Ai GROUP SUBMISSION

Legal and Constitutional Affairs
Legislation Committee

Privacy and Other Legislation Amendment Bill 2024 Inquiry

11 October 2024

A. Introduction

1. The Australian Industry Group (**Ai Group**) appreciates the opportunity to make a submission to the Senate Legal and Constitutional Affairs Legislation Committee's inquiry and report into the Privacy and Other Legislation Amendment Bill 2024 (**Privacy Bill**).

2. Ai Group is a peak national employer organisation representing traditional, innovative and emerging industry sectors. We have been acting on behalf of businesses across Australia for 150 years. Ai Group and partner organisations represent the interests of more than 60,000 businesses employing more than 1 million staff. Our membership includes businesses of all sizes, from large international companies operating in Australia and iconic Australian brands to family-run SMEs. Our members operate across a wide cross-section of the Australian economy and are linked to the broader economy through national and international supply chains. We make this submission to the Inquiry on behalf of our members.

3. We refer the Committee to our past submissions in relation to:

   (a) the Review of the *Privacy Act 1988* (Cth) conducted by the Australian Government's Attorney-General's Department – Submission – 27 November 2020 – see **Appendix A**.

   (b) the Discussion Paper for the Review of the *Privacy Act 1988* (Cth) released by the Attorney General's Department (**Discussion Paper**) – Submission – January 2022 – see **Appendix B**; and

   (c) the Privacy Act Review Report issued by the Australian Government's Attorney-General's Department (**Review Report**) – Submission – March 2023 – see **Appendix C**,

   (**Privacy Submissions**).

4. We reiterate the Privacy Submissions as they relate to the Privacy Bill that is the subject of this inquiry and with regard to any further legislation the Government may introduce as part of its ongoing review of the *Privacy Act 1988* (Cth) (**Privacy Act**).

5. We set out our further submissions below as relevant to the Privacy Bill. We have confined these further submissions to the impact of key measures of the proposed Privacy Bill as it relates to the domain of workplace relations and the difficulties that will be faced by our members if the Privacy Bill proceeds in the current form.

B. Managing the workplace relationship

6. Many of the changes as proposed in the Privacy Bill unreasonably constrain employers and persons conducting a business or undertaking (**employers**) from the legitimate collection, use, disclosure and storage of workers' information.

7. Employers legitimately collect, use, disclose and store workers' information:

   (a) to effectively manage their relationship with workers, including to monitor and manage workers' conduct and performance;

   (b) to comply with obligations under a variety of workplace laws, including but not limited to:

   - the *Fair Work 2009* (Cth) and other state or territory-based industrial legislation;
   - workers compensation laws;
   - work health safety laws;
   - anti-discrimination and gender equality laws;
   - workplace surveillance laws;
   - labour hire licencing laws;
   - net zero economy laws;
   - modern slavery; and
   - other industry or occupation-specific laws

   (c) in accordance with a contract between the parties;

   (d) to prevent damage or injury to an employer's property or to persons in the workplace and the general community;

   (e) to manage risks of vicarious liability for the actions of their workers, including when their workers use technology – for example: risks of unlawful sexual harassment[1]; and

[1] ANROWS, Workplace technology – facilitated sexual harassment: Perpetration, responses and prevention, 03/2024

(f) to prevent criminal offences, including but not limited to theft and fraud.

8. Consistent with this legitimate use, section 7B(3) of the Privacy Act currently provides for an 'employee records' exemption. This exemption operates so that an act or practice engaged in, by an organisation that is or was an employer of an individual is exempt from contraventions of the Privacy Act (including non-compliance with the Australian Privacy Principles (**APP**)) if that 'act or practice' is directly related to:

(a) a current or former employment relationship between the employer and the individual; and

(b) an employee record held by the organisation and relating to the individual.

9. The employee records exemption does not apply to:

(a) the collection of information that will ultimately form part of an 'employee record' – i.e., the exemption applies after it is collected; or

(b) acts or practices in relation to a job applicant or to relationships with workers who are not employees, such as independent contractors.

10. We deal with our key concerns below.

C. Increases to penalty provisions

11. The proposed expansion of regulatory powers and penalties will significantly and adversely impact employers.

12. Currently, subsection 13G(1) of the Privacy Act is a civil penalty provision which provides as follows:

13G Serious and repeated interferences with privacy

(1) An entity contravenes this subsection if:

(a) the entity does an act, or engages in a practice, that is a serious interference with the privacy of an individual; or

(b) the entity repeatedly does an act, or engages in a practice, that is an interference with the privacy of one or more individuals.

13. The Privacy Bill proposes to significantly expand the regulatory enforcement powers and penalties in the Privacy Act in relation to interferences with privacy as set out

below:

(a) Section 13G(1) will be repealed and substituted with subsection 13G(1):

13G Civil penalty provision for serious interference with privacy of an individual

(1) An entity contravenes this subsection if:

(a) the entity does an act, or engages in a practice, that is an interference with the privacy of an individual; and

(b) the interference is serious."

