Law Council
OF AUSTRALIA

Review of the *Privacy Act 1988* (Cth) – Issues Paper

Attorney-General's Department

17 December 2020

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639
Email mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

About the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and the Law Firms Australia, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar
- Law Firms Australia
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of more than 60,000 lawyers across Australia.

The Law Council is governed by a board of 23 Directors – one from each of the constituent bodies and six elected Executive members. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2020 Executive as at 1 January 2020 are:

- Ms Pauline Wright, President
- Dr Jacoba Brasch QC, President-elect
- Mr Tass Liveris, Treasurer
- Mr Ross Drinnan, Executive Member
- Mr Greg McIntyre SC, Executive Member
- Ms Caroline Counsel, Executive Member

The Secretariat serves the Law Council nationally and is based in Canberra.

Acknowledgement

The Law Council acknowledges the assistance of the Privacy Law and Media and Communications Committees of its Business Law Section, the Law Society of New South Wales, the Law Institute of Victoria, the Law Society of South Australia and the Law Society of Western Australia in the preparation of this submission.

Executive Summary

1. The Law Council appreciates the opportunity to provide this submission to the Attorney-General's Department (**the Department**) in response to the *Privacy Act Review Issues Paper* (**Issues Paper**).

2. The Law Council notes that the *Privacy Act 1988* (Cth) (**Privacy Act**) has now been in operation for over 30 years and that the *Privacy Amendment (Private Sector) Act 2000* (Cth) was introduced some 20 years ago, extending privacy obligations to the private sector to provide a minimum set of privacy protections for individuals. During this time there have been significant changes to the landscape in which these pieces of legislation operate and therefore the Law Council welcomes the current review of the legislative framework.

3. The Law Council has not sought to respond to each of the 68 questions tendered in the Issues Paper in the time available in which to respond. Instead, the Law Council's responses are grouped under the headings outlined in the Issues Paper, which are based on key themes or issues. The focus of the responses is on legal issues, noting that this area of law is highly sensitive to the speed of technological and social changes and impact on policy.

4. Noting that the Issues Paper is the first step in a broader review of the Privacy Act, the Law Council will endeavour to engage with its Constituent Bodies and other key stakeholders with the view to arriving at a settled and unified position on key privacy issues prior to participating in the next stage of the review.

5. The Law Council looks forward to contributing to future components of the Department's review. At this point in the consultation process, the Law Council provides the following recommendations, designed to assist in the Department's development of a Discussion Paper in early 2021, namely that consideration be given to:

    - Reinforcing accountability as part of Australia's privacy framework. This needs to be considered in the context of other obligations and the limitations of the consent driven model.

    - Amending the objects of the Privacy Act to include ensuring that acts and practices of Australian Privacy Principle (**APP**) entities do not unreasonably interfere with the privacy of individuals and providing enforceable rights for individuals to seek redress for an interference with their privacy, in addition to any complaints process.

    - Including, as expressly operative concepts within the APPs, additional matters to help to balance the rights of individuals and responsibility and accountability of APP entities, noting that these are not mutually exclusive. In this regard, consideration should extend to including:

        - responsibility and accountability of APP entities in their management of personal information about individuals; and

        - reasonableness and fairness of an act or practice of an APP entity in their management of personal information about individuals, having regard to:

            - a right of individuals in protection of the privacy of individuals;

    - societal interests in the protection of the privacy of individuals; and
    - the interests of entities in carrying out their functions or activities.
- resolving the inconsistency between the terms 'relate to' and 'about' to address any unintended consequences under the current definition of 'personal information' in section 6 of the Privacy Act.
- Amending the Privacy Act to expressly recognise pseudonymisation, use of controlled and safeguarded data environments and privacy enhancing technologies, processes and practices as a means to address the risk of re-identification that may cause harm to an individual.
- Amending the Privacy Act or subordinate legislation to identify and address common situations, such as business dealings with personal information, including the sale of personal information. Consideration could also be given to the development of industry specific codes or guidelines from regulators in relation to particular matters.
- Revisiting the small business exemption in its current form with a view to removing it. Any decision to remove the exemption for small business should be accompanied by Government-issued guidance, training and other assistance to support business compliance.
- Removing the employee records and political exemptions.
- Removing the journalism exemption. Such removal should appropriately balance the privacy rights of the individual with the need for free speech.
- Supplementing the framework for data privacy regulation with new (more descriptive) accountability requirements.
- Australia making an application for adequacy under Article 45 of the *General Data Protection Regulation* (**GDPR**). Questions concerning key definitions, the scope of exemptions (if any) and rights and remedies available to individuals are to be considered in this context and the working combination of the proposed changes noted and considered.
- Bringing the penalties for breaches of privacy in line with the penalties available under the Australian Consumer Law (consistent with the views of the Australian Competition and Consumer Commission (**ACCC**) in its *Digital Platforms Inquiry*).
- Increasing the resources of the Australian Information Commissioner (**OAIC**) to apply to the courts for civil penalties for serious or repeated interferences with privacy and to further its enforcement activities.
- Conducting research on the impact of notification to affected individuals and what makes for an effective notification in the context of the harm (if any).
- Establishing an independent certification body for data processed by certain companies.
- Undertaking a fundamental review of Australia's data protection and privacy legislation, which is specifically targeted at AI, is informed by the experiences of other jurisdictions and complements the current privacy legislation review processes.

6. The Law Council submits that care should be taken, and caution exercised, to ensure that all proposed changes are reviewed in the context of the regime as a whole, noting the potential for unintended consequences and the fact that all the changes must work in combination with each other. This may require further legal research and consultation with potentially a diverse set of stakeholders.

General Comments

7. The Law Council considers that the Privacy Act, can be enhanced to better equip entities, regulators, and individuals to deal with emerging technologies and new methods (and speed) of generating and transferring information.

8. The world has transformed considerably since the Privacy Act's inception with the advent of the internet facilitating a proliferation of data and information. Social media, new banking and payment methods, and a shift to move business to online formats (including legal transactions such as conveyances, and anti-fraud measures) have substantially altered the way in which we use, treat and generate information. The amount of personal information (much of which will be considered sensitive) being transferred with little to no oversight has expanded exponentially, and the Law Council is of the view that Privacy Act can be modified to better safeguard against misuse, mistake, or malfeasance. The implications for an individual in the event of a privacy breach can be significant, and permanent.

9. The Law Council considers that the APPs can be improved, and their scope extended to apply to more entities and a greater variety of circumstances.

10. The Law Council considers that 2021 presents a good opportunity to review the Privacy Act in light of significant international developments, including the positions represented by a number of Australia's key trading, diplomatic, and security partners including the European Union (**EU**), United Kingdom, Canada, Singapore and various jurisdictions in the United States.

