were to be extended to physical privacy, there are overlaps with the common law of trespass (and as applicable - nuisance). To the extent the right to seclusion needed to be more encompassing in its application OIC considers that there would be benefit in enacting separate causes of action.

6. What should be the test for actionability of a serious invasion of privacy? For example, should an invasion be actionable only where there exists a 'reasonable expectation of privacy'? What, if any, additional test should there be to establish a serious invasion of privacy?

The effects of a privacy breach on an individual will vary according to the individual circumstance. An individual may feel very comfortable expressing their sexual preference amongst their close friends while simultaneously they may be reluctant to do so among family or in their workplace. This is an individual's right of choice and it should remain so.

However, OIC recognises that a truly subjective test of privacy would be unworkable in practice. While many people would be 'accepting' of the fact that public spaces are subject to camera surveillance, there will always be some people who consider that their lawful social actions should not be monitored or recorded.

OIC considers the objective test of 'reasonable expectation of privacy' would reflect both community standards and provide sufficient flexibility for modern range of social discourses. For example, while a reasonable person would accept their actions and movement to be subject to CCTV surveillance in public spaces they would not necessarily accept those images to be disseminated to the wider public for the purposes of public entertainment.

Similarly, individuals with a high public profile would have a lesser expectation of privacy than the average citizen when they are in public and thus they would expect that their activities would be publicised to a greater degree. However, they would be similarly entitled to expect a degree of privacy in their personal lives.

OIC considers that once a reasonable expectation of privacy is established, then a breach of that privacy is a breach. Any determination on the seriousness of the breach could be addressed in the question of damages.

7. How should competing public interests be taken into account in a statutory cause of action? For example, should the Act provide that:

- competing public interests must be considered when determining whether there has been a serious invasion of privacy; or*
- public interest is a defence to the statutory cause of action?*

Queensland's IP Act and the *Right to Information Act 2009* (Qld) (**RTI Act**) give a right of access to information in the government's possession or under the government's control unless, on balance, it is contrary to public interest to give the access. Both Acts set out a public interest balancing test which sets out how competing public interest factors should be compared and considered when

making a decision about whether allow or refuse access to information. In the IP Act, the right to privacy is generally stated but there are qualified permissions that apply. Sometimes the qualifier is a vague term – ‘reasonable efforts to’; other times the qualifier is more definite – ‘the disclosure is authorised or required under a law’. The effect of the qualifier is that if its conditions are met there is no privacy breach.

In a QCAT hearing, the distinction between determination of privacy breach and defence of a privacy breach are indistinguishable in terms of determination of liability. The applicant has the onus of establishing that their privacy has been breached by the relevant government agency while it provides as its ‘defence’ that its actions fell within the relevant qualifier.

If a breach is established, the government agency becomes liable for all damages that flow from that breach.

This is consistent with the view that the right to privacy is a public interest that must be balanced against other public interests and that these will vary according to individual circumstance.

OIC suggests that this approach be applied to the statutory cause of action. OIC considers that where an action has been taken by an entity because of its reliance on a countervailing public interest, that entity would argue that in these circumstances, there is no serious breach of the affected individual’s privacy.

8. What guidance, if any, should the Act provide on the meaning of ‘public interest’?

The term ‘public interest’ is not defined in Queensland’s RTI Act or the IP Act, with the RTI Act providing a non-exclusive list of a broad range of consideration comprising the public interest. These Acts recognise that there are range of public interests, that these will apply to differing degrees according to circumstance and that the concept of what constitutes a public is neither static nor closed.

The concept that ‘the categories of public interests are not closed’ is also built into the IP Act. There is the capacity for the Information Commissioner to give an approval waiving or modifying an agency’s obligations to comply with the privacy principles if the public interest in waiver outweighs the public interest in compliance. This capacity recognises that from time to time, novel public interests considerations will arise that do not fit into the existing ‘public interest permissions’ available in the privacy principles.

In general terms, a public interest consideration is one which is common to all members of, or a substantial segment of, the community albeit that the consideration can apply to individual cases.

The OIC considers that the benefits of having a fluid definition of ‘public interest’ is that it can operate as a touch-stone of factors affecting the good order and functioning of the community and government affairs and of the well-being of citizens generally.

Accordingly, OIC’s position is that public interest should not be strictly defined in any proposed legislation but should allow the flexibility and fluidity necessary to reflect changing community norms.