(b) Section 13G(1B) will be inserted and lists non-exhaustive factors which a court may consider in determining whether an act or practice contravenes s.13G(1) as set out below:

- "*the particular kind or kinds of information involved in the interference with privacy;*
- *the sensitivity of the personal information of the individual;*
- *the consequences, or potential consequences, of the interference with privacy for the individual;*
- *the number of individuals affected by the interference with privacy;*
- *whether the individual affected by the interference with privacy is a child or person experiencing vulnerability;*
- *whether the act was done, or the practice engaged in, repeatedly or continuously;*
- *whether the contravening entity failed to take steps to implement practices, procedures and systems to comply with their obligations in relation to privacy in a way that contributed to the interference with privacy;*
- *any other relevant matter*[2].

(c) The Privacy Bill inserts a new civil penalty provision for interference with the

[2] Paragraph 51 of the Privacy and Other Legislation Amendment Bill 2024

privacy of individuals as follows:

"13H Civil penalty provision for interference with privacy of individuals

Civil penalty provision

(1) An entity contravenes this subsection if the entity does an act, or engages in a practice, that is an interference with the privacy of an individual."

(d) In effect, section 13H replaces section 13G(1)(b) but no longer requires the contravention to be 'repeated'. The maximum penalties are 2,000 penalty units (or five times the amount specified for an individual for bodies corporate – which currently amounts to $3,130,000). A court can alternatively determine that a particular act or practice is not a "serious interference with the privacy of an individual" under s.13G(1) and to instead determine the contravention to be of the 'lesser' offence under section 13H.

(e) The Privacy Bill proposes an addition regulatory and enforcement measure for contravening particular acts or practices of certain APPs under the new section 13K. A maximum penalty of 200 penalty units applies (or five times the amount specified for an individual for bodies corporate – which currently amounts to $313,000). However, depending on the circumstances, the non-compliance may also contravene sections 13G(1) or 13H(1), each of which have significantly higher penalties. The OAIC will have the capacity to issue infringement notices in relation to these contraventions.

(f) It is also proposed that the Federal Court or Federal Circuit and Family Court of Australia (Division 2), be empowered to make additional orders on its own initiative during proceedings if, in the proceedings, the Court has determined or will determine that an entity has contravened a civil penalty provision of the Privacy Act, including ss 13G(1), 13H(1) and 13K. This includes an order to pay damages by way of compensation for any loss or damage suffered, or likely to be suffered, by any individual as a result of the contravention.[3] Such orders may be made even if the Court does not make a civil penalty order against the entity for the contravention.

14. Consistent with our Privacy Submissions, we continue to oppose this unwarranted expansion of regulatory enforcement powers and penalties. We reiterate the importance of focusing on business uplift with respect to privacy. The focus should

[3] Paragraph 80UI (1), (2) and (5): Privacy and Other Legislation Amendment Bill 2024.

be on proactive initiatives to help mitigate such breaches occurring, including improved OAIC education material and programs and a specific industry engagement plan with key stakeholders that can identify specific resourcing needs.

15. If, however, these provisions are retained, the commencement dates must be deferred and not commence the day after Royal Assent as is currently proposed. If delayed, businesses must be given a reasonable time frame and be provided with sufficient transition support to ensure they have the capacity to meet these new compliance requirements.

D. Proposed statutory tort for serious invasions of privacy

16. Ai Group has opposed and continues to oppose the introduction of a statutory tort for serious invasions of privacy.

17. The proposed new cause of action would be available to an individual (**plaintiff**) against another person (**defendant**) if:

    (a) the defendant invaded the plaintiff's privacy by doing one or both of the following:

        - **intruding upon the plaintiff's seclusion**;
        - **misusing information** that relates to the plaintiff; and

    (b) a person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances; and

    (c) the invasion of privacy was intentional or reckless; and

    (d) the invasion of privacy was serious.

18. Relevantly:

    (a) "*intruding upon the seclusion*" includes, but is not limited, to:

        - physically intruding into the person's private space;
        - watching, listening to or recording the person's private activities or private affairs.

    (b) "*misusing information*" that relates to an individual includes, but is not limited to, collecting, using or disclosing information about the individual.

19. The meanings of expressions or provisions under the Privacy Act are not relevant for this cause of action. Instead, the meanings will be developed over time through court decisions.

20. We set out below our key concerns as to the application of this cause of action as follows:

    (a) Employers legitimately use worker information, including as set out in paragraph 7 above. Although an individual themselves may consider the retention or use of their personal information in the workplace as being an infringement of a right to privacy it should not always be considered. The prospect of compensation being ordered by way of damages is inappropriate considering the public interest in employers exercising a reasonable use of workers' information to effectively manage their workforce.

    (b) The introduction of a statutory tort for a serious invasion of privacy amounts to a significant change to the enforcement regime pertaining to privacy breaches that is not justified by any apparent shortcomings in the existing avenues available for enforcing individual rights to protection from an invasion of privacy or in the context of the flagged tranche 2 of amendments to the Privacy Act.

