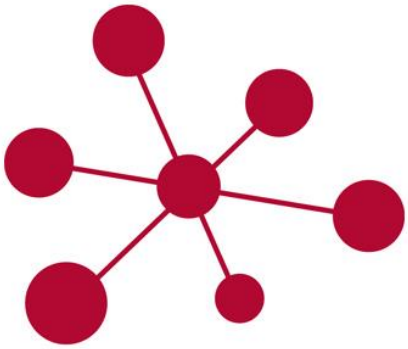

Submission to the Review of the Privacy Act 1988

November 2020

Level 5, 175 Liverpool Street, Sydney NSW 2000
Phone: 61 2 8898 6500 • Fax: 61 2 8898 6555 • www.piac.asn.au

About the Public Interest Advocacy Centre
The Public Interest Advocacy Centre (PIAC) is an independent, non-profit legal centre based in Sydney.

Established in 1982, PIAC tackles barriers to justice and fairness experienced by people who are vulnerable or facing disadvantage. We ensure basic rights are enjoyed across the community through legal assistance and strategic litigation, public policy development, communication and training.

Our work addresses issues such as:

- Reducing homelessness, through the Homeless Persons' Legal Service
- Access for people with disability to basic services like public transport, financial services, media and digital technologies
- Justice for Aboriginal and Torres Strait Islander people
- Access to affordable energy and water (the Energy and Water Consumers Advocacy Program)
- Fair use of police powers
- Rights of people in detention, including equal access to health care for asylum seekers (the Asylum Seeker Health Rights Project)
- Transitional justice
- Government accountability.

Contact
Chadwick Wong
Public Interest Advocacy Centre
[redacted]

T: [redacted]
E: [redacted]

Website: www.piac.asn.au

Public Interest Advocacy Centre

@PIACnews

The Public Interest Advocacy Centre office is located on the land of the Gadigal of the Eora Nation.

Contents

1. Introduction

The Public Interest Advocacy Centre (**PIAC**) welcomes the opportunity to comment on the review of the *Privacy Act 1988* (Cth).

PIAC's work focuses on tackling barriers to justice and fairness experienced by marginalised communities. As part of this work, we have a long history as a strong advocate for the protection of privacy rights of Australians, and have contributed to the numerous reviews over the past two decades on privacy reform both at federal and state levels. In our work, we have consistently identified significant gaps in the legal framework for the protection of the right to privacy, and have repeatedly recommended that a statutory cause of action to protect the right to privacy be enacted. This submission draws on our work in relation to previous inquiries on the same subject.

The review of the *Privacy Act* provides an opportunity for reform in areas of longstanding concern, including in relation to a direct right of action and a statutory tort for invasions of privacy. This is especially so given the context of NSW Parliament's consideration of the *Civil Remedies for Serious Invasions of Privacy Bill 2020* (NSW), introducing a statutory tort for serious invasions of privacy, as well as recent recommendations by the South Australian Law Reform Institute to introduce such a tort in South Australia.[1]

The opportunity is ripe for the introduction of a federal framework for a statutory tort, which will avoid creating an even more complex regulatory environment for businesses and individuals resulting from a patchwork of state-based frameworks.

It also provides an opportunity to consider whether fundamental concepts within the Act – particularly in relation to the objects of the Act, the definition of personal information and consent – remains fit for purpose in an age of digital transformation.

Our submission is limited to the following issues identified in the Issues Paper, where PIAC has direct experience:

- Objects of the Act (question 1)
- Definition of personal information (questions 2 and 3)
- Consent (questions 26 to 42)
- Direct right of action (question 56)
- Statutory tort for serious invasions of privacy (questions 57 to 62)

2. Context

As this Review's Terms of Reference identify, the digital economy, emergence of new technologies and the increasing amount of time spent by Australians online means that 'more personal information about individuals is being captured and processed raising questions as to whether Australian privacy law is fit for purpose'.[2] But while new technologies and the increased collection of personal information by businesses provides important context to the review of the *Privacy Act*, so too does the increased use of personal and sensitive information by government bodies.

---

1 South Australian Law Reform Institute, *Too much information: A statutory cause of action for invasion of privacy* (Final Report 4, 2016).

2 Terms of Reference, 1.

This increased use of personal information is reflected in the proposed draft *Data Availability and Transparency Bill* (**DAT Bill**). The DAT Bill proposes to allow sharing of public sector data – including a significant volume of personal information held by government agencies – in a wide range of circumstances, provided that the sharing is for a data sharing purpose, is consistent with the data sharing principles, and is in accordance with a data sharing agreement.[3]

Each of these limitations are very broad. The 'data sharing purposes' include the delivery of any government service, informing government policy and programs, and research and development (including commercial research and development).[4] The sharing of data to inform government policy and programs is intended to be interpreted 'broadly'.[5] Likewise, the 'data sharing principles' are broad and vague – each principle is defined by reference to the term 'appropriate' or 'agreed'. The data must be shared for an appropriate project; made available only to appropriate persons; in a setting that is appropriately controlled; with appropriate protections applied; with outputs that are as agreed (between the relevant data scheme entities); and with risks that are appropriately mitigated. As the Privacy Impact Assessment to the DAT Bill states, the 'high-level nature of the Data Sharing Principles poses a privacy risk'.[6]

Importantly, the proposed DAT Bill significantly expands the possible use and disclosure of an individual's personal information, in ways that could not reasonably be envisaged by an individual when providing their consent to the initial collection. This is because of the way the DAT Bill interacts with Australian Privacy Principle (**APP**) 6, under the *Privacy Act*. APP 6 generally permits use or disclosure of an individual's personal information only for the 'primary purpose', being the purpose for which it was collected. It cannot be used or disclosed for any other purpose unless the individual has consented, or one of the exceptions at subclause 6.2 or 6.3 of the *Privacy Act* applies. The DAT Bill has the effect of falling entirely within the exception of subclause 6.2(b), being an exception where use or disclosure is authorised by Australian law.[7] Given the DAT Bill 'authorises data custodians to share public sector data with accredited entities from all levels of government as well as industry, research and other private sectors',[8] there is significant potential for personal information to be shared far beyond what was originally envisaged by the individual.

