THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: CCW:CBns200323

20 March 2023

Dr James Popple
Chief Executive Officer
Law Council of Australia
DX 5719 Canberra

By email: natalie.cooper@lawcouncil.asn.au

Dear Dr Popple,

Privacy Act Review Report

Thank you for the opportunity to contribute to the Law Council's submission to the Attorney-General's Department in relation to its Privacy Act Review Report ("Report"). The Law Society's Privacy and Data Law, Public Law, Business Law, Human Rights, Criminal Law, Employment Law and Indigenous Issues Committees have contributed to this submission. The Law Society welcomes the release of the Report, which represents a crucial step in the long-overdue process of reforming the *Privacy Act 1988* ("the Act").

General comments

Privacy as a human right

As a broad observation, we note that many of the Report's proposals are based on provisions of the General Data Protection Regulation ("GDPR"), which it seeks to adopt or incorporate into Australian privacy law. While there are significant benefits to this approach, including a potentially considerable extension of privacy protections for individuals in Australia, we note that the GDPR exists within a vastly different legal and regulatory system, and crucially, is underpinned by a corpus of human rights law which does not exist in Australia. As such, there is a degree of uncertainty in the extent to which GDPR jurisprudence is compatible with Australian common law principles, and how the equivalent provisions of the GDPR would apply if adopted into Australian law.

Accordingly, we suggest consideration be given to recognising privacy as a 'right' in Australian law, which entitles individuals to protection in relation to the processing of their personal information. Such a right may assist in bridging the gap between Australian and European jurisprudence, and assist with the interpretation of the proposed 'fair and reasonable' test (Proposal 12.1), by providing a substantive basis from which 'reasonableness' may be determined. Obviously there would be a range of additional considerations that may require further consideration and discussion.

THE LAW SOCIETY OF NEW SOUTH WALES
170 Phillip Street, Sydney NSW 2000, DX 362 Sydney
ACN 000 000 699 ABN 98 696 304 966
lawsociety.com.au
T +61 2 9926 0333 F +61 2 9231 5809
E lawsociety@lawsociety.com.au

We further note that the introduction of formal legislative recognition of rights at a national level would provide a legal framework to 'resolve complex interactions between fundamental rights and freedoms', for example, in balancing concerns around the protection of national security with the right to privacy.[1]

Australia's place in the global economy

We also note, as a broad observation, that Australia's regulatory approach to privacy and data law must be mindful of Australia's unique economic conditions, and place in the global economy. While the privacy and data law regimes adopted internationally, in jurisdictions such as the European Union, United Kingdom, and California may be instructive, the Act must, in our view, account for Australia's specific economic requirements, and support technological growth and innovation to the greatest extent possible.

We also consider that the Act should be flexible enough to adapt to ongoing developments in international privacy and data law and ensure that Australia's regime remains in line with global standards.

Independent source of guidance

We suggest that consideration should be given to constituting a board or advisory panel, independent of the Office of the Australian Information Commissioner ("OAIC"), that would be responsible for providing independent and objective guidance on matters pertaining to the application of the Act, and for promoting a common understanding of privacy and data laws. In our view, such a body should be modelled on the European Data Protection Board, and should have standing under the Act. Such a body could also be responsible for carrying out privacy impact assessments on proposed legislation, both primary and subordinate.

In our view, various aspects of the Report and the broader program of reform, justify the constitution of an independent advisory board, noting in particular that:

- Many of the proposals expressly refer to the need for further guidance (see Proposals 4.1, 4.2, 10.2, 10.3, 11.2, 13.1, 13.3, 16.2, 17.1, 17.2, 19.2, 21.3, 21.5 and 24).
- The proposed board could support the enhanced functions of the OAIC as a regulator with additional enforcement powers.
- It could potentially supplant the need to empower the Information Commissioner with the ability to develop an APP Code under Proposal 5.1, which various stakeholders noted may be somewhat controversial.
- It could potentially assist in harmonising the various state and federal privacy and data law regimes.
- It is, in our view, consistent with the revised objects of the Act proposed under Proposals 3.1 and 3.2.
- It could substantially improve certainty and consistency in the application of new and potentially far-reaching obligations under the Act, noting many proposals are expressed as principles requiring further guidance, such as the new requirements in relation to automated decision making (Proposal 19), and the new obligations under the fair and reasonable test (Proposal 12).