    (c) Opening an avenue for prosecution on the basis of recklessness as envisaged is oppressive and will likely result in our members being compelled to take an excessively risk-averse stance with respect to the treatment of workers' information.

    (d) The nature of a tort, by focusing on redress by way of an award of damages, is unsuitable in relation to breaches of privacy in a workplace context. Also, the emphasis on damages and compensation in tort law may encourage speculative litigation by individuals claiming mental distress. Vicarious liability for the wrongs of an employee presents a significant risk for employers in the context of tort law. The various risk mitigation strategies and the litigation insurance costs which would be necessitated by the establishment of a privacy tort would not be in the public interest.

    (e) An actionable tort per se as is proposed (i.e. where there is no need for the claimant to establish any form of damage) exposes employers to an even greater risk which is not counterbalanced by any public benefit from introducing a tort of privacy.

(f) We consider that the forum with the appropriate expertise lies with the OAIC. The OAIC should be solely responsible for assessing breaches relating to privacy and acting on an affected individual's behalf. If there are concerns that the OAIC has insufficient resources to undertake its responsibilities or expeditiously resolve matters, a more appropriate response would be to increase the OAIC's resources. Creating another avenue and action for redress through the courts may generate other problems, including shifting the administrative burden from the OAIC to the courts, duplicating the OAIC's function, and potentially opening up the floodgates to a litigious culture. Such an outcome would be an administratively inefficient use of public resources and would most likely harm many businesses.

(g) The introduction of the statutory tort is unnecessary given that an employer's reasonable monitoring or use of employees' information in connection with work, including in areas of 'seclusion' is already comprehensively regulated by state and territory surveillance legislation.[4] Monitoring and surveillance has long been acknowledged by legal decision-makers as being a legitimate practice, particularly in the context of managing conduct and performance, as a pro-active step to prevent unlawful workplace behaviours in the virtual workplace environment and to ensure the health and safety of workers and the community.

21. If, despite our opposition, the statutory tort is to be retained in the Privacy Bill, we respectfully ask the Committee to consider the following changes to ensure that changes so that the new cause of action is not overly burdensome for our members:

(a) The definition of '*organisation*' which currently excludes small businesses where in a financial year its annual turnover for the previous financial year is $3,000,000 or less should similarly apply to the statutory tort. Exposing small and medium enterprises to the risks of a claim and significant compensation award (together with legal costs) is unjustified, overly burdensome and could threaten ongoing business viability.

(b) The employee records exemption or similar provision should apply to the statutory tort for a serious invasion of privacy for consistency, clarity and

[4] Listening Devices Act 1992 (ACT); Surveillance Devices Act 2007 (NSW); Surveillance Devices Regulation 2022 (NSW); Surveillance Devices Act 2007 (NT); Surveillance Devices Regulations 2008 (NT); Invasion of Privacy Act 1971 (Qld); Surveillance Devices Act 2016 (SA); Surveillance Devices Regulations 2017 (SA); Listening Devices Act 1991 (Tas); Listening Devices Regulations 2014 (Tas); Surveillance Devices Act 1999 (Vic); Surveillance Devices Regulations 2016 (Vic); Surveillance Devices Act 1998 (WA); Surveillance Devices Regulations 1999 (WA); Workplace Privacy Act 2011 (ACT); Workplace Surveillance Act 2005 (NSW)

for the reasons as set out above in paragraph 7.

(c) The meaning of "*information*" for the purposes of this cause of action should be aligned with the meaning of "*personal information*" under the Privacy Act. To have different meanings will create significant uncertainty, unnecessary complexity and may give rise to problematic inconsistencies in legal interpretation between the common law and the Privacy Act which creates legal risks for employers which cannot be easily managed.

(d) An employer should have a specific defence to the statutory tort for serious invasions of privacy in each of the following circumstances:

- where the employer collects, uses, discloses and stores a worker's information in circumstances where such use is not required or authorised by law but is reasonably necessary for reasons as set out in paragraph 7;
- where the employer lawfully and reasonably conducts monitoring and surveillance of an employee when they are working or using an employer's property at home or in another remote location for reasons as set out in paragraph 7 – irrespective of whether the employee considers those locations as being areas of **seclusion**;
- where the employer is required to and has complied with the requirements in the APPs in the Privacy Act in relation to information to which the statutory tort has application.

(e) The Privacy Bill should explicitly identify the public interest in employers exercising the reasonable use of workers' information to effectively manage their workforce, including for the reasons in paragraph 7.

(f) The cause of action should require an applicant to prove harm. Compensation should not be awarded in the absence of proven harm.

(g) It should be specified that matters referred to in paragraph 7 must be considered by a court a relevant factor when determining remedies.

E. Automated decision-making

22. Australian Privacy Principal 1 (**APP 1**) requires that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP policy.