To this context must be added the data breaches which have occurred in respect of public sector data in a number of high-profile incidents, with significant consequences. These include:

- the Department of Immigration and Border Protection's data breach in February 2014, resulting in the release of sensitive personal information of people in immigration detention, including asylum seekers;
- the Federal Court's data breach in March 2020 resulting in the publication of the identities of asylum seekers;

---

3 *Data Availability and Transparency Bill* (**DAT Bill**), cl 13(1).
4 DAT Bill, cl 15(1).
5 Explanatory Memorandum to the Data Availability and Transparency Bill 2020, Draft September 2020 (**Explanatory Memorandum**), Part 1, [30].
6 Information Integrity Solutions, *Privacy Impact Assessment – Draft Data Availability and Transparency Bill 2020*, 6 September 2020 (**Privacy Impact Assessment**), 38.
7 Ibid, 25.
8 Explanatory Memorandum, above n 5, Part 1, [18].

- the Services NSW data breach in 2020 which resulted in the personal information of 186,000 customers being stolen; and
- the data breach involving 54,000 NSW driver's licences being found in open cloud storage in 2020.

It is unsurprising, then, that according to the Office of the Australian Information Commissioner (**OAIC**)'s 2020 Australian Community Attitudes to Privacy Survey, 83% of Australians 'would like the government to do more to protect the privacy of their data.'[9] Privacy remains a major concern for 70% of Australians in 2020,[10] with 61% of Australians identifying data security and data breaches as among the biggest privacy risks.[11] Only 36% of Australians are comfortable with government agencies sharing their personal information, with 40% of Australians uncomfortable with this. 70% of Australians are uncomfortable with government agencies sharing their personal information with businesses.[12]

When it comes to marginalised communities, the OAIC further reported:

> Two-thirds of Australians believe that vulnerable groups, such as children under 12 years old (68%) and 13-17 years old (64%), elderly Australians (67%) and people with an intellectual disability (67%), require additional protection under the Privacy Act. A significant minority of Australians also support the additional protection of young adults (42%), people who speak English as a second language (39%) and new migrants to Australia (38%).[13]

It is within this broader context that review of the *Privacy Act* must be situated. Increased use of personal information by a greater range of actors – including businesses, government, accredited researchers and non-government organisations – means that the *Privacy Act* must be strengthened to ensure the protections of an individual's right to privacy remain appropriate. Where breaches occur, individuals must have recourse to effective remedies which provides both redress for the breach and safeguards against future breaches.

3. Objects of the Act (Question 1)

PIAC submits that the objects of the Act need to be strengthened to recognise the right to privacy, consistent with international law. The right to privacy is one of the cornerstones of modern democracy, established as such during the modern development of the international human rights framework in the twentieth century.

The right is clearly articulated in international law. It is recognised in the Universal Declaration of Human Rights and various international treaties to which Australia is a signatory.[14] Article 17 of International Covenant on Civil and Political Rights provides:

---

9 Office of the Australian Information Commissioner, *2020 Australian Community Attitudes to Privacy Survey*, September 2020, 65.
10 Ibid, 4.
11 Ibid, 6.
12 Ibid, 27.
13 Ibid, 68.
14 See, for example, *Universal Declaration of Human Rights*, art 12; *International Covenant on Civil and Political Rights,* art 17; *Convention on the Rights of the Child*, art 16.

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.[15]

In the domestic context, the right to privacy has been specifically enshrined in the human rights legislation of the Australian Capital Territory[16], Queensland[17] and Victoria[18].

The right to privacy is not an absolute right; it must accommodate certain other human rights and interests, including the freedom of expression and implied freedom of political communication. But as a fundamental human right, it would be inappropriate for privacy to be traded off against business interests or an interest in the dissemination of gossip.

In circumstances where there remains no federal charter of human rights, and no recognition of the right to privacy at a federal level, the interpretation of the *Privacy Act* must be grounded in the internationally-recognised right to privacy. Recognising this in the objects clause allows for the Act to be interpreted through this lens, in the absence of a more substantive right at federal level.

For these reasons, the objects should be amended to:

- recognise and promote the right to privacy – not merely the 'protection' of the privacy of individuals. This would ensure better alignment of the Act with the existing object to 'implement Australia's international obligation in relation to privacy';
- remove the reference to the right to privacy being balanced with the 'interests of entities in carrying out their functions or activities'. As submitted above, the right to privacy is a fundamental human right, recognised at international law and in a number of domestic jurisdictions. While the Act must provide a framework to balance the right to privacy with other human rights, including the freedom of expression, freedom of the media and implied freedom of political communication, it should not be balanced against business interests. Instead, business interests should be aligned with and work in concert with the right to privacy; and
- provide redress for individuals whose right to privacy has been subject to arbitrary or unlawful interference. This reflects our submission on the direct right of action, addressed below, and strengthens the existing object in relation to complaints.