11. Finally, while the current review of the Privacy Act is not considering any privacy issues related to the COVID-19 pandemic, the Law Council suggests that the pandemic itself has highlighted some shortcomings of the Privacy Act and of Australian privacy regulation more generally.

From 'notice and consent' (user privacy self-management) to accountability of APP entities

12. The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth), which commenced in March 2014, implemented a number of the recommendations made by the Australian Law Reform Commission (**ALRC**) in its *For Your Information* report, tabled in August 2008.[1]

13. These amendments predated the now ubiquitous use of smartphones, social media, digital platforms, e-commerce, health and wellness devices and other Internet of Things services, as well as automated decision making by governments and businesses using diverse, joined and analysed data points relating to behaviour of individuals, whether or not reasonably identifiable.

[1] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, August 2008).

14. The Law Council notes that *Bill C-11 for An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act* was introduced into the House of Commons of Canada on 17 November 2020. Clause 12 of that Bill provides a list of factors that must be considered in determining whether a collection, use or disclosure is only for purposes that a reasonable person would consider appropriate in the circumstances, being:

    (a) the sensitivity of the personal information;

    (b) whether the purposes represent legitimate business needs of the organisation;

    (c) the effectiveness of the collection, use or disclosure in meeting the organisation's legitimate business needs;

    (d) whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits; and

    (e) whether the individual's loss of privacy is proportionate to the benefits in light of any measures, technical or otherwise, implemented by the organisation to mitigate the impacts of the loss of privacy on the individual.

15. In line with the above, the Law Council suggests that consideration is given to updating the Privacy Act to expressly address how the obligation on accountability may be addressed and legitimate use and disclosure of personal information articulated.

Recommendation:

- **Consideration should be given to reinforcing accountability as part of Australia's privacy framework. This needs to be considered in the context of other obligations and the limitations of the consent driven model.**

Objectives of the Privacy Act (Question 1)

16. The Law Council notes that the objectives do not form part of the operative provisions of the Act.

17. The Law Council submits that consideration should be given to including an operative provision to the effect that APP entities should only collect, use or disclose personal information about individuals to the extent, and for purposes, that a reasonable person would consider appropriate in the circumstances, similar to the lawful grounds of processing expressed in Article 6 of the GDPR.

18. The objects clause should also include an object of promoting fair and responsible handling by APP entities of personal information about individuals, through implementation of reliable and effective data governance, and appropriate monitoring, oversight and review processes and practices.

19. The Law Council also suggests that a further objective be included of providing enforceable rights for individuals to seek redress for an interference with their privacy, in addition to any complaints process.

Recommendation:

- **Consideration should be given to amending the objects of the Privacy Act to include ensuring that acts and practices of APP entities do not unreasonably interfere with the privacy of individuals and providing enforceable rights for individuals to seek redress for an interference with their privacy, in addition to any complaints process.**

Australian Privacy Principles

20. The Law Council notes that the Privacy Act does not define 'privacy' or the circumstances in which an act or practice is to be taken to cause harm to an individual. Most operative provisions in the Privacy Act use 'privacy' as an adjective in a description of something else (for example, privacy policy, Privacy Act, Australian Privacy Principle, privacy authorities, and so on). Section 2A of the Privacy Act is one of the rare instances where privacy is used as a noun and concept in and of itself. However, section 2A is not an operative provision, and the concept is not further explained. The Privacy Act does not assess risk or harm on the privacy of individuals or require any assessment of whether any impact is reasonable or unreasonable. Indeed, the Privacy Act does not generally use risk or harm (other than in relation to whether a data beach is notifiable) as operative concepts. The Act does not purport to create a fundamental right to privacy.[2] Rather, it establishes a co-regulatory model enabling privacy rights to be balanced and, in some cases, overridden by other rights and obligations.

21. The Law Council recommends that the Department consider the feasibility of including, as expressly operative concepts within the Act, the following:

    - responsibility and accountability of APP entities in their management of personal information about individuals; and
    - reasonableness and fairness of an act or practice of an APP entity in their management of personal information about individuals, having regard to:
        - a right of individuals in protection of the privacy of individuals;
        - societal interests in the protection of the privacy of individuals; and
        - the interests of entities in carrying out their functions or activities.

22. In this way, such expressly operative concepts could become relevant considerations in determining whether and when there is an interference with the privacy of an individual.

[2] As is the case under European Union law.

Recommendation:

- **Consideration should be given to including, as expressly operative concepts within the APPs, additional matters to help to balance the rights of individuals and responsibility and accountability of APP entities, noting that these are not mutually exclusive. In this regard, consideration should extend to including:**
  - **responsibility and accountability of APP entities in their management of personal information about individuals; and**
  - **reasonableness and fairness of an act or practice of an APP entity in their management of personal information about individuals, having regard to:**
    - **a right of individuals in protection of the privacy of individuals;**
    - **societal interests in the protection of the privacy of individuals; and**
    - **the interests of entities in carrying out their functions or activities.**

Definition of personal information (Questions 2 to 5)

23. The Law Council considers that the definition of 'personal information' should be broad enough to encompass an 'identified individual' and 'individuals who are reasonably identifiable' and remain technology neutral. Currently, there is some argument as to the scope of the information to be covered as it 'relates' to an individual or is 'about' an individual. This may be confusing to both individuals and entities alike.

24. Section 6 of the Privacy Act relevantly provides that personal information is:

> *Information or an opinion about an identified individual, or an individual who is reasonably identifiable:*
>
> *(a) whether the information or opinion is true or not, and*
>
> *(b) whether the information or opinion is recorded in a material form or not.*

25. The definition covers two categories of information. The first is information about an identified individual. This would include information such as name, address, or phone number, which directly identifies an individual.

26. The second category is information about an individual who is reasonably identifiable. The Law Council considers that reference to 'about' and 'relate' should be clarified in the Privacy Act. The Law Council notes that the refence to reasonably identifiable and matters noted in items (a) and (b) of the definition make the definition sufficiently broad to encompass the matters such as geolocation or matters that individuate a person without identifying that person as covered by the first limb of the definition noted above.

27. Recent litigation regarding the definition of personal information has not sufficiently clarified the legislative definition of what constitutes personal information for the

purposes of data collection. In *Privacy Commissioner v Telstra Corporation Ltd*,[3] the appeal arose due to differences in the way in which the Privacy Commissioner and the Administrative Appeals Tribunal approached interpretations of personal information. With the Federal Court of Australia's consideration limited to narrowly defined grounds of appeal, the Court was only required to determine the meaning of the phrase 'about an individual', and only provided guidance in assessing whether information meets the definition personal information.