9. Should the cause of action be confined to intentional or reckless invasions of privacy, or should it also be available for negligent invasions of privacy?

It is OIC's experience that many privacy breaches are neither intentional nor reckless. They can occur for reasons such as reliance on an out-dated process, thoughtlessness or even misguided benevolence – a medical practitioner may pass on sensitive medical information about a patient to their family with the anticipation this will enable them to assist in the patient's care.

If it is not intended that the cause of action include a punitive component, then the motivation of the perpetrator is an irrelevant consideration.

Ultimately, it is the individual whose personal information has been abused or misused who suffers the primary damage. OIC considers that the focus should be on the damage and its potential remedy rather than the motivation of perpetrator. The damage suffered by reason of good intent is every bit as real as that suffered by reasons of malice or wilful negligence.

There is often a reasonableness component to privacy. OIC suggests that the issue as to whether reasonable actions were taken to avert or minimise the privacy breach would, in some cases, form a complete defence to a claim of privacy breach or in other cases go towards mitigation of damages.

Accordingly if it were the case that an entity failed to take reasonable action to protect someone's privacy, then an action for negligent invasion of privacy should be able to be pursued.

It is not clear whether the proposed cause of action will lie against an individual or if the individual is an employee, against the employer or both. If both, one of the relevant factors that should be considered is the actions taken by the employer to prevent the breach of privacy – in essence, the now well-established defences to vicarious liability. OIC submits a specific reference to where liability ultimately lies should be incorporated in any statutory cause of action scheme.

10. Should a statutory cause of action for serious invasion of privacy require proof of damage or be actionable per se?

OIC notes that the ALRC has previously recommended that a statutory cause of action for invasions of privacy should be actionable without proof of damage and that invasions of privacy may result in distress, humiliation and insult that fall short of provable damage.

However, OIC submits the applicant should provide proof of damage given that orders arising out of a statutory cause of action are remedial in nature.

QCAT has the option to make an award of damages in privacy matters for 'pain and suffering, hurt and humiliation'. OIC acknowledges that for privacy, the damage suffered would often be non-pecuniary in nature and the quantification of these damages is problematic. However, this is a factor faced and dealt with in a number of jurisdictions include discrimination, general negligence (nervous shock) and personal injury.

11. How should damage be defined for the purpose of a statutory cause of action for serious invasion of privacy? Should the definition of damage include emotional distress (not amounting to a recognised psychiatric illness)?

OIC considers that the definition of damage should include the suffering of humiliation or emotional distress as category of damages. In practice, this will invariably be the only or most significant damage experienced as a consequence of privacy breach.

Queensland's IP Act provides that a complainant is entitled to a stated amount of not more than \$100,000 to compensate the complainant for loss or damage, including for any injury to the complainant's feelings or humiliation suffered by the complainant.

12. In any defence to a statutory cause of action that the conduct was authorised or required by law or incidental to the exercise of a lawful right of defence of persons or property, should there be a requirement that the act or conduct was proportionate, or necessary and reasonable?

OIC considers that the focus should not be on whether there is a justifiable breach, but whether there is a breach of the right to privacy in itself.

There are reasonable components built into privacy principles to provide exemptions that allow an agency flexibility of use for exigent circumstances, such use or disclosure for law enforcement or public health and safety.

13. What, if any, defences similar to those to defamation should be available for a statutory cause of action for serious invasion of privacy?

OIC is of the opinion that it would be inappropriate for defences similar to those available for defamation to be included as defences to a statutory cause of action for serious invasion of privacy.

Defamation occurs where one person communicates, by words, photographs, video, illustrations or other means, material which has the effect or tendency of damaging the reputation of another.

While privacy has identification of the individual as a common core component to defamation, it is otherwise a wholly different concept. Defamation concerns 'publication' only whereas privacy incorporates controls over the collection, storage, access and amendment and secondary use of personal information as well as its disclosure.

Also, privacy is concerned with an entity's dealings with personal information and the quality and more pertinently, the veracity of the information is irrelevant. The definition of personal information includes incorrect information about an individual.

OIC acknowledges that judicial pronouncement of the impact of the publication of defamatory material and the corresponding awards of damages would provide useful guidance for the statutory cause of action jurisdiction.

14. What, if any, other defences should there be to a statutory cause of action for serious invasion of privacy?

The Queensland system does not have 'defences' for a privacy breach. Rather, it defines a breach as occurring in the absence of qualifying permissions. That is, the 'defences' are built into the breach offense.