4. Definition of personal information (Questions 2 and 3)

PIAC considers that the definition of personal information requires updating to reflect the way in which technical data and inferred personal information can be (and are) now used to to identify individuals.

In relation to technical data, PIAC has limited experience in matters involving online identifiers. However, as a matter of principle, we support clarifying the definition of personal information to ensure it captures all manners in which individuals are identified or can be reasonably identified. To that end, we support the ACCC's recommendation to clarify the definition to ensure it captures

---

15 *International Covenant on Civil and Political Rights,* 16 December 1966, [1980] ATS 23 (entered into force generally on 23 March 1976).
16 *Human Rights Act 2004* (ACT), s 12.
17 *Human Rights Act 2019* (Qld), s 25.
18 *Charter of Human Rights and Responsibilities Act 2006* (Vic), s 13.

technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual.

In relation to inferred personal information, PIAC's submission draws from our experience as a leading energy consumer advocate. There is an emerging potential to collect a significant amount of data through smart household appliances, such as through smart vacuums, smart TVs and virtual voice assistants, as well as smart energy meters. The information that is collected may include:

- in relation to smart meters, information about a household's energy usage and patterns, habitual behaviours, times when a household is occupied or vacant and changes to the composition or behaviours of a household;
- in relation to smart vacuums, high-end Roombas collect data on the layout of a person's house and sends this data back to the company, iRobot, which could be shared with other businesses, such as Amazon, Apple or Google.[19] This creates the potential to ascertain valuable information about individuals and households, such as income levels based on the size and location of the home or lifestyles based on the furniture in the home;
- in relation to smart TVs, a recent study by Princeton University and the University of Chicago found that tracking of user data was widespread on devices that allow internet connection for TVs, such as Amazon Fire TV and Roku TV. The data that was collected included viewing histories and habits, which could be tied to device identifiers and wireless network identifiers (WiFi SSIDs).[20]

Currently, much of this data would may not fall within the definition of 'personal information', on the basis that the information collected concerns a household or does not, in and of itself, reasonably identify an individual. However, combined with other data sources, this information can be used to create a very detailed picture of people's homes, habits and spending that many people may be unaware of. While PIAC does not necessarily oppose the collection or use of this data, for instance in ways that may enable better tailored and more cost effective energy retail offers to consumers, we consider this information should fall within the protections of the *Privacy Act* framework to better empower consumers.

5. Consent (Questions 26-42)

As a general position, PIAC echoes the joint submission of the Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia, in relation to consent, particularly the limitations to the effectiveness of consent in a data context, and the need for strategies to focus on both improving the process of consent and to combat consumer harm through other regulatory means. Our further responses to the consent questions raised in the Issues Paper reflect PIAC's experience with specific marginalised communities.

---

19 Maggie Astor, 'Your Roomba may be mapping your home, collecting data that could be shared', *New York Times* (online), 25 July 2017 <https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html>

20 Hooman Mohajeri Moghaddam et al, 'Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices' (Paper presented at CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, November 2019), 131–147, <https://dl.acm.org/doi/10.1145/3319535.3354198>

While there are limitations in the effectiveness of consent – for reasons such as the complexity of collection notices, the difficulties in avoiding participation in data driven technologies, or a lack of understanding from consumers about how their data may be used in future – consent must nevertheless form a key basis for the use of personal information. This is because, when used effectively, consent can be both empowering and protective.

For example, energy consumers who rely on life support equipment at home must notify their retailers/distributors of their circumstances to be placed on Life Support Registers. If someone is on a Life Support Register it means that they cannot be disconnected for non-payment of bills and there are additional requirements around notification of outages. Currently, every time an individual (or their carer/agent) switches their energy retailer, they have to resubmit medical confirmation of their need for life support equipment. This is tedious, can impose a cost (to get the medical confirmation again from a doctor) and creates a risk that they could drop off the register inadvertently (for example, they forget to let their new retailer know they require life support or proper processes are not followed to get them on the register). To ensure the safety of the person, it is important that the individual is able to consent to their previous retailer/distributor passing on their medical confirmation to the new retailer/distributor.[21] Consent used in this way empowers the individual to make decisions about their choice of retailer. At the same time, strict requirements around consent ensure that the person can control where their medical information is distributed, and is not passed on to third parties without their consent.

For consent processes to be effective and empowering for people to manage their personal information, they must:

- be given in plain language, appropriate for the intended audience. For instance, businesses that work with migrant communities must ensure consent processes are tailored accordingly;
- be clear as to the information to be collected;
- be clear as to who holds the information;
- be specific as to the primary purpose of the collection. That is, in answer to question 28 of the Issues Paper, individual consents for each primary purpose must be sought. The example given above in relation to Life Support Registers provides a clear case study as to why this must be so;
- have in place pro-consumer defaults. To this end, there should be opt-in boxes to ensure people are explicitly aware of what they are agreeing to, outside of the primary purpose for the collection;
- ensure that if an individual refuses to consent to their personal information being collected, used or disclosed for a purpose that is not necessary or central to providing the relevant product or service, they are still able to access the service (in response to question 29a of the Issues Paper). To that end, the consent process must clearly state what personal information is required for the provision of the product or service, and what is not; and
- inform people as to how they can withdraw consent (and ensure that the process for withdrawal of consent is easy).