[1] Australian Human Rights Commission, 'Position Paper: A Human Rights Act for Australia' (March 2023) 15.

Indigenous data sovereignty

We note that a priority reform identified in the National Agreement on Closing the Gap recognises the principle of Indigenous data sovereignty,[2] that is, the right of Indigenous people to govern the collection, ownership and application of data as a cultural and economic asset.

It has been argued that:

> Aboriginal and Torres Strait Islander peoples, families and communities, heavily overrepresented in social disadvantage–related data will also be overrepresented in the application of these new technologies, but in a data landscape, Indigenous peoples remain largely alienated from the use of data and its utilization within the channels of policy power. Existing data infrastructure, and the emerging Open Data infrastructure, neither recognise Indigenous agency and worldviews nor consider Indigenous data needs.[3]

The Closing the Gap priority reforms are a whole of government concern, and in our view, this requires proceeding with this reform in a way that is consistent with enlivening Indigenous data sovereignty principles.

Question 1: Should there be a criminal offence for re-identifying de-identified information? What exceptions should apply?

We note that Proposal 4.7 contemplates a criminal offence that is strictly limited to malicious re-identification of de-identified information, with the intention to causing harm or obtaining an illegitimate benefit, subject to certain exceptions.

Where re-identification occurs as the result of poor information handling practices, in the absence of intent, we do not consider the imposition of a criminal offence appropriate, but suggest consideration should be given to providing further guidance to assist entities to avoid negligent or inadvertent re-identification.

While there may be some justification for instituting a criminal offence for very severe and malicious re-identification, we consider that such harm would be more appropriately dealt with under the proposed statutory tort for serious invasions of privacy in accordance with Proposal 27. We also suggest consideration should be given to including in the Act a civil prohibition on reverse engineering personal information provided in de-identified form, or which has been agreed to be de-identified.

Question 2: Should consent be required for the collection, use, disclosure and storage of other tracking data, such as health data, heart rate and sleeping schedule, in addition to precise geolocation tracking data?

We support, in principle, broadening the categories of data for which consent is required to be obtained in addition to geolocation tracking data, consistent with the Report's overarching theme of enhancing privacy protections for consumers by improving the quality of privacy notices and consents.

More broadly however, we note that although consent is a necessary aspect of privacy regulation, an overreliance on consent is unduly burdensome on consumers, and may not

---

[2] Walter, M, Lovett, R, Maher, B, Williamson, B, Prehn, J, Bodkin-Andrews, G, Lee, V. "Indigenous Data Sovereignty in the Era of Big Data and Open Data." *Aust J Soc Issues*. 2021; 56: 143– 156. doi: 10.1002/ajs4.141.
[3] Ibid.

result in improved privacy outcomes, given the complicated and technical nature of information handling practices. Accordingly, in addition to enhanced consent requirements, we suggest greater emphasis should be placed on organisational accountability in the collection and handling of sensitive information including geolocation and other data. In this context, we note the proposed 'fair and reasonable' test (Proposal 12.1) may provide more robust consumer protections than a purely consent-based model.

Question 3: If you are a small business operator, what support from government would be helpful for you to understand and comply with new privacy obligations?

The Law Society supports, in principle, the removal of the small business exemption from the Act, subject to the implementation of the measures in Proposal 6.1 to facilitate small business compliance.