28. The Law Council supports a reconsideration of the definition of personal information with the view to clarifying the uncertainty regarding technical data, in line with recommendation 16(a) of the ACCC's *Digital Platforms Inquiry*.[4] In the Law Council's view, there is merit in expressly aligning the language used in Privacy Act and the Consumer Data Right regimes as well as the GDPR, provided the definition preserves technological neutrality.

29. The Law Council notes that the current definition would include inferred personal information and already provides important protection of individuals, particularly individuals on social media platforms who are targeted by advertisers based on inferred personal information. To the extent that this is not clear, the Act and additional guidance can address this issue.

30. In lieu of clear guidance by the courts, the Law Council recommends amendment to the precise meaning and scope of the term to ensure that organisations better understand when information collected becomes personal information.

31. Guidance should reconcile Australia's protection of personal information with the GDPR broader protections of 'any information relating to an identified or identifiable natural person', which can include 'inferred' or 'derived data' created about individuals.[5] Responding to the absence of clear guidance from the court, the Law Council supports the Productivity Commission's finding that due to personal information having always attracted an element of uncertainty, its definition under the Privacy Act ought to be clarified.[6]

Recommendation:

- **Consideration should be given to resolving the inconsistency between the terms 'relate to' and 'about' to address any unintended consequences under the current definition of 'personal information' in section 6 of the Privacy Act.[7]**

32. The Law Council cautions against an approach within the Privacy Act to require de-identification to remove the risk of re-identification of any individual entirely. Rather, an assessment of whether an individual is identifiable should be made on the basis of whether, in the relevant circumstances, the risk of re-identification that may cause harm to an individual can be reasonably assessed as very low.

33. In this regard, relevant circumstances could include context of the data, and take into account technical, operational and legal controls and safeguards in relation to access to, and use of, relevant information and other factors that may impact on the possibility

[3] [2017] FCAFC 4.
[4] Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, July 2019) rec 16(a).
[5] *General Data Protection Regulation* (European Union) art 4 ('*GDPR*').
[6] Productivity Commission, *Data Availability and Use* (Report No 82, 31 March 2017) 34 ('Finding 3.4').
[7] Noting that *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4 was decided under the now superseded definition of personal information.

of re-identification or incidence of harm to an individual. This could include improvements over time in algorithms and technologies for mosaic or pattern recognition and risks of attribute disclosure or spontaneous recognition.

34. Further, the Law Council suggests that consideration should be given to amending the Privacy Act to expressly recognise pseudonymisation, use of controlled and safeguarded data environments and privacy enhancing technologies, processes and practices as a means to address the risk of re-identification that may cause harm to an individual.

Recommendation:

- **Consideration should be given to amending the Privacy Act to expressly recognise pseudonymisation, use of controlled and safeguarded data environments and privacy enhancing technologies, processes and practices as a means to address the risk of re-identification that may cause harm to an individual.**

Flexibility of the APPs in regulating and protecting privacy (Question 6)

35. The current legislative framework generally works well to facilitate technological neutrality and a risk-based, principles led approach. Data privacy laws around the world are principles-based, and in the Law Council's view, this remains the best approach. However, this matter warrants further consideration once priorities are set and attention turns to the drafting of required amendments. For example, some APPs may benefit from additional guidance.

36. The Law Council considers that there is scope for greater clarity around protections and obligations in the current legislative framework. To achieve this, the Law Council suggests that consideration could be given to either amending the Privacy Act or subordinate legislation to identify and address more common situations, such as business dealings with personal information, including the sale of personal information. Consideration could also be given to the development of codes or guidelines from regulators in relation to particular industries which may benefit from such guidance.

37. The framework could be improved by providing clarity for stakeholders, including insolvency practitioners or corporate trustees, who may become responsible for dealing with personal information despite not being involved when the collection of such personal information occurred. In particular, the Law Council notes that liquidators are often made offers to purchase a distressed company's client list (mostly service-based companies), and the Law Council suggests that they would benefit from having clear provisions which set out their obligations when dealing with personal information.

Recommendation:

- **Consideration should be given to amending the Privacy Act or subordinate legislation to identify and address common situations, such as business dealings with personal information, including the sale of personal information. Consideration could also be given to the development of industry specific codes or guidelines from regulators in relation to particular matters.**

Exemptions

Small business exemption (Questions 7 to 12)

38. In its current form, the Privacy Act provides for an exemption for agencies and organisations with an annual turnover of less than $3 million,[8] although these entities are bound by the APPs in certain circumstances.[9] Small businesses and not-for-profit organisations that would otherwise not be covered by the Privacy Act retain the choice to be treated as an organisation for the purposes of the Act, by publicly committing to good privacy practices and adhering to the APPs.[10]

39. There are a range of considerations at play in considering an equitable regulatory regime for small businesses which balances privacy risk with the need to avoid an overly burdensome compliance regime.

40. On one view, there is limited justification for small businesses not to comply with basic privacy protections, supporting the position that minimum threshold should be removed in its entirety. In this regard, it is noted that ninety-three per cent of Australian businesses have an annual turnover of $2 million or less.[11] This means that only a small percentage of Australian businesses are subject to the obligations under the Privacy Act (noting that the Privacy Act threshold is $3 million). However, nearly all Australian businesses (by virtue of payment methods and ecommerce) will collect, use and may even disclose personal information.

41. Processes and practices for compliance with the Privacy Act should now be quite well understood, and therefore may no longer be considered a significant compliance cost for businesses that collect and handle personal information about individuals as a reasonable incident to their core business.

42. Where handling of personal information is a core business activity, the carve-in from the small business exemption will generally mean that the Privacy Act already operates. In most cases, businesses do not pay or otherwise give an individual any benefit for collection or use of their personal information. Without any obligations being imposed on small businesses, individuals are at both a significant disadvantage commercially (it is well established that personal information is a valuable revenue-generating commodity when leveraged), and are subject to their personal information being exposed without protection. The benefits that businesses gain from collection

[8] *Privacy Act 1988* (Cth) ss 6C, 6D.
[9] Ibid s 6D(4).
[10] Office of the Australian Privacy Commissioner, *Privacy Opt-in Register* (Web Page) <https://www.oaic.gov.au/privacy/privacy-registers/privacy-opt-in-register/>.
[11] Australian Bureau of Statistics, *Counts of Australian Businesses, including Entries and Exits* (Catalogue No 8165.0, 20 February 2020). The Law Council notes that the threshold under the Privacy Act is annual turnover less than $3 million.

and handling of personal information may mean that the burden of compliance with the Privacy Act is a reasonable cost of doing business responsibly and fairly.