[21] PIAC's position more generally is that the Life Support Register should be maintained by the distributor (or even having one central register) and a consumer would remain on this register regardless of who their retailer is or whether they switched retailers. This issue is currently being considered by the Australian Energy Market Commission.

Strict consent requirements are all the more important in the context of the proposed DAT Bill. As described above, the proposed DAT Bill significantly expands the possible use and disclosure of an individual's personal information, in ways that could not reasonably be envisaged by an individual when initially providing their consent, given the way in which the Bill interacts with APP 6. Requiring an individual to provide consent for each primary purpose goes some way to ensure consent remains effective even with the introduction of the DAT Bill.

Entities that collect personal information should also be required to have regard to the objects of the *Privacy Act* – specifically, as proposed by PIAC, individuals' right to privacy. This helps ensure that the burden of preventing unreasonable and inappropriate use of personal information does not fall solely on the consumer to understand their rights, but also on the entitiy seeking to collect that information.

This requirement to have regard to an individual's right to privacy is especially important for government collection of personal information. Marginalised communities have disproportionately greater interactions with government services. People who rely on government services may not be in a position to provide informed consent given the inherent power imbalance when requesting services. In certain circumstances, even where a person is informed about how their personal information will be handled, it can be practically difficult to withhold consent for the proposed management of their personal information. For example, consent procedures for the use of immigration detention medical records – where a person arriving in detention signs a consent form to say that their information can be used to assist with their placement – have been criticised as inadequate for allowing a person's information to be used by the Department of Home Affairs for purposes other than a patient's health care. [22]

For the same reasons, we support the 'no-go zones' guidance issued by the Office of the Privacy Commissioner of Canada, in relation to purposes which would generally be considered inappropriate for the collection, use or disclosure of personal information, regardless of consent.[23] The six identified 'no-go zones' should be considered and adapted for an Australian context.

6. Direct right of action (Question 56)

PIAC strongly supports the implementation of a direct right of action for individuals to litigate a claim for breach of privacy under the Act.

6.1 Issues with the current process

The current process for individuals seeking to enforce their rights under the Act is clumsy and provides limited recourse. As the Issues Paper outlines, individuals may make a complaint about breaches of the Act to the Commissioner, who may investigate, conciliate and decline complaints. If the Commisioner investigates a complaint and finds it to be substantiated, they may make a determination. A complainant would then need to apply to the Federal Court or Federal Circuit

---

22 David Marr, Oliver Laughland and Bill Code, 'Asylum seekers' medical records being used against them, says mental health chief – video', *Guardian Australia*, 5 August 2014 <https://www.theguardian.com/world/video/2014/aug/04/asylum-seeker-health-records-used-against-them-video>.

23 Office of the Privacy Commissioner of Canada, *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)*, May 2018 <https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/>.

Court for an order enforcing such a determination. The court then hears the matter de novo, which may result in a different decision.

Where a determination is made by the Commissioner, the parties are also able to seek review by the Administrative Appeals Tribunal. Any such decision by the Tribunal may then be subject to judicial review in the ordinary course. But as the Issues Paper identifies, 'the entity that is alleged to have breached the individual's privacy is not a party to proceedings in either merits or judicial review'.

These issues with the current process and the lack of a direct right of action will be made starker if the DAT Bill as currently proposed is enacted. This is because remedies for individuals affected by data sharing decisions under the proposed scheme would rely on 'existing avenues for redress in other schemes'.[24] Given the anticipated significant increase to the amount of public sector data being shared, it is essential that the *Privacy Act* be amended to provide a direct right of action for individuals.

6.2 How a direct right of action should be framed

Any direct right of action must be clear and simple – for the public to understand, for individuals to exercise, for entities to respond, and for courts to determine jurisdiction.

For this reason, PIAC endorses the approach taken in relation to the Consumer Data Right in the banking sector, and noted as an 'alternative' in the Issues Paper. That is, individuals ought to have a choice as to whether they apply directly to the courts, or to seek conciliation through the OAIC. The OAIC already has a conciliation process available to complainants. That process allows individuals to pursue a no-cost, less formal and quicker resolution to their complaint, and ought to continue. Based on PIAC's experience in working with complainants from marginalised communities, we expect that the majority of complainants, particularly those with less serious or complex complaints, would prefer to seek resolution of their complaint initially through conciliation rather than to go through lengthy court processes.

For individuals with serious or more complex complaints, for whom conciliation has failed or for those who do not wish to go through the conciliation process, they should be able to apply to the courts directly. This approach is the same as for the Consumer Data Right.[25] Allowing individuals to access the courts directly is important for several reasons:

- individuals would have greater control over their personal information, and would be better empowered to exercise their rights;
- it creates an additional incentive for APP entities to comply with their obligations under the Act;
- it allows for more efficient legal cases to be conducted. In PIAC's experience, allegations of breaches of privacy often occur in tandem with other causes of action. For example, we recently represented a mother who alleged disability discrimination against her daughter by her daughter's school, as well as breaches of her daughter's privacy by the school. Allowing direct right of action to the court would mean that her complaints against the school could be

24 Explanatory Memorandum, above n 5, Part 1, [54].
25 *Competition and Consumer Act 2010* (Cth), s 56EY.

dealt with holistically, without having to make separate complaints before separate commissions (being the Australian Human Rights Commission (**AHRC**) and the OAIC);
- it allows representative complaints (class actions) to be brought in circumstances where it may not be economic to make an individual application; and
- it provides greater opportunity for courts to interpret the Act, better enabling the public, as well entities holding personal information, to understand their rights and obligations, as well as better enabling the OAIC to provide oversight of the legislation.