OIC notes that in practice, this provides both flexibility of practice and ease of understanding.

15. What, if any, activities or types of activities should be exempt from a statutory cause of action for serious invasion of privacy?

Please refer to OIC's response to Question 3.

16. Should the Act provide for any or all of the following for a serious invasion of privacy:

- *a maximum award of damages;*
- *a maximum award of damages for non-economic loss;*
- *exemplary damages;*
- *assessment of damages based on a calculation of a notional licence fee;*
- *an account of profits?*

It is common in privacy regimes to have a cap on the damages available to compensate an individual for loss or damage suffered by the individual because of the act or practice that was a breach of the entity's obligation under the relevant legislation.

OIC submits that because the circumstances of each breach will be individual and the damages suffered as a consequence of the breaches will be similarly idiosyncratic, it would not be appropriate to too closely confine the issue of damages.

If the purpose of damages is to compensate the applicant for damage suffered as a consequence of the privacy breach, the applicant should have the onus to show they have suffered damage (both pecuniary and non-pecuniary) and damages should be confined accordingly.

17. What, if any, specific provisions should the Act include as to matters a court must consider when determining whether to grant an injunction to protect an individual from a serious invasion of privacy? For example, should there be a provision requiring particular regard to be given to freedom of expression, as in s 12 of the Human Rights Act 1998 (UK)?

As noted in the response to Question 7, Queensland's IP Act and RTI Act give a right of access to information in the government's possession or under the government's control unless, on balance, it is contrary to public interest to give the access.

Both Acts establish a public interest balancing test which sets out the steps for how competing public interest factors should be compared and considered when making a decision about whether allow or refuse access to information. Schedule 4 of the RTI Act outlines a non-exhaustive list of factors the Parliament considers relevant to determining whether the disclosure of information would, on balance, be contrary to the public interest.

A similar approach could be taken when considering the granting of an injunction. It is noted that in a jurisdiction that is focussed on the damage suffered by an individual in respect of a breach of their privacy, actions for injunctions should consider the preventative or mitigating consequences of the grant.

OIC acknowledges that 'freedom of expression' could be a competing public interest consideration which would need to be balanced against the public interest in the protection of privacy.

18. Other than monetary remedies and injunctions, what remedies should be available for serious invasion of privacy under a statutory cause of action?

In Queensland's statutory scheme, QCAT can make an order that the complaint, or a part of the complaint, has been substantiated, together with, if considered appropriate, orders that are both broad in application and targeted to specific circumstances. Most of the legislated categories of orders do not involve monetary compensation. The orders QCAT can make include:

- that an act or practice of the respondent is an interference with the privacy of the complainant and that the respondent must not repeat or continue the act or practice
- that the respondent must engage in a stated reasonable act or practice to compensate for loss or damage suffered by the complainant
- that the respondent must apologise to the complainant for the interference with the privacy of the complainant
- that the respondent must make stated amendments of documents it holds
- an order that the complaint, or a part of the complaint, has been substantiated together with an order that no further action is required to be taken
- an order that the complaint, or a part of the complaint, has not been substantiated, together with an order that the complaint or part is dismissed; and
- an order that the complainant be reimbursed for expenses reasonably incurred in connection with making the complaint.

The purpose of redress is to place the party which has suffered damage in the position they would have been had the breach not occurred. OIC's view is that there should be no restrictions on the remedies available for an individual to achieve that result.

OIC acknowledges that once privacy has been breached, restoration of the individual's original position is usually not possible. OIC's experience is that privacy complainants are generally realistic about the efficacy of remedial orders and compensatory measures.

However, they do see a two-fold value in being able to pursue their issue to a conclusion. Firstly, it validates themselves and their complaint. Privacy complainants commonly report that the way in which their personal information was treated disregarded them as an individual person. They also report that their feelings about how the information was treated were minimised and only considered in a minor way in the agency's handling of their complaint by the agency. Complainants consider that an individual remedy brings the focus back to them as a person.

The second benefit of pursuing a privacy complaint is the deterrent effect. This is reflected in commonly made statements by complainants that they don't want the breach to be repeated or for it to happen to others. To this end, a privacy complaint and consequent remedial orders can be means to avoid a repetition of the breach and reduce privacy risks by highlighting non-compliant, outmoded systems and practices.