23. The APPs do not apply to:

(a) "*Small business operators*,"[5] except in certain circumstances (a business is a "small business" in a financial year its annual turnover for the previous financial year is $3,000,000 or less); and/or

(b) "*Employee records*".[6]

24. Part 15 of the Privacy Bill introduces new requirements to APP 1, requiring organisations to include specific information in APP privacy policies about the kinds of personal information used in, and the types of decisions made by, automated decision-making (**ADM**) that "*could reasonably be expected to significantly affect the rights or interests of an individual*".[7] The Explanatory Memorandum states that such circumstances include where ADM "*limits access to employment opportunities*"[8].

25. Specifically, Part 15 imposes new information requirements if:

(a) the entity has arranged for a computer program to make, or do a thing that is substantially and directly related to making a decision; and

(b) the decision could reasonably be expected to **significantly affect the rights or interests of an individual**; and

(c) **personal information** about the individual is used in the **operation** of the computer program to make the decision or do the thing that is **substantially and directly related to making the decision**.[9]"

26. The information which must be included in an APP privacy policy is:

(a) "**the kinds** of **personal information** used in the operation of such computer programs; and

(b) the kinds of such decisions made solely by the operation of such computer programs; and

(c) the kinds of such decisions for which a thing, that is **substantially and directly related to making the decision**, is done by the **operation** of such

[5] Section 6C, Privacy Act 1988
[6] Section 7B(3), Privacy Act 1988. We note that Part 15 has application to circumstances when the employee records exemption does not apply, including at the point of collection, in respect of job applicants and the workplace relationships which are not employment arrangements.
[7] Paragraph 1.7(b), Privacy and Other Legislation Amendment Bill 2024.
[8] Para 343.c. Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024.
[9] Paragraph 1.7 of the Privacy and Other Legislation Amendment Bill 2024

computer programs"[10].

27. We outlined our concerns regarding the implementation of legislation in relation to automated decision making in our Privacy Submission, including in Appendix B, and reiterate those concerns here in respect of what has been proposed.

28. We remind the Committee that ADM and other artificial intelligence tools are generally commercial or proprietary programs and often necessarily operate in an opaque way. The information they use may not be known to our members and is often held by the creator, developer or facilitator of such a program. This makes it extremely difficult for our members to be open and transparent as required by Part 15 – particularly in situations where the transparency relates to the:

    (a) "**operation**" of the program; and

    (b) "**kinds of personal information**" that the program uses or infers.

29. Additionally, we ask the Committee to provide further clarification on:

    (a) The meaning of "*significantly affect the rights or interests of an individual,*" particularly in the context of workplace relations, including recruitment through to termination of employment.

    We note also that in the Government Response to the Privacy Act Review Report, its support was to a narrower concept: "substantially automated decisions **with a legal or similarly significant effect** on an individual's rights" and which should be supplemented by OAIC guidance. We do not agree with the broadening of this concept as proposed[11].

    In considering this, we respectfully ask the Committee to also have regard to the Government's stated intentions to deliver tranche 2 amendments.

    (b) The meaning of "*substantially and directly related to making the decision*" particularly in the context of workplace relations' decision, including in relation to recruitment through to termination of employment.

    In considering this, we again respectfully ask the Committee to have regard to the Government's stated intentions to deliver tranche 2 amendments.

    (c) The scope of "*personal information*" relevant to ADM.

[10] Paragraph 1.8 of the Privacy and Other Legislation Amendment Bill 2024.
[11] Australian Government – Government Response – Privacy Act Review Report, 2023 – page 11.

This requirement should only apply to "personal information" that the employer directly provides to the "computer program".

It should not apply to information which may be created by ADM in its processing of such information, including any digitally created profiles or inferred personal information.

30. Overall, we agree that privacy is a relevant consideration in a discussion about ADM, AI and other emerging technologies. However, there are a range of dimensions and activities related to AI, not limited to privacy and human rights. We appreciate that a diversity of perspectives need to be properly captured and are concerned about the potential for fragmented and conflicting regulation or legislation that could arise in absence of proper coordination between multiple bodies on this subject. There would be a benefit if privacy and other matters associated with AI were considered as part of coordinated discussion between the various Federal departments, agencies, authorities and stakeholders around policy issues that arise from new and emerging technologies such as AI. This will help to ensure that government's potential role in promoting AI investment and uptake is not inadvertently stifled by other government activities that may inhibit it. This valuable coordinating role would also ensure consistent policy, efficient use of stakeholder resources, and helping to connect industry capability.

31. These are matters that we have previously raised in various submissions including to the AHRC and Department of Industry, Science, Energy and Resource[12]. Subsequent to this, we note that the Government released its AI Action Plan, and Critical Technologies Blueprint and Action Plan. Most recently, we have raised these concerns in the context of our submission to the Government's proposals paper for introducing mandatory guardrails for use of AI in high-risk settings[13] (i.e., including in employment) which foreshadows requirements for human oversight of, and intervention in, AI system deployment, as well as requirements to inform end-users about how AI is being used. These and other government activities are also more broadly relevant to our point in this submission regarding the need for better coordination across Federal departments, agencies and authorities around interrelated reforms.