PIAC agrees with the proposal to allow the Commissioner to be heard in proceedings as amicus curiae. The same process as applies to the AHRC ought to be applied here[26] – that is, the Commissioner ought to be given the function of intervening in cases involving privacy rights and obligations, but this must be subject to leave being granted by the court, and subject to any conditions imposed by the court. This ensures that the court is able to determine, in any given proceeding, whether the Commissioner's involvement will assist its processes, or whether it will increase delay in proceedings.

We consider this approach to be simple, as it allows applicants and respondents to understand which forum a complaint is to be conducted and the process and rules that apply. Once the decision is made, the complaints process is streamlined – either it proceeds through the well-worn path of conciliation at the OAIC, or it proceeds as a normal court proceeding. The ability of the Commissioner to intervene, with leave of the court, further assists with the streamlining of the resolution of complaints.

In contrast, PIAC does not support the two other options for a direct right of action proposed in the Issues Paper, being either a limitation of the right to 'serious breaches' of the Act, or making it a condition to go through a conciliation process before applying to the courts. This is because both of these options create additional complexities to the framework, when one of the reasons for creating a direct right of action is to simplify the manner in which individuals can protect their privacy:

- in relation to the proposal to limit the right to 'serious breaches' of the Act, it is not clear how 'serious breaches' would be defined, and who would determine whether the threshold was met. If the courts are required to determine whether a breach is sufficiently 'serious' in order to determine whether it has jurisdiction (prior to considering the substance of the application), this adds an extra process with attendant time, costs and resources burden. If the Commissioner is required to make this determination prior to a complainaint filing a court application, this creates even greater time, costs and resources burden. This is especially so if the court then has jurisdiction to consider the Commissioner's determination of the 'seriousness' of the breach;

- likewise, requiring all individuals to go through a conciliation process before applying to the courts adds unnecessary complexity, and limits rights of individuals for no identifiable benefit. As already submitted, where the conciliation process is optional, individuals with less serious or complex complaints are likely to prefer a process which is cost-free, less formal and which may provide a quicker resolution. It may be desirable for the OAIC to promote and encourage

[26] See, for example, *Australian Human Rights Commission Act 1986* (Cth) ss 11(1)(o) and 31(j); *Disability Discrimination Act 1992* (Cth), s 67(1)(l).

use of this process. For individuals who choose to apply directly to the courts, PIAC's experience in human rights matters is that the court will generally order mediation as an early step anyway.[27] As earlier submitted, PIAC's experience is that allegations of breaches of privacy can often occur in tandem with other causes of action. Requiring an individual to first go through the conciliation process for their privacy allegations creates inefficiency in the system.

- If individuals are required to go through a conciliation process, and the OAIC's existing investigation and determination functions are kept, an individual would be required to elect, after a failed conciliation process, to either make an application to the court or to continue with the OAIC process and seek an investigation and determination by the Commissioner. If the individual decides to continue with the OAIC's process, but is unsatisfied with the Commissioner's determination (or refusal to determine), they would then be required to go through merits review at the Administrative Appeals Tribunal and potentially judicial review afterwards. This is a needlessly complex process for individuals.

PIAC also does not support a cap on the damages that may be awarded. There is no reasonable justification for adding a cap. As the Issues Paper identifies, capping the award of damages may lead to lesser, rather than more serious, breaches of the Act coming before the courts. The introduction of a cap also benefits perpetrators of privacy breaches, by potentially making it more economical for them to make settlement offers relative to the cap rather than having the matter tested before courts. Applicants who pursue claims are also more likely to be wealthier individuals, for whom the award of damages is less important than other forms of relief, such as a declaration of breach or public apology. Rather than introducing a cap to 'reduce the incentive for parties to litigate', it is preferable that the OAIC *encourage* use of its conciliation mechanisms to resolve complaints.

We consider this proposal effectively balances the rights of individuals to exercise greater control over their personal information with the need to ensure court resources are used appropriately. In effect, the proposal has the following in-built mechanisms to balance against court resources being overburdened:

- a conciliation process remains available, and its use is encouraged by the OAIC to settle complaints;
- the Commissioner is able to seek leave to intervene in matters to assist the court in resolving disputes; and
- the courts' general powers to manage its resources remain unaffected, including court-ordered mediation and alternative dispute resolution processes, as well as processes in relation to vexatious litigants.

7. Statutory tort (Questions 57 to 62)

PIAC strongly supports the introduction of a statutory tort for serious invasions of privacy, for the reasons as follows.

---

27 See, for example, the Federal Court of Australia's Central Practice Note (CPN-1) and Administrative and Constitutional Law and Human Rights Practice Note (ACLHR-1).