19. Should a statutory cause of action for a serious invasion of privacy of a living person survive for the benefit of the estate? If so, should damages be limited to pecuniary losses suffered by the deceased person?

OIC is aware that there are significant differences between the jurisdictions as to whether privacy rights survive the death of the individual. In Queensland your right to privacy ceases on death. The capacity for an estate to initiate – as opposed to continuing – a privacy complaint that occurred while the relevant individual was alive has yet to be tested in law.

The IP Act has a provision that allows a person to act on behalf of an individual to the extent that the individual has authorised. OIC has taken this provision as meaning that where a will specifically authorises an executor to initiate and pursue a privacy complaint on behalf of the individual's estate, there is sufficient authorisation. The proviso is that the act that is the subject of the complaint must have occurred when the person was alive.

To date this approach has not been tested in a determinative forum.

OIC acknowledges that in the event of acceptance of the action, the issue as to what is an appropriate remedy remains problematic. The remedial actions that QCAT can order are largely non-financial in nature (see OIC response to the previous question). However, OIC also notes that this issue is not unique to privacy. The concept of Nominal Defendant is well established in motor accident law.

20. *Should the Privacy Commissioner, or some other independent body, be able to bring an action in respect of the serious invasion of privacy of an individual or individuals?*

It is unclear how this would work in practice. If an individual is unable or unwilling to bring an account that could grant them relief, it is difficult to see how an independent body could pursue this action on their behalf.

OIC suggests that it could be appropriate for the Privacy Commissioner to have a role akin to that of State Coroners, where they could independently investigate an incident and issue findings while leaving the 'prosecution' of those findings as a matter for the individual concerned.

21. *What limitation period should apply to a statutory cause of action for a serious invasion of privacy? When should the limitation period start?*

In Queensland OIC has the discretionary authority to not accept a privacy complaint if it is lodged more than 12 months *after the complainant has first become aware* of the act or subject that is the subject of the complaint. This recognises that individuals may not become immediately aware that their privacy has been breached; more usually that awareness results from their information being disseminated in the public domain. This contrasts with the area of defamation where the defamatory action and the dissemination are the same event.

It is conceivable that if the limitation period were one year, unscrupulous operators could 'sit' on the information for that year before using the information on the anniversary date.

Privacy is an individual right and persons can suffer personal damage as a result of a privacy breach. The 'damage' suffered by an individual often commences when they become aware of the privacy breach. In Queensland the statutory period of limitation for personal injury is three years from the date on which the action occurred.⁴ OIC considers that accordingly, a period of three years from when person first becomes aware of the privacy breach would be sufficient time for an individual to seek redress for it. OIC suggests that this period could be extended by leave of the relevant court.

22. *Should a statutory cause of action for serious invasion of privacy be located in Commonwealth legislation? If so, should it be located in the Privacy Act 1988 (Cth) or in separate legislation?*

Given the lack of uniformity of laws regulating the handling of personal information across Australia and the practical reality that privacy breaches can occur across jurisdictions, it is OIC's view that a statutory cause of action be located in separate Commonwealth legislation. If the tort will be actionable directly in the Courts it may be preferable to create a separate statute, to distinguish the tort of invasion of privacy from complaints handled under the privacy legislation.

Consistent with its responses throughout this submission, OIC considers that there should be strong parallels between the existing Commonwealth privacy jurisdiction and the new statutory cause of action jurisdiction.

⁴ Section 11 of the *Limitation of Actions Act 1974* (Qld).

23. Which forums would be appropriate to hear a statutory cause of action for serious invasion of privacy?

It is OIC's view that a statutory cause of action for serious invasion of privacy should be dealt with in the same way as any other civil proceeding.

24. What provision, if any, should be made for voluntary or mandatory alternative dispute resolution of complaints about serious invasion of privacy?

OIC supports that provision is made for mandatory alternative dispute resolution of complaints.

While there is a statutory right of action in QCAT for privacy matters in Queensland, an applicant is unable to progress to QCAT unless informal resolution has at least been considered twice – firstly by the agency directly and thence through OIC's mediation service. This mechanism is common to Australian privacy complaint jurisdictions.

Recourse to QCAT is rarely utilised. In the last four years of operation, only nine privacy complaints have been brought before QCAT.

25. Should a person who has received a determination in response to a complaint relating to an invasion of privacy under existing legislation be permitted to bring or continue a claim based on the statutory cause of action?