[12] Ai Group submission to DISER (1 December 2020), https://www.aigroup.com.au/globalassets/news/submissions/2020/diser_ai_action_plan_dec2020.pdf ; Ai Group submission to AHRC (26 March 2020), https://www.aigroup.com.au/globalassets/news/submissions/2020/ahrc_human_rights_and_technology_discussion_paper_26mar_2020.pdf .

[13] Introducing mandatory guardrails for AI in high-risk settings: proposals paper - Consult hub (industry.gov.au)

F. Conclusion

32. We respectfully ask the Committee to consider our submissions and recommend the Privacy Bill be amended to address our concerns as outlined above.

ABOUT THE AUSTRALIAN INDUSTRY GROUP

The Australian Industry Group (Ai Group®) is a peak national employer organisation representing traditional, innovative and emerging industry sectors. We have been acting on behalf of businesses across Australia for 150 years. Ai Group and partner organisations represent the interests of more than 60,000 businesses employing more than 1 million staff. Our membership includes businesses of all sizes, from large international companies operating in Australia and iconic Australian brands to family-run SMEs. Our members operate across a wide cross-section of the Australian economy and are linked to the broader economy through national and international supply chains.

Our vision is for thriving industries and a prosperous community. We offer our membership strong advocacy and an effective voice at all levels of government underpinned by our respected position of policy leadership and political non-partisanship.

With more than 250 staff and networks of relationships that extend beyond borders (domestic and international) we have the resources and the expertise to meet the changing needs of our membership. Our deep experience of industrial relations and workplace law positions Ai Group as Australia's leading industrial advocate.

We listen and support our members in facing their challenges by remaining at the cutting edge of policy debate and legislative change. We provide solution-driven advice to address business opportunities and risks.

OFFICE ADDRESSES

NEW SOUTH WALES

Sydney
51 Walker Street
North Sydney NSW 2060

Western Sydney
Level 2, 100 George Street
Parramatta NSW 2150

Albury Wodonga
560 David Street
Albury NSW 2640

Hunter
Suite 1, "Nautilos"
265 Wharf Road
Newcastle NSW 2300

VICTORIA

Melbourne
Level 2 / 441 St Kilda Road
Melbourne VIC 3004

Bendigo
87 Wil Street
Bendigo VIC 3550

QUEENSLAND

Brisbane
202 Boundary Street Spring Hill
QLD 4000

ACT

Canberra
Ground Floor,
42 Macquarie Street
Barton ACT 2600

SOUTH AUSTRALIA

Adelaide
Level 1 / 45 Greenhill Road
Wayville SA 5034

WESTERN AUSTRALIA

South Perth
Suite 6, Level 3 South Shore Centre 85
South Perth Esplanade
South Perth WA 6151

www.aigroup.com.au

Appendix A

Ai GROUP SUBMISSION

Australian Government
Attorney-General's Department

Review of the *Privacy Act 1988*

November 2020

CONTENTS

1. EXECUTIVE SUMMARY

The Australian Industry Group (**Ai Group**) welcomes the opportunity to respond to the review into whether the scope of the *Privacy Act 1988* (Cth) (**Privacy Act**) and its enforcement mechanisms remain fit for purpose (**Review**).

In September 2019, Ai Group made a submission to the Australian Government's consultation on the Final Report of the Digital Platforms Inquiry by the Australian Competition and Consumer Commission (**ACCC**).

Many of the issues raised therein are being further examined in the context of the present Review. Overall, industry recognises the importance of protecting customer information and data, and supports a data and privacy regime which can benefit both customers and businesses through outcomes such as improved transparency and customer experience.

It is essential that reforms which arise as a result of the present Review do not result in excessive or overlapping regulation and that any additional obligations placed upon business recognise the importance of ensuring industry is not excessively burdened as the economy seeks to lift itself from the damaging impacts of the COVID-19 pandemic.

It is important that the important exemptions that have long excluded employee records from application under the Privacy Act are retained.

Also, the current actions available for privacy breaches are sufficient and there is no significant evidence that would justify implementing a direct right of action which would encourage litigation and overlap with the functions of the Office of the Australian Information Commissioner (**OAIC**).

2. OBJECTIVES OF THE PRIVACY ACT

The Issues Paper refers to recommendations from the ACCC's Digital Platforms Inquiry (**DPI**) Final Report, including its recommendation to consider: whether the objectives of the Act remain appropriate to require the protection of privacy to be balanced with the interests of business in carrying out their functions or activities; and whether there should be a greater emphasis placed on privacy protections for consumers to empower them to make informed choices.

During the DPI, despite the ACCC's references to consumer surveys to support some of its arguments on behalf of the consumer, we raised questions as to whether the issues and recommendations properly reflected consumer views and expectations that are material in nature. As the ACCC's Final Report acknowledged, there is the concept of the "privacy paradox":[1]

> *In essence, the privacy paradox refers to a perceived discrepancy between the strong privacy concerns voiced by consumers who, paradoxically, do not appear to make choices that prioritise privacy.*

[1] ACCC, Final Report, Digital Platforms Inquiry, June 2019, p. 384.