The removal of the exemption is, in our view, reasonably necessary to promote consistency and uniformity in the application of privacy legislation, in accordance with the long-standing views of the OAIC.[4]

In considering the forms of government assistance that may be appropriate to assist with compliance, we support the development of information and training resources tailored to the needs of various small businesses, and suggest guidance may be obtained from recent initiatives implemented by the United Kingdom Information Commissioner's Office[5] and New Zealand Office of the Privacy Commissioner.[6]

In particular, we suggest consideration be given to developing the following forms of government support:

- Template privacy policies, notices and consent forms, to be made available at the time of registering an ABN and/ or business name. All existing ABN holders should also be notified of their new obligations under the Act and be provided with template documentation.
- Tailored advice and education provided by the OAIC (or the proposed independent advisory board referred to above under 'General comments').
- Free online training and information seminars with respect to privacy and data management, as well as cyber security training and assistance.
- A small business hotline and/ or live chat service.

We note, however, there is a risk that removing the small business exemption may have a cooling effect on innovation, particularly for start-ups and new businesses. Accordingly, we suggest consideration be given to empowering the Commissioner to make limited exemptions from the Act, either for specific periods of time, or from particular requirements of the Act if, in practice, compliance with specific obligations proves unduly burdensome for certain classes of small business.

Question 4: How should employers provide enhanced transparency to employees about the purposes for which their personal and sensitive information is collected, used and disclosed?

As noted in our previous correspondence, the Law Society supports either removing or

[4] Office of the Australian Information 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].
[5] United Kingdom Information Commissioner's Office, SME web hub – advice for all small organisations https://ico.org.uk/for-organisations/sme-web-hub/.
[6] New Zealand Office of the Privacy Commissioner, Privacy Statement Generator https://www.privacy.org.nz/tools/privacy-statement-generator/.

significantly narrowing the employee records exemption.[7] In our view, there is no clear distinction between the privacy risks faced by an individual whose personal information is being handled by an employer, as opposed to any given business with which they have interacted. We also note that employee records frequently contain highly sensitive information, such as health data, criminal records, and financial information.[8]

Accordingly, we suggest that if the exemption is to be retained, it should be constrained to legitimate employer activities relating to personal information (such as reasonable administrative action) and should be subject to the enhanced privacy protections set out in Proposal 7.1.

In considering how notice might adequately be given by employers in accordance with Proposal 7.1(a), we note some guidance may be gleaned from California's recently enacted *California Privacy Rights Act of 2020*, under which employers are required to provide a privacy notice to employees and/or job applicants before or at the time personal information is collected, specifying:

- The categories of sensitive personal information collected.
- Whether that information will be sold or shared.
- The length of time the employer intends to retain each category of personal information.
- The categories of all third parties that the employer discloses to or allows to collect consumer's personal information.[9]

We also suggest further consideration should be given to enhancing transparency in the use of workplace surveillance technology to collect personal and sensitive employee information. The rapid development in the sophistication of workplace surveillance technology poses significant regulatory challenges. In NSW, workplace surveillance technology was the subject of a recent Parliamentary Inquiry,[10] which recommended, *inter alia*:

- Enacting clear privacy protections for workers, including consultation and consent requirements and dispute resolution processes (Recommendation 2).
- Developing a best practice framework to guide the use of workplace surveillance measures (Recommendation 4).
- Amending workplace surveillance laws to require external approval prior to an employer undertaking or implementing workplace surveillance measures (Recommendation 5).
- Enhancing notification requirements such that employers must provide reasonable response timeframes and establish processes for employees to negotiate and oppose proposed surveillance activities (Recommendation 6).

In seeking to enhance transparency in the ways in which employee information is collected and used, it may be appropriate to draw upon, or incorporate, the recommendations of the NSW Parliamentary Committee Report.