43. It is noted that many small businesses are involved in providing to commercial clients who insist that a given business agreed to be covered by the Privacy Act simply to avoid arguments about the scope of the exemption. This is common in the information technology and human resources related service industries. Removal or additional clarity as to the scope of the enforcement may assist to ease the compliance burden on the small business and its clients. This can make it difficult to administer and apply in a consistent manner.

44. The Law Council queries whether the small business exemption in its current form strikes the right balance between protecting the privacy rights of individuals and avoiding imposing onerous obligations on smaller enterprises.

45. The Law Council supports the recommendation of the OAIC that exemptions should be minimised to achieve uniformity and consistency and require an ongoing review of their suitability.[12]

46. If the exemption were to be removed, acknowledging that new compliance requirements may be an impost on business, it may be worth considering a transition period to removing the exemption and ensuring that any legislative amendments be accompanied by Government-issued guidance, training and other assistance to support business compliance. The Privacy Commissioner should also be authorised to make class exemptions from requirements of the Privacy Act if, in practice, compliance with specific obligations proves unduly burdensome for certain small businesses as a class.

Recommendation:

- **Consideration should be given to revisiting the small business exemption in its current form with a view to removing it. Any decision to remove the exemption for small business should be accompanied by Government-issued guidance, training, and other assistance to support business compliance.**

Employee exemption (Questions 13 to 15)

47. The employment relationship naturally gives rise to the need to collect and generate a vast volume of personal information which is often sensitive. Further, the workplace is often a place where employees may be exposed to technologies such as biometric, fingerprint or other scanners and artificial intelligence (**AI**) to improve security or productivity, or fatigue monitoring technology to promote workplace health and safety. Such programs will (in addition to the employing entity) include many other service providers and their providers in turn. Typically, such programs use and generate a large volume of personal information (including sensitive personal information).

48. By and large, the implementation of these technologies is not based on consent of the employees. Naturally, arguments arise about the nature of the impact on privacy and impact on other workplace rights.[13] The scope for disagreement is likely to grow as more tools are used to monitor the performance and behaviour of employees,

[12] Office of the Australian Privacy Commissioner, Submission PR 215 (28 February 2007) cited in Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, August 2008) [33.41].

[13] *Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946 (1 May 2019) (Full Bench of the Fair Work Commission).

particularly those in regulated industries, such as financial services where monitoring and surveillance is often required to address codes of conduct and compliance related obligations applicable in the sector. In mining and engineering industries, testing, screening and forms of monitoring and surveillance address health and safety matters. These complexities are magnified for global organisations, seeking to treat all employees fairly and consistently across the workforce, despite the location of their employment.

49. The Privacy Act, together with guidelines provided by the OAIC suggests that employers can lawfully store employee data without breaching the Act if the employee record relates directly to the employment.[14] However, this has been cast into doubt and scope of the exemption tested by the recent decision of the Fair Work Commission in *Lee v Superior Wood*, which decided that requiring an employee to consent to biometric attendance scanning was not a lawful direction as it infringed on the employee's rights under the Privacy Act.[15] The effect of this decision is that the exemption relating to employee records only applies to data already held by the employer, and does not encompass records that are 'yet to be held by an organisation'.[16] The decision that the employment exemption does not apply until the information is collected, subjects only the collection process to the Privacy Act. Where employees are entitled to refuse to allow their employer to collect and store 'sensitive information' about them, including biometric data and fingerprints, there may be little utility of retaining this exemption.

50. The Law Council suggest that the employee records exemption fails to provide the required clarity to employers seeking to comply with their respective compliance obligations and employees seeking to have certainty as to their privacy rights in the workplace.[17] The exemption is of itself not comprehensive and remains difficult to apply as a matter of practice.[18] Contractors and other workplace participants are excluded and complex factual arguments arise as to whether a given practice is *directly* related to the *current or former employment relationship* and held in the employee record *relating to the* individual (emphasis added).[19]

51. Moreover, the employee records exemption does not cover state or territory government entities under the Privacy Act,[20] as well as organisations acting under Commonwealth/state contract who would often hold extremely sensitive or intimate information, [21] such as health, financial information, family details and the results of psychological tests conducted prior to employment.[22]

---

[14] Office of the Australian Information Commissioner, 'Employee Records Exemption' (Web Page, December 2015) <https://www.oaic.gov.au/privacy/privacy-for-organisations/employee-records-exemption/>.
[15] [2019] FWCFB 2946 (1 May 2019) [14].
[16] *Privacy Act 1988* (Cth) s 7B; *Lee v Superior Wood* [2019] FWCFB 2946 (1 May 2019) [54].
[17] See guidance on how to assess surveillance measures in the European Data Protection Board's *Recommendations 2/2020 on the European Essential Guarantees for surveillance measures* (adopted on 10 November 2020), with interference with data privacy rights by surveillance measures only being justifiable where certain essential guarantees are in place: European Data Protection Board, *Recommendations 2/2020 on the European Essential Guarantees for surveillance measures* (10 November 2020) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf>.
[18] This is especially so for global organisations complying with data protection requirements without a corresponding exception for employees. In fact, to the contrary, in many countries (such as Germany) employee privacy receives a heightened sense of protection noting the sensitive nature of data to be processed and lack of bargaining power.
[19] *Privacy Act 1988* (Cth) s 7(B)(3).
[20] Ibid s 6C.
[21] Ibid ss 7B (2), (5).
[22] House of Representatives Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (June 2000), [3.30].

52. Based on the above, the Law Council recommends that consideration be given to the removal of this exemption. An individual faces the same privacy risks regardless of whether their information is disclosed by an employer, or a business with which they have interacted, and therefore employee information should be given the same protection as other information under the APP. In this regard, the Law Council notes the conclusion of the Standing Committee on Legal and Social Affairs in relation to this issue, which found that employees should be entitled to expect the necessary confidentiality of their information is ensured.[23]

53. The Law Council understands that Australia is an outlier among countries with comprehensive data privacy laws as Australia is the only such nation to exclude employee personal information from the operation of data privacy laws. Removing this exemption would likely bring Australian privacy law into line with Australia's international trading partners, for example jurisdictions within the EU, Canada and New Zealand. In doing so, such an amendment would likely improve efficiencies for businesses (both Australian and international businesses) which have staff in Australia and abroad, as a similar set of laws regarding employee privacy would simplify processes for staff when moving between locations.

54. However, the Law Council notes that these issues will need to be considered in light relevant industrial laws and workplace surveillance legislation that prescribes various notice and consent requirements for workplace surveillance regulated under state-based legislation. The degree of overlap with other fields of law and the practical realities of technology implementations suggests that consent will be of limited value in the employment context, especially once the relationship is on foot. Protection will need to come from transparency and accountability measures, augmented with consent where genuine choice is an option.