> *One possible explanation for the privacy paradox is that consumers claim to care about their privacy in theory but, in practice, the value they derive from using a digital platform's services outweighs the 'price' they pay in allowing the collection of their user data. A further explanation is that, while consumer attitudes are often expressed generically in surveys, actual behaviours are specific and contextual, and therefore, consumers' generic views regarding privacy do not necessarily predict their context-specific online behaviours.*

Even so, the ACCC did not appear to give much weight to this concept on the basis that the privacy paradox rests on the premise of consumers making informed decisions in their transactions with digital platforms; the ACCC was of the view that consumers may be prevented from making informed choices.

Notwithstanding the ACCC's views, we consider that the potential for a privacy paradox highlights a need to conduct more rigorous consumer interviews and dialogue to accurately identify the drivers of consumer perceptions. Without accurate identification of drivers, there is risk that the Final Report's recommendations (in this case, proposed changes to the objectives of the Act) will not address potential underlying issues.

For instance, the Government's interest in this area of reform relates to providing transparency and consumer value. However, the proposed reforms that are based on these aspirations may instead lead to impractical outcomes for consumers such as information and communication overload. There are also practical questions about: whether the consumer would actually go searching for information as a result of increased information and communication; and whether consumers will ultimately be disadvantaged by not getting access to, for example discounts or specials, as a result of new requirements such as opt-in consent discussed below.

On its face, the ACCC's Final Report was substantive in content. However, upon review, we considered more work was required. In absence of this, there appeared to be theoretical assumptions and hypotheses made in the Final Report, requiring further analysis and assessment including in relation to underlying causes for purported issues and options to address these. A compelling case was not sufficiently made to identify what actual consumer harm or detriment had occurred by the collection and use of data to justify these recommendations. A robust and considered cost-benefit assessment for any recommendations will also be required. In absence of these considerations, it is unclear whether the recommendations will provide material benefit to consumers and businesses in the long term, which may result in potentially unintended consequences.

For instance, one Ai Group member commented that the DPI Final Report read more like an Issues Paper, which would usually initiate a multi-staged consultation process. The ACCC provided commentary that there previously has not been significant reflection on the implications and consequences of the business models of digital platforms. A further comment was that reflections on perceived issues cannot provide a basis for recommendations, but rather act to initiate investigation and quantitative and qualitative analysis, which would provide an evidence base for any recommendations. They cannot provide the basis for recommendations on their own. Future

analysis and assessment could include: detailed consumer interviews (with questions more specific than those provided in the Final Report); analysis of interviews to determine causes (including consumer and business behaviour); and assessment of functionality of current privacy frameworks against these consumer and business behaviours.

These are initiatives where the Attorney-General's Department can substantively improve upon the outcomes in the ACCC's Final Report.

3. DEFINITION OF PERSONAL INFORMATION

Technical information and reference to GDPR

We note that the Issues Paper discusses the contemporary definition of personal information which may be achieved by aligning it with the definition of personal information in the GDPR. In our submission to Recommendation 16(a) of the DPI Final Report, we made a number of comments which are relevant to this consultation.

A concern of Ai Group members was that changing the definition of personal information will shift the emphasis from consumer protection (i.e. protecting identification of individuals) to data protection (i.e. protecting identification of devices e.g. capturing technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual). The latter form of protection is based on the GDPR definition of personal information. It is unclear how defining such information as personal information will materially benefit consumers.

In addition, we note that the current definition of "personal information" already includes things like IP addresses in situations where they can reasonably identify someone (or are associated with other information that is about someone or which could reasonably identify someone). As the OAIC points out in their own guidance, whether a person is reasonably identifiable "is an objective test" which depends on the "context in which the issue arises".[2] The Final Report's recommendation to amend the Privacy Act and define things like IP addresses and other metadata as "personal information" in all cases (even in circumstances where the metadata can't reasonably identify someone) is not necessary as: if the information could reasonably identify someone, it is already covered by the definition; and if it cannot reasonably identify someone, then it does not require the same level of protection as other personal information.

Further, while the Final Report's recommendation purports to be in alignment with the GDPR, the proposed expansion of the definition for personal information under the Privacy Act will actually be broader in scope than the GDPR. For businesses already subject to the GDPR (as well as those which are not), this will likely create a new regulatory burden. Smaller businesses will also likely face a greater burden than larger businesses.

Further work will be required to properly assess whether the current definition of personal

[2] OAIC, Australian Privacy Principles Guidelines, Chapter B: Key Concepts, July 2019, p. 20.

information is appropriate. A proper assessment of options will also be required, including cost-benefit assessment.

Multiple approaches to personal information

As we raised during the DPI, questions remain on how changing the definition of personal information will fit with other multiple forms of regulation in this area, including the Consumer Data Right (**CDR**) and industry specific regulations. Making changes to the definition of personal information will likely create additional complexity and uncertainty.