---

[7] Letter from the Law Society of NSW to the Law Council dated 24 November 2020.
[8] European Commission, Submission to the Attorney-General's Department, *Privacy Act Review Discussion Paper*, 1 February 2022, 2.
[9] See Elizabeth Harding, 'CPRA and Employee Data – What businesses need to know' (2022) 12 *The National Law Review*. https://www.natlawreview.com/article/cpra-and-employee-data-what-businesses-need-to-know.
[10] Select Committee on the impact of technological and other change on the future of work and workers in New South Wales, Parliament of NSW, *Final report – Workplace surveillance and automation*, Report No 2 (2022).

Question 6: If privacy protections for employees were introduced into workplace relations laws, what role should the privacy regulator have in relation to privacy complaints, enforcement of privacy obligations and development of privacy codes in the employment context?

We consider the OAIC to be the appropriate agency to oversee and administer the privacy rights of employees with respect to the records held by employers. In our view, this approach would promote the greatest level of consistency and uniformity in the application of privacy principles and regulations. This could also be undertaken together with appropriate input from workplace relations and safety regulators.

Question 8: What additional requirements should apply to mitigate privacy risks relating to the development and use of facial recognition technology and other biometric information?

We suggest further consideration should be given to adopting an enhanced risk assessment process for the use of facial recognition technology ("FRT") in line with the model law proposed by the UTS Human Technology Institute.[11] The Law Society sees merit in a risk-based approach to regulating the use of FRT, in which the relevant legal requirements are calibrated to the assessed level of risk, under mandatory Facial Recognition Impact Assessments.

In relation to the capture and use of FRT and biometric data more broadly, it is, in our view, essential to adopt a technology neutral, risk-based approach to regulation. We note that unique risks may be involved where there are secondary uses of sensitive biometric data, collected with or without consent. For example, where biometric data has been inputted algorithmically into a secondary AI system, merely erasing an individual's data at the point of capture may be insufficient to remedy the relevant privacy risks.

Accordingly, we suggest that in developing strategies to mitigate privacy risks associated with biometric data collection, it is crucial to be mindful of the potential downstream privacy risks caused by the amalgamation of data, and interrelatedness of various technologies, particularly in the context of AI.

Questions 12-14: People experiencing vulnerability

We agree with Proposal 17.3. As a starting point, we direct the Law Council's attention to the Australian Banking Association ("ABA") *Banking Code of Practice*[12] ("Banking Code") in particular chapters 14, 17 and clause 54 within chapter 17. We also refer the Law Council to the ABA's Industry Guidelines, including *Preventing and responding to family and domestic violence*[13] and *Preventing and responding to financial abuse (including elder financial abuse)*[14] which assist with interpreting the Banking Code.

In our view, the legislation should provide an inclusive definition of vulnerability that should encompass matters including age-related impairment, cognitive impairment, disabilities, First Nation status, English fluency, literacy levels, socio-economic capacity, physical or mental illness and any other personal or financial circumstances that might indicate vulnerability. We suggest that these factors should act as red flags to put institutions on notice that a more considered and careful approach is required in relation to that particular customer, while taking care to preserve

[11] Human Technology Institute (UTS), *Facial recognition technology: Towards a model law*, Report (2022).
[12] Australian Banking Association, *Banking Code of Practice,* Revised 5 October 2021, 22, 25.
[13] Australian Banking Association, Industry Guideline *Preventing and responding to family and domestic violence,* Version 2.0, updated March 2021.
[14] Australian Banking Association, Industry Guideline *Preventing and responding to financial abuse (including elder financial abuse),* updated March 2021.

that individual's autonomy as much as possible. We note that individuals should not be assumed to lack requisite capacity merely because they exhibit factors that go to vulnerability.

Questions 15 – 16: Individual Rights

We support the proposed right to access information under Proposal 18.1, but question whether it may be inappropriate for organisations, particularly large organisations, to charge 'nominal fees' under 18.1(e). In our view, an entity's costs in complying with its privacy obligations under the Act should be construed as reasonable costs of doing business, noting that exceptions for frivolous or vexatious requests are included under Proposal 18.6(c). However, consideration should be given to allowing small businesses to charge nominal fees to comply with Proposal 18.1 given the costs associated with removing the small business exemption.