Recommendation:

- **Consideration should be given to the removal of the employee records exemption.**

Political exemption (Question 16)

55. The Law Council considers that although political parties should be allowed to process personal information they should also be required to comply with applicable laws. In the Law Council's view there is little policy justification for this exemption and that therefore consideration should be given to removing the exemption from the Privacy Act.

Recommendation:

- **Consideration should be given to removing the political exemption.**

Journalism exemption (Questions 17 to 19)

56. There are good policy reasons to reconsider this exemption noting the increased volume of publication by alternative channels.

57. Should the exemption be retained, the Law Council is of the view that consideration should be had regarding the preconditions.

[23] Ibid [3.33].

58. One precondition to the operation of the current exemption is that a media organisation is 'publicly committed' to 'observe standards' that 'have been published in writing by the organisation or a person or body representing a class of media organisations'.[24] In the case of non-broadcast media, this creates a situation where media organisations are able to write their own exemption, without any precondition of review or approval by any third party, regulator or otherwise.

59. The Law Council appreciates that assertion of legitimate expectations of individuals to personal privacy should not be allowed to automatically block fair and vigorous reporting and free speech enjoyed in an open democracy. However, consideration should be given as to whether it is appropriate for review and oversight of a media organisation's balancing of public interest and of legitimate expectations of privacy of individuals to be left solely to media organisations, and effectively free of any sanctions or even real negative incentives.

60. The Law Council notes that New Zealand recently renewed an exemption for a 'news entity', to the extent that it is carrying on 'news activities'.[25] 'News activity' is defined as gathering, preparing, or compiling, for the purposes of publication, any news, observations on news and current affairs, and publishing any news, observations on news and current affairs. This definition appears to include databases gathered in the course of investigative journalism, for obituaries or as 'backgrounders' for journalists, and hence appears intended to exclude rights of access and correction of affected individuals.

61. In the Law Council's view, the Department as part of this review, should consider a definition of 'news activity' appropriate to cover activities preparatory for and reasonably incidental to publication of news as broadly defined.

Recommendation:

- **Consideration should be given to removing the journalism exemption. Such removal to be appropriately balanced by balancing the privacy rights of the individual with the need for free speech.**

Notice and consent (Questions 20 to 35)

Consent requirements including default privacy settings

62. The Law Council acknowledges that strengthening consent requirements would be beneficial for specific classes of data, such as health data, and would work to strengthen individual privacy. However, in principle, general consent should not be exclusively relied upon. A recent study of the EU's GDPR has observed the consequences of general consent requirements,[26] including issues with consent fatigue.[27] The study also concluded that opt-out consent banners 'are unlikely to produce intentional/meaningful consent expression'.[28] Without transparency and

[24] *Privacy Act 1988* (Cth) s 7B(4)(b).
[25] *Privacy Act 2020* (NZ) s 8(b)(x).
[26] *GDPR* art 6.
[27] Christine Utz et al, '(Un)informed Consent: Studying GDPR Consent Notices in the Field' (Conference Paper, ACM SIGSAC Conference on Computer and Communications Security, 13 November 2019) <https://dl.acm.org/doi/pdf/10.1145/3319535.3354212> ('(Un)informed Consent').
[28] Ibid 2.

clarity, it is unlikely that consent would be informed and unambiguous – particularly where privacy policies are lengthy, complex, vague and difficult to navigate.[29]

63. To address distrust surrounding informed consent, the Law Council suggests that a key focus of reform should instead be centred on improving transparency and clarity, rather than requesting systematic consents in a chain of multiple (often instantaneous) data transfers.

64. The ACCC has acknowledged that information asymmetry and power imbalances affect people's capacity to demonstrate consent and exercise choice.[30] Consideration should be had to the impact for vulnerable people (for example, for reasons of disability, limited education, or financial pressure), who may be at risk of not fully appreciating what providing consent means.

Default privacy settings

65. A survey conducted evaluating consumer's knowledge of data collection in the EU, demonstrates that the predominant assumption is that 'no data is collected unless [consumers] make a decision' recommending that while it is not the current practice, 'privacy by default is the expected functionality'.[31]

66. The OAIC states that it is the responsibility of a business to ensure that withdrawal of consent is as easy as giving consent, and businesses 'must inform individuals about this right to withdraw consent'.[32] However, lack of transparency and difficulty in navigating default privacy settings may risk consumers merely 'clicking through' any disclosures and consent agreements without understanding how their data will be used. In the interests of the privacy of consumers, consideration should be given to the appropriateness of a 'tick-box' and/or pre-filled approach to consent.

67. This approach to privacy by design is consistent with the principle that should an organisation be benefiting from consumer's data, then that organisation should bear the burden of ensuring informed consent within the default privacy settings. The economic costs for a person to correct/retrieve/delete their own record is likely to unfairly outweigh the initial 'cost' of the organisation who collected their data.

68. As discussed above, the notice and consent requirements are increasingly problematic. The Law Council suggests that as part of the current review, consideration be given to developing a new requirement for organisations to only collect, use or disclose personal information about individuals to the extent and for purposes that a reasonable person would consider appropriate in the circumstances.

69. Many data collections are intermediated by devices, such as the Internet of Things devices, where the affected individual is not the person notified or providing consent. Consumers may already be overwhelmed or fatigued by information. Provision of more, or even better, information places the onus on the consumer to then read, assimilate and evaluate that information.

70. Further, personal information about an individual collected for a different primary purpose is able to be re-used, for example in the artificial intelligence context, to inform how a particular individual or household will be dealt with, in circumstances

[29] *GDPR* art 4(11).
[30] Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, July 2019) ch 7.
[31] Christine Utz et al, '(Un)informed Consent', 13 (emphasis added).
[32] *GDPR* art 7(3); Office of the Australian Information Commissioner, 'Australian entities and the EU General Data Protection Regulation (GDPR)' (Web Page, 8 June 2018) <https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation/>.

where because an individual is not identifiable to the operator of the AI system, the secondary use is not a regulated secondary use of personal information about an (identifiable) individual. Data and technology enable decision-makers to use information about particular (but not identified or identifiable) individuals or households and to make decisions about how an individual or household is treated without the affected individual or household knowing that this 'deidentified information' has been collected, used and disclosed in this way, with potential adverse consequences to their rights and interests.

71. Even where an individual is identifiable and the relevant secondary use is therefore regulated under privacy law, issues often arise as to the adequacy of notice and consent, and in particular, whether purported consent is informed, understood, explicit and current.

72. The existing data privacy laws are intended to empower individuals by informing them around how data about them may be being collected and used, and thereby enable them to exercise a choice. This is the 'notice and choice', or 'notice and consent', framework for data privacy regulation. However, the capacity to choose, or withhold consent, is often significantly constrained.