We have also raised this issue during Treasury's inquiry into the future direction for the CDR.[3] Using the banking sector as an example, with the introduction of the CDR, there now exists the Australian Privacy Principles (**APPs**) regime under the Privacy Act and the CDR Privacy Safeguards regime under the *Competition and Consumer Act 2010* (Cth). This effectively creates a dual privacy regime, with regulatory oversight of the CDR Privacy Safeguards by the ACCC and OAIC. Such an outcome creates complexity and compliance costs for businesses that have to comply with both regimes, and also for small businesses that may not currently be subject to the Privacy Act and therefore not familiar with privacy regulatory regimes.[4]

To help clarify these new requirements, the OAIC has consulted with stakeholders about its CDR Privacy Safeguard Guidelines. The Government allocated $90 million in its 2018-19 Budget and 2018-19 MYEFO over five years for the OAIC and other relevant agencies to ensure that they can properly administer the new regime.[5] This has been followed more recently in the 2020-21 Budget announcements to invest $28.6 million in 2020-21 to continue the implementation of the CDR and commence work on its rollout in the energy sector. Additional funding has also been allocated to the ACCC to progress the CDR and Treasury to support information and awareness.

However, more can be done to support industry. Proper cost-benefit assessments need to be undertaken including compliance cost impacts on industry. With respect to multiple privacy and data regimes, there may be no additional benefit of protecting the privacy and security of consumers through the CDR, while creating an additional compliance burden on businesses. Government should consider ways to alleviate such regulatory burdens.

Alternative approaches do not appear to have been properly considered before the Final Report's recommendation was made. For example, instead of immediately resorting to changing the legal definition for personal information, a solution could be for the OAIC to provide additional guidance around the existing definition on a case by case basis. Such an approach would be a more proportionate response to address issues of legal uncertainty, without creating an unnecessary regulatory burden for businesses.

---

[3] Ai Group submission to Treasury (June 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/Treasury_CDR_Inquiry_5Jun_2020.pdf.
[4] OAIC, "OAIC commences consultation on draft CDR Privacy Safeguard Guidelines" (Media release, 17 October 2019).
[5] Treasury, "Consumer Data Right Overview" (Booklet, September 2019), p. 6.

4. FLEXIBILITY OF THE APPS IN REGULATING AND PROTECTING PRIVACY

Australian context

The Issues Paper raises the question about whether the framework of the Privacy Act is effectively providing sufficient clarity about protections and obligations.

For the purposes of this submission, we wish to provide a general comment about the role of regulation in the current Australian context. In short, we would be concerned if there were to be broader reform of the privacy regime that shifted from the current flexible principles-based regulatory approach.

A general criticism about regulation is that it is too slow and inflexible to adapt and respond to technological change. Thoughtful strategy and credible policy responses from governments and regulators are important to plan for and respond to economic and technological change in ways that will meet community expectations.

Well before COVID-19, Australian businesses have been in transition to and within the Fourth Industrial Revolution. Now, amidst a pandemic-driven recession, businesses are facing challenges greater than any in living memory, highlighting broader economic vulnerabilities, raising questions about the scope of our domestic capabilities and resilience of global supply chains. This unstable environment presents an opportunity for industry to emerge more globally competitive by taking fuller advantage of Industry 4.0 and digitalisation. This transition includes entry into new technology sector markets, which requires positive measures from Government. However, more can be done to make us globally competitive. Regulation can boost or break the growth of an early stage industry sector or for an incumbent business that is seeking to make a transition. The extent to which new technologies are regulated can act as an investment barrier and diminish our attractiveness relative to other jurisdictions.

Highly reactive or overly change-averse responses risk curtailing innovation, reducing competitiveness and limiting the benefits of developments like digitalisation. A policy and regulatory vacuum is likely to provoke subsequent hasty overreaction to any problems that emerge. Regulation has a role in addressing reasonable public concerns including around privacy. But there are also often alternative approaches to the regulatory "stick", including consultation and dialogue, codes of practice, transitional support and education. Where regulatory measures are warranted, they still require careful development.

As a general rule, governments should proactively:

- consult about major technological and economic changes;
- consider the full range of options for response;
- adopt regulatory responses only where they are proportionate and likely to provide net community benefits; and

- develop any regulatory response in full consultation with affected stakeholders.

Governments should also reinvigorate best practice regulation initiatives, and study global best practices in regulation and business support that encourage – rather than inhibit – innovation and productivity.

Returning to the question in the Issues Paper, it is important to consider whether the current privacy regime is appropriate in light of the above context. We consider that a principles-based approach to privacy regulation, as currently reflected in the Privacy Act, is flexible enough to enable future proofing and therefore technology neutrality in a rapidly changing environment. This strikes the appropriate balance between protecting the privacy of individuals and regulating businesses.