In relation to the right to object to the collection, use or disclosure of personal information under Proposal 18.2, we note that this right is somewhat limited in its utility and application. While an individual is entitled to a written response to their objection from the relevant entity, there is no requirement for the entity to take remedial action resulting from receipt of a valid objection. For organisations, the increased burden of compliance may incentivise them to simply provide generic, proforma responses, with little subsequent recourse for the individual. While the Report notes that this right would be 'modelled on the corresponding right in the GDPR', we note that the right to object in the GDPR is also underpinned by the lawfulness of processing requirements under Article 6.

In any event, we suggest consideration should be given to specifying a reasonable timeframe for the delivery of written responses by entities under Proposal 18.2.

We support the proposed right to erasure under Proposal 18.3, which is, in our view, fundamental in empowering individuals to exercise control over their personal information. We also support the proposed rights to correction and de-indexing in Proposals 18.5 and 18.6 respectively, noting that some caution may need to be exercised in considering 18.6(b). In our experience, entities may attempt to contract out of rights and responsibilities, and anti-avoidance measures may assist to guard against unintended consequences.

Question 17: What types of [substantially automated] decisions are likely to have a legal or similarly significant effect on an individual's rights?

We support a broad conception of 'legal or significant effects' in considering the widespread use of automated decision making ("ADM") by government and the private sector. Any decisions affecting the essential needs of individuals or access to basic goods, services and utilities (including the pricing of goods and services), as well as government services, should in our view be construed as 'significant'. We also note that ADM may be deployed at multiple levels of the supply chain, and that automated decisions by any relevant intermediaries could have significant effects on the rights of individuals.

We also support the view previously espoused by the Law Council, that the relevant decisions should be considered in a form that would allow it to be focused on the technology of the day and to be updated regularly.[15]

[15] Law Council of Australia, Submission to the Attorney General's Department, *Privacy Act Review Discussion Paper*, 27 January 2022, 16.

Question 18: Should there be exceptions to a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made?

We support in principle the right set out in Proposal 19.3, but note that there is likely to be significant ambiguity in what is meant by 'meaningful information' as it relates to complex algorithms.[16] It may simply not be possible to explain the inner workings of many automated systems at all, or at least not in a way that meaningfully helps individuals to understand how decisions have been made. This not only means that the right to information is somewhat hollow, but providing individuals with an explanation that does not in fact assist understanding may further diminish trust in the decision-making process. We refer the Law Council to some research on this topic, which suggests ways in which automated decision-making can be usefully explained, much of which is summarised in this report by Julian Fell, Ben Spraggon and Matt Liddy, "How to wrench open the black box of algorithms that decide our fate".[17]

Further consideration is also required in respect of how the proposed changes would intersect with doctrines of commercial in confidence and/or trade secrets. These doctrines often protect information about the design and processes of automated systems, including when those systems are built by private industry under government contract. Presumably, removing the exemption, and thus giving individuals a right to this information, would abrogate those doctrines. It may be that this is an appropriate balance to strike from a rights perspective, but commercial entities may argue that such a policy setting may hinder the development of automated systems. We note that the ABC report referenced above also briefly discusses this concern.

In addition, we suggest consideration should be given to implementing an express right to prevent individuals from being subject to decisions based solely on automated processing, in line with Article 22 of the GDPR.

In considering the future role of ADM, particularly in the delivery of government services and assistance, we suggest that due consideration should be given to the findings of the Robodebt Royal Commission, which we note are currently impending.

Questions 19 – 25: Direct marketing, targeting and trading

We support, in principle, the Report's proposals in relation to direct marketing and trading of personal information as defined by Proposal 20.1, namely:

- Providing individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes (Proposal 20.2).
- Introducing a requirement that an individual's consent must be obtained to trade their personal information (Proposal 20.4)
- Prohibiting direct marketing to a child unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests (Proposal 20.5).
- Prohibiting trading in the personal information of children (Proposal 20.7).