7.1 Considerations to date

Recommendations for the establishment of a statutory cause of action for breaches of privacy have been made over the past decade by an increasing number of reviews, including:

- the NSW Law Reform Commission in its 2009 report, *Invasion of Privacy*;[28]
- the Victorian Law Reform Commission (**VLRC**) in its 2010 report, *Surveillance in Public Places*;[29]
- the Australian Law Reform Commission (**ALRC**) in its June 2014 report, *Serious Invasions of Privacy in the Digital Era;*[30]
- the NSW Legislative Council Standing Committee on Law and Justice's 2016 inquiry into remedies for the serious invasion of privacy in NSW;[31]
- the South Australian Law Reform Institute's 2016 review into a tort of invasion of privacy;[32]
- the ACCC's 2019 Digital Platforms Inquiry (**DPI**) Final Report;[33] and
- the AHRC, in its 2019 *Human Rights and Technology* discussion paper.[34]

The extensiveness of previous consultations and the longstanding recommendations made by numerous reviews was also recognised in the ACCC's DPI report.[35]

The Issues Paper acknowledges concerns raised in previous reviews and by stakeholders, and appears to accept that:[36]

- there is currently no tortious right of action for invasion of privacy under any statute in Australia, at either federal or state level;
- a tort of privacy would provide individuals with an option to take civil action against an individual or entity and seek damages as compensation;
- the cause of action available under equity for breach of confidence provides limited redress; and
- the common law has not recognised a tort for invasion of privacy in Australia.

However, the Issues Paper also suggests that the development of criminal laws – primarily relating to voyeurism and non-consensual sharing of intimate images – since the ALRC's recommendations in 2014 'may negate the need for a tort of privacy on a policy basis'.[37] It further notes that if such a tort is not developed by the legislature, it could yet be developed at common law.[38]

PIAC does not agree. We consider there remains a need to develop a cause of action in tort for serious breaches of privacy, and that such a cause of action is best developed by the legislature

---

28 New South Wales Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009).
29 Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010) (**VLRC Report**).
30 Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era, Final Report,* Report 123, (2014) (**ALRC Report**).
31 Legislative Council Standing Committee on Law and Justice, Parliament of NSW, *Remedies for the serious invasion of privacy in New South Wales*, Report No 57 (2016).
32 South Australian Law Reform Institute, *A statutory tort for invasion of privacy*, Final Report 4 (2016).
33 Australian Competition and Consumer Commission, *Digital Platforms Inquiry*, Final Report, (2019) (**DPI Report**).
34 Australian Human Rights Commission, *Human Rights and Technology*, Discussion Paper (2019), 92.
35 DPI Report, above n 33, 494.
36 Issues Paper, 70-72.
37 Issues Paper, 71.
38 Issues Paper, 72.

rather than through common law. It is high time that Australian law caught up with other common law jurisdictions, including New Zealand, Canada, the US and the UK in this regard.[39]

7.2 Gaps in the legal framework remain

The legal framework for the protection of privacy is patchy, relying on various federal and state legislation, equity and some criminal offences. There are also limitations to each of these protections:

- in relation to the ***Privacy Act*** as it currently stands, it fails to protect against invasions of privacy that involve interference with one's person or territory. The protections are limited to the protection of personal information. The ALRC's proposed tort in relation to intrusion upon seclusion is not dealt with by the *Privacy Act*. The proposed tort in relation to misuse of private information is also not covered by the *Privacy Act* in a vast range of circumstances, including where that misuse is is by another private individual, by a small business operator, by a media organisation, or registered political parties, or the misuse is in relation to employee records.

  These limitations mean that even if a direct right of action allowing individuals to litigate claims for breaches of their rights under the Act is legislated, individuals will nevertheless have limited recourse for invasions to their privacy which lie outside the parameters of the legislation. Considering that the *Privacy Act* covers only a small part of the ALRC's proposed tort, a direct right of action will not provide sufficient remedy in itself;

- in relation to equitable remedies available for **breach of confidence**, the Issues Paper notes some of the limitations to this avenue. A cause of action for breach of confidence may be available in relation to information which is provided in confidence and in circumstances where there is a pre-existing obligation of which the respondent is aware, and there is unauthorised use of that confidential information. Breaches of confidence may also arise where a party comes into possession of information which they know, or ought to know, is confidential.[40] But the limitations here are clear – again, it is limited to breaches relating to information and does not cover intrusions upon seclusion (where such intrusion is not accompanied by misuse of personal information). It also remains unclear whether equitable compensation is available for emotional distress arising from a breach of confidence,[41] notwithstanding two decisions of state courts which answered the question in the affirmative;[42]

- **criminal offences** also provide only limited protections of individual privacy. They do not 'negate' the need for a tort of privacy on a policy basis. At the outset, we submit that the existence of criminal offences for certain types of privacy breaches does not negate the need for civil remedies for victims of such breaches. Civil remedies, including damages, declarations, injunctions and apologies are equally important to uphold privacy rights. To a limited extent, some of these remedies may be available for breach of confidence.

---

39 See discussion of frameworks in these jurisdictions in the VLRC Report, above n 29, 22-23, and in Normann Witzleb, 'Another Push for an Australian Privacy Tort – Context, Evaluation and Prospects' (2020) 94 Australian Law Journal 765.

40 ALRC Report, above n 30, [3.48].

41 Ibid, [3.50].

42 *Wilson v Ferguson* [2015] WASC 15; *Giller v Procopets* [2008] VSCA 236.

Further, as the Issues Paper identifies, federal and state criminal offences in relation to privacy primarily concern voyeurism and the non-consensual recording and sharing of intimate images. This covers only a certain type of serious breaches of privacy. It does not provide any protection for privacy breaches unrelated to intimate images or sexual gratification – for instance, victims of large scale data breaches.