OIC considers that an individual who has received a determination in response to a complaint about a breach of their privacy should be permitted to bring or continue a claim based on the statutory cause of action where the complaint was substantiated but no declaration was made as to remedial action or where the form of remedy being sought was not provided for under existing legislation.

However, while OIC considers that individuals should have access to an appropriate remedy, provisions should be made to circumvent the potential for remedial 'double dipping' and providing the same form of remedy more than once.

26. If a stand-alone statutory cause of action for serious invasion of privacy is not enacted, should existing law be supplemented by legislation:

- providing for a cause of action for harassment;*
- enabling courts to award compensation for mental or emotional distress in actions for breach of confidence;*
- providing for a cause of action for intrusion into the personal activities or private affairs of an individual?*

While OIC's preferred position would be for a stand-alone statutory cause of action, OIC would be generally supportive of any movement to providing greater protection of personal information.

27. In what other ways might current laws and regulatory frameworks be amended or strengthened to better prevent or redress serious invasions of privacy?

OIC suggests that consideration should be given to expanding the scope of which entities are covered by privacy legislation to enable more inclusive access by individuals to obtain an enforceable remedy if their privacy has been breached.

In general terms there is no privacy law in Queensland that applies to acts of privacy breach by individuals, small business or small community sector organisations.

OIC notes that international jurisdictions have broader applicability of privacy legislation. For example, New Zealand's *Privacy Act 1993* applies to any person or body of persons, whether corporate or unincorporated, and whether in the public or private sector. Organisations not covered by the Privacy Act are limited to members of Parliament, courts and tribunals in relation to their judicial functions and the news media when they are conducting their news activities.

Canadian privacy legislation is framed around Canada's private and public sector. The *Personal Information Protection and Electronic Documents Act* applies to all organisations that collect, use or disclose personal information in the course of their commercial activities, except those provinces which have enacted legislation that is deemed to be substantially similar. Public bodies that operate in Canada's public sector, such as educational, health care and local government bodies are subject to Canada's *Privacy Act 1983*.

OIC commonly receives enquiries from members of the public about the use of surveillance cameras by individuals and private sector organisations that are not subject to State or Federal privacy legislation. Broader applicability of privacy legislation would result in greater deterrence against invasions of privacy by individuals and access to the right to an effective remedy if a breach of privacy should occur.

28. In what other innovative ways may the law prevent serious invasions of privacy in the digital era?

The increasing digitisation of communication has compounded the gaps in privacy coverage. The ease by which personal information can be collected and communicated globally has increased the potential damage of misused personal information. For a relatively small cost, a disgruntled individual can operate a surveillance drone aircraft over their neighbour's property and that neighbour has very limited protections over the individual's use and online dissemination of the captured footage concerning them.

OIC notes with interest New Zealand's recent *Harmful Digital Communications Bill*, which creates a new criminal offence for sending messages or posting material online with intent to cause harm - including threatening and offensive messages, harassment, damaging rumours and invasive photographs. This initiative is in part aimed at preventing cyber-bullying.

Another innovative concept is the 'right to be forgotten' – the destruction of personal information holdings once the immediate purpose for the holding has been fulfilled.

The *Serious Invasions of Privacy in the Digital Era: Issues Paper* identifies that a possible solution to providing individuals with an enforceable right of removal of certain information is the introduction of a 'right to be forgotten and to erasure'. This proposal would introduce a requirement that organisations, such as social media service providers, permanently delete information at the request of the individual who is the subject of that information. OIC notes that whether and how such a right could be incorporated into Australia law was discussed at the Australian Internet Governance Forum on 16-17 October 2013⁵ and suggests that ALRC seek advice as to the outcomes from this discussion which may inform this issue.

This exists currently to an extent in privacy law. The Commonwealth's APP 11.2 states that when an APP entity no longer requires personal information there is the capacity for the entity to destroy the information or to ensure that the information is de-identified. Similarly, NPP 4(2) of Queensland's IP Act requires health agencies to take reasonable steps to ensure that the individual the subject of the personal information can no longer, and can not in the future, be identified from the personal information.

OIC considers that the ability for an individual to more broadly request that their personal information which has gone beyond immediate use to be deleted or destroyed is a key issue suitable for further discussion and consideration.

⁵ See <http://www.igf.org.au/> for more information.