[16] Further, for the proposed right to be meaningful, it will be critical to anticipate, for resourcing purposes, that the exercise of this right may result in a large number of complaints to OAIC, as Proposal 18.9 notes:

> Proposal 18.9 An APP entity must take reasonable steps to respond to an exercise of a right of an individual. Refusal of a request should be accompanied by an explanation for the refusal and information on how an individual may lodge a complaint regarding the refusal with the OAIC.

[17] 12 December 2022, ABC News. Available online: https://www.abc.net.au/news/2022-12-12/robodebt-algorithms-black-box-explainer/101215902.

However, we note that the broad definition of 'targeting' in Proposal 20.1(c) represents a significant expansion of the existing law, and potentially captures a range of legitimate business activities beyond targeted advertising or marketing, including profiling.

Profiling is defined in Article 4 of the GDPR as:

> …any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

The recent decision of the Federal Court in *Australian Energy Regulator v Origin Energy Electricity Ltd*[18] highlights the value and necessity of accurately profiling a relevant customer base, particularly in dealings involving vulnerable groups. In that case, Origin Energy's automated processes for dealing with customers experiencing hardship and payment difficulties resulted in it breaching its own hardship policies and the retail rules by:

- unilaterally establishing new customer payment plans if the customer's previous payment plan had been cancelled for non-payment, while failing to consider a customers' capacity to pay,
- increasing a customer's payment amounts following a review of the customer's usage, while failing to consider the customers' capacity to pay, and
- cancelling customer payment plans where it was unable to discuss with the customer a review of their payment plan, including in circumstances where customers were continuing to make their payments under the existing plans.[19]

Accordingly, we suggest further consideration should be given to limiting the definition of 'targeting' in Proposal 20.1(c) to activities involving targeted advertising and marketing only.

We suggest an added obligation if clients are identified as vulnerable, or potentially vulnerable – that entities be required to suspend direct marketing, targeting and trading of data in relation to those individuals, until:

- they have effectively communicated with those individuals their right to opt out, and
- provided clear information on the mechanics of doing so, noting that the process of opting out must be easy and accessible.

We suggest, at a minimum, the regulation of direct marketing, targeting and trading should protect against the exploitation of vulnerable individuals. Our members advise that they are aware of same day pay lenders exploiting very vulnerable individuals, including Stolen Generations survivors, some of whom experience extreme financial hardship, mental and physical illness, trauma (including intergenerational trauma) and literacy issues. We understand that a number of these clients received reparations or payments from the National Redress Scheme, and then received unsolicited text messages from same day pay lenders. They subsequently became indebted to those lenders without the capacity to repay the loans, without receiving effective communication (and in some cases, any information at all) about the terms of the loan. We understand that one community legal centre in NSW assisted 134 clients in similar circumstances with respect to debts to same day pay lenders in the last financial year.

[18] [2022] FCA 80.
[19] Australian Energy Regulator, Australian Government, Origin penalised $17 million for customer hardship breaches. https://www.aer.gov.au/news-release/origin-penalised-17-million-for-customer-hardship-breaches.

Question 27: Should the extraterritorial scope of the Act be amended to introduce an additional requirement to demonstrate an 'Australian link' that is focused on personal information being connected with Australia?

We support the proposal to introduce an additional requirement in subsection 5B(3) of the Act to demonstrate an 'Australian link', which would effectively clarify that foreign organisations will only be regulated to the extent that their handling of personal information has a connection to Australia.

We hope this input is of assistance. Please contact Nathan Saad, Policy Lawyer, on (02) 9926 0174 or nathan.saad@lawsociety.com.au in the first instance if you have any queries.

Yours sincerely,

Cassandra Banks
President