7.3 A statutory tort

PIAC submits that a statutory cause of action is necessary. The recognition of a cause of action for breach of privacy should not be left to incremental development of common law through the courts. The reluctance of superior courts to date to embrace the cautious invitation extended by the High Court in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*[43] to develop a tort of privacy in Australia[44] suggests that common law development of such a tort may take a long time, if it ever happens. This development is made all the more difficult in circumstances where applicants have avoided framing their claims under a tort of privacy, even where the point may be arguable: see, for example, *Smethurst v Commissioner of Police*.[45] A new statutory cause of action would accord with public expectation that victims of invasion of privacy are not left without recourse to a legal remedy.

The creation of a statutory cause of action would have the following advantages over common law development:

- it is a less time-consuming process than waiting for appropriate cases (requiring determined applicants who are adequately funded and resourced) to come before the courts;
- it provides greater certainty and uniformity by clarifying rights and responsibilities;
- it prevents even greater patchwork in regulatory settings from eventuating, if some states develop a statutory cause of action and other states rely on slowly developing common law;
- it allows potential respondents, including businesses, to understand the scope of their obligations, to predict whether or not their conduct will give rise to legal liability for breach of privacy and to put in place appropriate procedures to minimise the risk of a breach;
- it avoids the need to try to fit breaches of privacy into pre-existing legal actions, such as breach of confidence – which again carries with it uncertainty for businesses, not knowing where or how equity and common law will develop;
- it does away with the distinction between equitable and tortious causes of action and allows for a more flexible approach to damages and remedies; and
- it strengthens the recognition of privacy in the law as a right in itself deserving of protection.

Given the limitations of the *Privacy Act* in dealing with personal information only, we consider that a new, standalone statute containing a tort for the serious invasion of privacy ought to be enacted. Any statutory tort should not be inserted into the *Privacy Act*.

---

43 (2001) 208 CLR 199.
44 *Giller v Procopets* [2004] VSC 113, [187]-[189] and *Kalaba v Commonwealth of Asutralia* [2004] FCA 763, [6].
45 [2020] HCA 14, [48], [86]-[90] (Kiefel CJ, Bell and Keane JJ), [197] (Gordon J), [205] (Edelman J)

PIAC submits the elements of the statutory tort should be as follows (addressing questions 59 to 61 of the Issues Paper).

7.3.1 Types of invasions of privacy

PIAC supports the ALRC's proposal that there be two forms of invasion of privacy which form the first element of the tort. The ALRC recommended an applicant be required to prove:

- there has been an intrusion of their seclusion or private affairs, including by unlawful surveillance, such as by taking a photo of someone in a change room; or
- there has been misuse or disclosure of private information, such as disclosure of their medical records to a newspaper or posting sexually explicit photographs of the person on the internet.[46]

Any new legislation should contain a non-exhaustive list of examples of conduct that may be an invasion of privacy. This would provide the public with guidance, and provide certainty and clarity by giving context to the cause of action and the circumstances in which it might arise. PIAC submits there needs to be sufficient flexibility in the Act for it to be appropriately adapted to changing social and technological circumstances.

PIAC also recommends that the cause of action extend to physical privacy intrusions such as unreasonable search and seizure, or media harassment. These physical privacy intrusions may not necessarily result in disclosure of private information, but may nonetheless amount to arbitrary or unlawful interference with privacy.

7.3.2 Reasonable expectation of privacy

PIAC submits that the tort should be actionable where a person in the position would have a 'reasonable expectation' of privacy in the circumstances, measured by an objective standard. PIAC considers the 'reasonable expectation' test is fluid enough to take account of factors such as the nature and incidence of the act, conduct or publication, the age and circumstances of the applicant, the relationship between the parties and the place where the alleged invasion of privacy took place. This is the standard recommended by the ALRC.[47]

PIAC supports the recommendation of the ALRC that a non-exhaustive list of matters be included to assist the court to determine whether the applicant would have had a reasonable expectation of privacy in all of the circumstances. These matters include, for example:

- the nature of the private information, including whether it relates to intimate or family matters, health or medical matters, or financial matters;
- the means used to obtain the private information or to intrude upon seclusion, including the use of any device or technology;
- the place where the intrusion occurred; and
- the purpose of the misuse, disclosure or intrusion.[48]

In addition to the factors proposed by the ALRC, PIAC recommends that 'cultural background' should be expressly included when a court considers the relevant attributes of the applicant. In

46 ALRC Report, above n 30, 73.
47 ALRC Report, above n 30, Recommendation 6-1.
48 ALRC Report, above n 30, Recommendation 6-2.

PIAC's experience of working with First Nations Peoples there are cultural expectations of privacy that will be relevant and require specific consideration. PIAC further recommends that the extent to which the individual is in a position of vulnerability also ought to be a factor in considering whether there was a reasonable expectation of privacy.

7.3.3 Fault: intentional, reckless or negligent invasion of privacy

In contrast to the ALRC's recommendation, PIAC considers that the tort should not be confined to intentional or reckless invasions of privacy, but should extend to negligent invasions of privacy. It is important that the tort extends to those negligent acts where the impact of the breach of privacy can be just as serious for the applicant as that of a deliberate or reckless breach. An organisation, for example, with inadequate security procedures might negligently release personal information about a number of its clients. It is undesirable that victims of these privacy breaches should have no legal recourse.