73. For clarity, the Law Council is not proposing that the 'notice and choice' or 'notice and consent' framework be removed in its entirety or that these concepts are incompatible. Rather, consideration should be given to supplementing the existing framework with the new accountability requirements (based on reasonableness) and a requirement for APP entities to develop and to implement a privacy management program, in addition to the requirements of APP 1.

Recommendation:

- **Consideration should be given to supplementing the framework for data privacy regulation with new (more descriptive) accountability requirements.**

Control and security of personal information (Questions 43 to 47)

Security and retention

74. The increasing number of notified data breaches under the data breach scheme indicate that neither humans nor technology are infallible when it comes to securing personal information.

75. The Law Council also notes that there is a strong agreement to suggest that APP entities should be provided with clear incentives to encrypt personal information, or otherwise to implement technological protection measures and operational procedures to mitigate risks of data exfiltration, including risks arising through internal inadvertence or error, and external malicious extraction. Additional clarity will be helpful where breaches involve multiple third parties. This is related to the issues of accountability as noted above.

76. The requirements under the Privacy Act placed on entities to destroy or de-identify personal information are generally reasonable as they are principles-based and allow for risk-based decisions. Additional guidance as to what may be reasonable may assist to promote compliance. This will be especially relevant in regulated industries

where the question of deletion and de-identification is often linked with ability to comply with other obligations (for example, in human resources and finance related matters).

Erasure of personal information

77. This is a complex area, often leading to inconsistent and potentially conflicting outcomes. The Law Council notes the Productivity Commission's finding that the 'human rights' framing of privacy is unhelpful, as it is 'unlikely to see cultural change' because 'it encourages data to be viewed as a risk rather than an asset'.[33]

78. The 'right to erasure' requires careful consideration and detailed consultation with a broad cross section of stakeholders, not least because there may be numerous unintended consequences. As a minimum, very careful consideration will need to be given the following factors:

- the 'right to erasure' often applies only to personal information collected based on consent. Substantial questions about the role of consent as part of a broader regulatory structure and needs to be addressed before 'right to erasure' can be addressed; and

- the 'right to erasure' is the subject of multiple intricate exemptions which will need to be considered in the context of the law in Australia. This will raise questions of intellectual property rights, competition law and media law related issues. Careful and detailed analysis will be required of regime that require entities to retain data and address how these requirements interact with protection of personal information.

79. The Law Council will continue to engage with this issue throughout the course of the current review, and beyond.

80. In considering this issue, the right to be forgotten would benefit from a focus on a property right to personal information, similar to the terms found under a confidentiality agreement (where, upon the conclusion of a business relationship, the owner has the right to direct the holder to return the information or destroy it). Similarly, the view of personal information being property would also guide the discussions regarding data rectification and portability.

81. Moreover, there would need to be a balance between what might be one person's right to data with another person's right to erasure, as data can often be interlinked or inseparable.[34] A case of such conflict might arise when a user's right to data portability impinges on other users' right to be forgotten, because the data of the users are inseparable and prevent the latter from having their data erased.[35]

82. Consistent with the Law Council's submission to the Treasury's *Digital Platforms Inquiry*,[36] it may be useful instead to explore the exemption of information collected in prescribed circumstances. As an example, the Law Council has noted that it would not be practicable to erase one person from CCTV footage.[37] It is also not practicable to delete personal information in unstructured data environments or where the data

[33] Productivity Commission, *Data Availability and Use* (Inquiry Report No 82, 31 March 2017) 308.
[34] Wenlong Li, 'A Tale of Two Rights: Exploring the Potential Conflict between Right to Data Portability and Right to be Forgotten under the General Data Protection Regulation' (2018) *International Data Privacy Law* 8(4) 309-17.
[35] Ibid.
[36] Law Council of Australia, Submission to the Treasury, *Digital Platforms Inquiry* (18 September 2019) [31].
[37] Ibid.

forms part of a larger set and connection to the person is obtuse, incidental or very limited.

Overseas data flows and third-party certification (Questions 48 to 52)

83. The Law Council considers that current mechanisms for notice in the Privacy Act are generally adequate.

84. On overseas data flows, the Privacy Act makes it clear that the transferring organisation remains accountable for the personal information transferred outside Australia. Subject to some exceptions, APP 8 requires that before an APP entity discloses personal information about an individual to an 'overseas recipient', the entity must take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information. Where an entity discloses personal information to an overseas recipient, it is accountable for an act or practice of the overseas recipient that would breach the APPs.[38] Under the Privacy Act, central to the cross-border discussion, are concepts such as use, disclosure and the ability to demonstrate 'effective control' of the information held by the regulated entity or agency, so called APP entities. This is based on APP 8 and the guidance of the OAIC.[39]

85. Generally, this means that many cross-border arrangements are documented in contracts dealing with the specific services (such provision of cloud-based services, sizable IT outsourcing programs and implementation of 'Software as a Service' arrangements). This provides for a degree of flexibility and clarity on cross border flows and does so on a transaction or case by case basis. Many global organisations incorporate models of data transfers applicable under the GDPR, such standard contractual clause (**SCC**) as approved by the European Commission and subject to the recent European Court of Justice in *Schrems and Facebook Ireland v Data Protection Commissioner* (**Schrems II**).[40] This has generally been non-contentious, and conflicts of laws issues potentially triggered by using a working combination of legal transfer mechanisms to address requirements of APP 8 remain untested.

86. The Law Council anticipates that, in the future, a more detailed mechanism will be required to demonstrate compliance with the SCCs as amended.[41] The Schrems II decision and pending changes to the SCCs have created some uncertainty and may pose a challenge to interoperability of the existing cross-border mechanisms.

87. The Law Council recommends that serious consideration be given to Australia making an application under Article 45 of the GDPR for adequacy under the GDPR (**adequacy**). Adequacy would involve an assessment of the regime as a whole with reference to matters such as the rule of law, effective enforcement of privacy rights, the existence and effective functioning of one or more independent supervisory

[38] *Privacy Act 1988* (Cth) s 16C.
[39] Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines* (July 2019) ch 8 <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information/>.
[40] (2020) CJEU Case C-311/18.
[41] European Data Protection Board, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (10 November 2020) <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en>.

authorities and the entry by Australia of the relevant conventions.[42] The advantages of a successful adequacy application include that:

- a 'transfer shall not require any specific authorisation' and would make transfers interoperable as these apply to the EU/European Economic Area;[43]
- some of the uncertainty created by the Schrems II decision would be removed; and
- it would not require that Australia replicates provisions of the GDPR. This allows Australia to retain many of the concepts and features of the Privacy Act and related rights and causes of action, provided that the regime itself is considered 'adequate' as assessed.

88. The Law Council notes that such an application could apply to Australia, as a country, a territory or one or more specified sectors (for example the private sector or the government sector).

89. The Law Council appreciates that consideration will require further research and a detailed review and is willing to provide the support as needed. The Law Council considers that the pending consideration of the issues raised at the Discussion Paper stage of the consultation process provide an opportunity to scope the relevant assessments and commence some of the preliminary consultation and research that will naturally be required. In addition, it allows the consideration of issues to be considered in the context of the entire regime, helping to ensure that the potential for unintended consequences is minimised. For example, issues such the scope of definition of personal information, existence of exemptions and the existence of a direct right of action or additional causes of action and other remedies would need to be considered as part of any assessment and the working combination or rights and remedies considered in context.

90. Additionally, consideration could be given to making the data controller/processor liable for the actions of the overseas parties, by reference to their respective capacity as controller/processor as defined in the GDPR.[44] The Productivity Commission supports the contention that, due to a lack of a comprehensive plan to capitalise on the use of data in innovative, value-adding ways, Australia has not achieved the extent that 'opportunities being taken overseas exemplify'.[45] In doing so, the Law Council suggests that there may be scope for the OAIC and Attorney-General to be able to prevent the data from flowing to countries that are deemed unsafe, or not in the national interest based on clearly specified factors and criteria.

Recommendation:

- **Consideration should be given to Australia making an application for adequacy under Article 45 of the GDPR. Questions concerning key definitions, the scope of exemptions (if any) and rights and remedies available to individuals are to be considered in this context and the working combination of the proposed changes noted and considered.**

[42] *GDPR* art 45(2).
[43] Ibid art 45(1).
[44] Ibid art 3(2)(a)-(b).
[45] Productivity Commission, *Data Availability and Use* (Inquiry Report No 82, 31 March 2017) 99.

Enforcement powers under the Privacy Act and role of the OAIC (Questions 53 to 55)

91. The Law Council notes the recommendations of the ACCC in its *Digital Platforms Inquiry* about bringing the penalties for breaches of privacy in line with the penalties available under the Australian Consumer Law. Such an approach could serve to elevate the status of privacy law and would act as a significant deterrent against severe and/or repeated offences against the Privacy Act. This proposal should be further explored by the Department in the context of the current review.

92. The Law Council is aware of concerns that budget constraints faced by the OAIC may at times impede its ability to bring enforcement proceedings. In this regard, it is critical that the OAIC be appropriately resourced to apply to the courts for civil penalties for serious or repeated interferences with privacy and to further its enforcement activities.

Recommendations:

- **Consideration should be given to bringing the penalties for breaches of privacy in line with the penalties available under the Australian Consumer Law (consistent with the views of the ACCC in its Digital Platforms Inquiry).**
- **Consideration should be given to increasing the resources of the OAIC to apply to the courts for civil penalties for serious or repeated interferences with privacy and to further its enforcement activities.**

Direct right of action (Question 56)

93. The Law Council does not currently have a settled position regarding the possible creation of a direct right of action or the creation of a tort (see below) for invasion of privacy. The Law Council intends to resolve this matter through further research and consultation with its stakeholders, with the aim of reaching a position that will inform the Department's review as it progresses in 2021.

94. Regardless of the position that is adopted this proposal requires further and detailed consultation. Once the policy decision is made, it will become a drafting issue that can be framed to support the rights as created. For example, Article 82 of the GDPR gives any person who has suffered 'material or non-material damage as a result of an infringement of this Regulation' the right to receive compensation and envisages court proceedings to exercise that right.

95. As a minimum, any amendment introducing such a right will need to:

- clearly articulate and remain complementary to enforcement taken by the OAIC;
- address the degree of harm required and in doing so be consistent with the definition of an 'eligible data breach' and the operation of the mandatory reporting under Part IIIC of the Privacy Act; and
- address what types of damages give rise to the cause of action. For example, will harm encompass loss of control of one's personal information, an issue

currently before the English and Welsh Court of Appeal in *Lloyd v Google LLC.*[46]

96. In addition, the formulation of the direct action needs to address relevant litigation rules and practices to address what scope, if any, exists for representative or class actions. Many data breaches involve multiple individuals who are the victims. Typically, these are low value claims for everyone affected (absent specific financial loss or distress, which would be the remit of an individual claim under the GDPR). There are policy and commercial reasons that may make collective action attractive as it is unlikely that victims will go to the effort of seeking compensation individually where the individual values are low for everyone.

97. This needs further research, consideration and consultation as noted above. The Law Council will continue to engage with its Constituent Bodies, Sections and Advisory Committees with the view to arriving at a settled position prior to the next stage of the review.

Statutory tort (Questions 57 to 62)

98. Like the above response to the issue of a direct right of action, the Law Council does not currently have a settled position regarding a stand-alone statutory tort of privacy.

99. Several of the Law Council's Constituent Bodies have pointed to sound policy reasons to support the introduction of a stand-alone statutory tort of privacy, particularly in a landscape in which technological developments continue to increase the risk of intrusion into an individual's privacy and broad dissemination of private information.

100. Further, it has been highlighted that while regulatory and criminal responses are vitally important, it is also appropriate that individuals who are the subject of serious incursions of privacy causing harm have an improved ability to pursue redress (including compensation).

101. Conversely, it has been noted that the myriad of transactions and occurrences which involve the potential for actual or alleged incursions on one's individual privacy are continuous. Further, the issue of personal rights to privacy, in the lay sense, is a matter which many individuals are likely to feel strongly about.

102. Considering the above, it may be queried as to whether the introduction of a statutory tort of privacy, may potentially attract considerable attention from a litigation perspective. This may particularly be the case in the context of laypersons aggrieved by objectively trivial or inconsequential incursions on their perceived rights to privacy. Many analogies may potentially be drawn with the tort of defamation and the nature of some of the smaller claims which it generates. This consideration gives rise to the need to ensure the complaints amounting to a potential breach of the Privacy Act are justified, fair and not trivial.

103. As the ALRC has recommended, the design of any legal privacy protection should be 'sufficiently flexible to adapt to rapidly changing technologies and capabilities, without needing constant amendments'.[47] This recommendation is particularly salient in light of the exponential pace at which new technologies such as AI and blockchain are developing, and the evolving scope of their application.

---

[46] [2019] EWCA Civ 1599.

[47] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Report No 123, June 2014) 36.

104. The Law Council will continue to engage with its Constituent Bodies, Sections and Advisory Committees with the view to arriving at a settled position prior to the next stage of the review, however it is clear that any proposed statutory development for such a cause of action must be subject to a rigorous consultation process including careful scrutiny of the detail of proposed legislation.