This is especially so in relation to big data breaches. In each of the public sector data breaches referred to above – being data breaches by Services NSW, the Department of Immigration and Border Protection and the Federal Court of Australia – the impact on victims may have been significant, involving sensitive information being published and potentially putting individuals in personal danger. There are countless examples of big data breaches in the business sector – for example, the Commonwealth Bank's 2018 data breach, in which it could not determine whether magnetic tapes containing information from almost 20 million customer accounts from 2000 to 2016 were securely destroyed; or a breach by Sonic HealthPlus, a subcontractor for Bupa, who was in turn contracted by the Department of Home Affairs, which led to the personal health information of 317 applicants for an Australian visa to be emailed to a member of the general public via Gmail. In many of these instances, it is unlikely that the privacy breach would reach the thresholds of 'intentional' or 'reckless'. That should not prevent legal recourse for individuals who are victims of invasions of their privacy arising from negligence.

We note that NSW's *Civil Remedies for Serious Invasions of Privacy Bill* proposes a differentiated fault element, whereby negligence is only included as a fault element for government entities or corporations, with individuals only liable for intentional or reckless conduct: see cl 11. PIAC considers this an innovative solution which warrants further consideration.

7.3.4 Proof of Damage

Any new legal action in privacy should be actionable *per se*. That is, PIAC considers that it would be inappropriate and potentially very restrictive to require an applicant to prove that any actual loss or damage arose from the alleged invasion of privacy. In many cases, there will be a lack of clear, provable damage arising from a breach of privacy. This is unsurprising: privacy is a human right. As such, it is designed to protect a facet of one's individual dignity. One's dignity is vitally important but its intrinsic nature makes it difficult to quantify in monetary terms the impact of any damage to it.

The majority of clients for whom PIAC has acted in breach of privacy matters have suffered distress, humiliation and insult as a result of invasions of their privacy, rather than any provable psychiatric or economic damage. In some cases, the effect of a breach of privacy may simply be to stop someone doing something that they would normally do. For example, if they have been

subjected to unauthorised surveillance, they may feel reluctant to leave their home. In this type of situation, it is difficult to point to any provable damage in a legal sense.

This was also the approach recommended by the ALRC,[49] NSW Standing Committee[50] and the VLRC.[51]

7.3.5 Defences

In order to balance competing public interests against an individual's right to privacy, PIAC submits that a number of defences should be included in the statutory framework. PIAC considers the following defences should be included in any legislation:

- the respondent's conduct was authorised or required by law;
- the respondent's conduct was incidental to the lawful right of defence of person or property, and was a reasonable and proportionate response to the threatened harm;
- consent, including implied consent – but only where that consent is specific to the conduct alleged to have breached the person's privacy;
- the respondent's conduct was in the public interest, where public interest is a limited concept and not any matter that the public may be interested in. This may include – as proposed by the ALRC – freedom of expression, the implied freedom of political communication, freedom of the media to investigate and report on matters of public concern, the proper administration of government, open justice, public health and safety and national security

Regarding the final public interest defence, it should be noted that the various law reform bodies have taken different views in their privacy inquiries. PIAC agrees with the approach taken by the VLRC, namely, that it is most appropriate for competing public interests to be one of a number of defences to the proposed cause of action. This is converse to the view of the ALRC that different public interests should be incorporated into the cause of action itself. PIAC agrees with the VLRC's recommendation that the public interest defence should specify that 'public interest is a limited concept and not any matter the public is interested in'.[52]

There are two problems with the alternative approach of incorporating a balancing test into the cause of action itself. First, it places an unreasonably onerous evidentiary burden on applicants and is likely to discourage the bringing of claims under the statute. Second, the question of balancing countervailing public interests only arises where the respondent seeks to rely on a public interest defence.

PIAC also cautions against the inclusion of wide categories of activities, organisations or types of activities or organisations that are automatically exempt from the operation of the proposed cause of action. If the cause of action is framed appropriately, there is no need for general exemptions.

7.3.6 Damages & remedies

PIAC agrees with the approach taken by the ALRC that a range of remedies should be made available to the court to order where a person has been aggrieved by an invasion of their privacy. Breaches of privacy may arise in a wide range of circumstances, and it is appropriate that the

---

49 ALRC Report, above n 30, Recommendation 8-2.
50 NSW Standing Committee Report, above n 31, [4.49].
51 VLRC Report, above n 29, [7.201]-[7.202].
52 VLRC Report, above n 29, [7.187].

available remedies reflect the varying impact that the invasion may have. In many of the privacy cases that PIAC has dealt with, clients have been less concerned with obtaining compensation than they have been with obtaining a comprehensive and meaningful apology from the respondent.

Accordingly, PIAC supports a range of possible remedies for breach of privacy, including

- monetary damages compensating for economic and non-economic loss;
- exemplary damages;
- an order requiring the respondent to apologise to the applicant;
- a correction order;
- an order for the delivery and destruction of material;
- an order requiring implementation of a policy or procedures;
- a declaration;
- other remedies or orders that the Court thinks appropriate in the circumstances.

PIAC also submits that the court should be empowered to deal with systemic breaches of privacy. It is not uncommon for conduct breaching privacy to be widespread, institutionalised and affect large numbers of people.

8. Conclusion

PIAC welcomes the review of the *Privacy Act* and the opportunity to comment on issues that should be addressed. The review provides an opportunity to update the Act to ensure it meets community expectations about the use of their personal information and their right to privacy, and provides a chance for Australian law to catch up with much of the common law world. PIAC looks forward to ongoing participation in this review.