105. In drafting the legislation, it will be necessary to strike the appropriate balance between protection of privacy, freedom of expression and communication and national security, and the courts will need to be empowered to weigh up the public interest in privacy against any other countervailing public interests.

Notifiable Data Breaches scheme: impact and effectiveness (Questions 63 to 65)

The impact of the notifiable data breach scheme and its effectiveness in meeting its objectives

106. Australia has seen a welcome increase in the notification of data breaches since the introduction of the Notifiable Data Breaches (**NDB**) scheme. However, Australia's notification rate remains lower than many European nations who are subject to the notification regime under the GDPR.[48]

107. In line with Accenture's findings that two-thirds of Australian consumers are concerned with the management of financial data, the OAIC Notifiable Data Breaches Report found that 37 per cent of personal information involved in the breach included financial details, such as bank account or credit card numbers.[49] The 'My Health Record' initiative, which was met with widespread opposition with 2.5 million Australians choosing to opt out of making patient data available to health practitioners,[50] suggests a need to address the general public's concerns about data mismanagement. Of particular concern, is the OAIC's recent report on the types of data breaches notified under the scheme found that 64 per cent of total reported breaches were a result of 'malicious or criminal attacks',[51] aimed at exploiting consumer data for financial gain.

108. More generally, the Law Council understands that entities have responded to the commencement of the NDB Scheme by uplifting many of their operational processes. Typically, this will be interdisciplinary in that multiple functions are involved in dealing with matters that may be reportable. This includes, security, customer facing and various risk and governance functions. This has helped embed many privacy enhancing measures within many entities. These factors suggest that generally the scheme has worked effectively and many of the implementation issues are operational (as opposed to legal) in nature.

109. However, there remains an open question as to the impact of the notifications once made and whether these are effective. There is scope for work to be undertaken in this area to assess the impact on individuals. The consultation process would benefit from more empirical work on assessment of harm and impact on notifications on

[48] DLA Piper, *GDPR Data Breach Survey 2020* (20 January 2020) <https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/>.
[49] Office of the Australian Information Commissioner, *Notifiable Data Breaches Report: July-December 2019* (28 February 2020).
[50] Christopher Knaus, 'More than 2.5 million people have opted out of My Health Record' *The Guardian* (online, 20 February 2019) <https://www.theguardian.com/australia-news/2019/feb/20/more-than-25-million-people-have-opted-out-of-my-health-record>.
[51] Office of the Australian Information Commissioner, *Notifiable Data Breaches Report: July-December 2019* (28 February 2020) 8.

individuals. In doing so, it would be important to look at various cohorts, by reference to age, demographics and prior experiences with data breach and harm experienced (if any).

110. The consultation process also provides an opportunity to assess the notification process where multiple regulators may be involved. This relates to ability to comply and doing so efficiently, especially for global entities or entities in highly regulated industries.

Recommendation:

- **Consideration should be given to conducting research on the impact of notification to affected individuals and what makes for an effective notification in the context of the harm (if any).**

Interaction between the Privacy Act and other regulatory schemes (Questions 66 to 68)

The desirability and feasibility of independent certification scheme to monitor and demonstrate compliance with Australian privacy laws

111. While the Privacy Act has existing obligations for data transfers, there is a lack of specificity as to what the appropriate measure is, and there is an overreliance on the judgment/discretion of the information security team in each organisation.

112. It may therefore be desirable to have an independent certification body for data processed by certain companies. Similar to the GDPR certification, which is perceived to be voluntary, the certification process could be enforced through obligations under the certification agreement, independent of the need to comply with the GDPR (for example, Article 30 relating to record-keeping obligations).

Recommendation:

- **Consideration should be given to the establishment of an independent certification body for data processed by certain companies.**

Data privacy and artificial intelligence

113. The Terms of Reference for the current review of the Privacy Act are not geared directly toward the increasingly prominent issues regarding data privacy and artificial intelligence. Similarly, the Department of Industry, Science, Energy and Resources' consultation, *An AI Action Plan for All Australians: A Call for Views,* does not focus squarely on these issues.

114. The EU has already identified and legislated to mitigate a number of data privacy risks relating to AI, through the GDPR. The GDPR implements general limitations on the collection, use and transmission of data, which can impact AI, but also a number of rules more specifically directed towards AI, including:

- the requirement for processing to be fair.[52] Fair processing requires that data 'controllers' consider the likely impact of their use of AI on individuals and continuously reassess it. In particular, fair processing requires that AI systems do not produce bias;

- the principle of data minimisation.[53] The data minimisation principle requires that personal data be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed';

- the 'right of access by the data subject',[54] allowing the data subject access to 'meaningful information about the logic involved' in solely automated decision-making;

- a 'right to explanation' of automated decisions (though there are significant restrictions on the types of automated decisions that are covered — which must both be 'solely' based on automated processing and have legal or similarly significant effects);[55] and

- data protection impact assessments (**DPIAs**).[56] DPIAs are designed to assess the impact of a processing activity on the protection of personal data, where the processing is likely to result in a high risk to the rights and freedoms of natural persons.[57]

115. The Law Council encourages the Australian Government to consider undertaking a fundamental review of Australia's data protection and privacy legislation, which is specifically targeted at AI, and informed by the experiences of other jurisdictions.[58] A robust review in this space is necessary in order to support and promote responsible innovation and adoption of AI in Australia, which hinges on the safe and secure availability and sharing of data.

Recommendation:

- **Consideration should be given to undertaking a fundamental review of Australia's data protection and privacy legislation, which is specifically targeted at AI, is informed by the experiences of other jurisdictions and complements the current privacy legislation review processes.**

[52] *GDPR* art 5(1)(a).
[53] Ibid art 5(1)(c).
[54] Ibid art 15.
[55] Ibid art 22.
[56] Ibid art 35.
[57] See Centre for Information Policy Leadership, *Artificial Intelligence and Data Protection: How the GDPR Regulates AI* (March 2020) <https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_-1.pdf>.
[58] See also Office of the Australian Information Commissioner, Submission to the Department of Industry, Innovation and Science, *Artificial Intelligence: Australia's Ethics Framework* (24 June 2019) <https://www.oaic.gov.au/engage-with-us/submissions/artificial-intelligence-australias-ethics-framework-submission-to-the-department-of-industry-innovation-and-science-and-data-61/>; Office of the Australian Information Commissioner, Submission to the Australian Human Rights Commission, Artificial Intelligence: Governance and Leadership White Paper (19 June 2019) <https://www.oaic.gov.au/engage-with-us/submissions/artificial-intelligence-governance-and-leadership-white-paper-submission-to-the-australian-human-rights-commission/>.