As the former Privacy Commissioner, Karen Curtis, stated:[6]

> *By encouraging organisations to recognise the business advantages of good personal information handling practices and regulating their behaviour accordingly, government regulators can minimise regulatory intervention and red tape. This has been a common theme of our regulatory approach where a legislative framework is balanced by an emphasis on business privacy awareness and self-regulation. The idea is to inculcate the values and objectives of privacy law in business rather than just the superficial rules. When this happens organisations will be better equipped to deal with technological change because they will understand the ideas behind the laws – the principles – and will not become as confused by detailed technology-specific regulations.*

In reference to the former Commissioner's remarks, the ALRC concluded:[7]

> *In this way, principles-based regulation aims to minimise the need for enforcement by 'encouraging organisations to understand the values behind the law and change their behaviour accordingly; not because they might get caught out by a regulator, but because they understand why the law is there and what its objectives are'.*

In contrast, an alternative to principles-based regulation (i.e. prescriptive regulation) runs the risk of stifling innovation and making Australia less competitive compared to its more advanced peers. Regulation should be drafted to allow it to be nimble and flexible rather than overly prescriptive and heavy handed in the first instance. This will be especially important, given the significant wide scope of this DPI and its potential impact on a wide range of stakeholders.

[6] ALRC, "For Your Information: Australian Privacy Law and Practice" (Report 108, August 2008), p. 237.
[7] Ibid.

EU GDPR

In the Final Report for the DPI, the ACCC made several recommendations to adopt privacy reforms similar to the EU GDPR. Here, the ACCC suggested it was not looking at wholesale adoption of the GDPR, but would look to more closely align with the GDPR. We would like to highlight issues that may arise in considering the GDPR which the AGD should be cognizant of when considering privacy regulatory reforms:

- Some businesses may be subject to and compliant with the GDPR; if the privacy regime is changed to align with the GDPR, there may be an assumption that the regulatory burden would be minimal for businesses. But not all businesses, including smaller businesses, are subject to the GDPR and will likely see a greater regulatory burden and create a competitive disadvantage.

- For businesses compliant with the GDPR, there is a false economy if an ACCC recommendation varies from the GDPR. This issue is discussed further in the context of consent requirements.

- The GDPR operates in a very different legal framework than Australia's Privacy Act and relies on different administrative and enforcement structures. For these reasons, it cannot simply be implemented into Australia.

- Given the GDPR is relatively new, the Centre for Information Policy Leadership identified unresolved issues and challenges with the GDPR one year after it commenced operation, "where organisations feel the Regulation has not lived up to its objectives and has presented practical difficulties, despite their dedication to implementing the new requirements".[8] The International Association of Privacy Professionals also found more work is still required for companies to comply with the GDPR.[9]

- The potential impact of any GDPR type reforms to Australian businesses must also be carefully assessed. We should learn from the successes and failures of the GDPR and consider the real impact GDPR has had on individuals and businesses in Europe and elsewhere. We should not simply align to GDPR where the scope and potential impact of GDPR is unclear or untested, or where requirements are overly cumbersome with limited positive impact on privacy protection.

[8] Centre for Information Policy Leadership, "GDPR One Year In: Practitioners Take Stock of the Benefits and Challenges" (May 2019).
[9] International Association of Privacy Professionals, "GDPR compliance: Hits and misses" (May 2019).

5. EMPLOYEE RECORDS EXEMPTION

The Privacy Act currently provides an exemption under ss. 7(1)(ee) and 7B(3) for acts done or practices engaged in by an organisation that is or was an employer of an individual if the act or practice is directly related to:

- a current or former employment relationship between the employer and the individual; and
- an employee record held by the organisation and relating to the individual.

Employee records are defined under s. 6 of the Act as records of personal information relating to the employment of the employee. Although the definition of 'employee records' under the Act is not exhaustive, it includes health information about the employee and personal information about all or any of the following:

- the engagement, training, disciplining or resignation of the employee;
- the termination of the employment of the employee;
- the terms and conditions of employment of the employee;
- the employee's personal and emergency contact details;
- the employee's performance or conduct;
- the employee's hours of employment;
- the employee's salary or wages;
- the employee's membership of a professional or trade association;
- the employee's trade union membership;
- the employee's recreation, long service, sick, personal, maternity, paternity or other leave;
- the employee's taxation, banking or superannuation affairs.

The policy considerations which justified the employee records exemption are set out in the explanatory memorandum to the *Privacy Amendment (Private Sector) Bill 2000* which stated:

> *The Government has agreed that the handling of employee records is a matter better dealt with under workplace relations legislation.*
>
> *…*
>
> *Acts and practices in relation to "employee records" are exempted as it is recognised that the handling of employee records is a matter better dealt with under workplace relations legislation.*

These considerations which resulted in the establishment of the employee records exemption remain apposite today and it is neither necessary nor appropriate to expose employers to the administrative and financial burden of applying additional controls to the handling of employee records. The Issues Paper suggests that the rationale for introducing the exemption reflected the largely state-based responsibility for workplace relations laws at the time. Although much of the regulation of employment is now provided for by Federal statute, the situation remains that the employment relationship, including obligations regarding record keeping requirements continue to be codified in dedicated workplace legislation.

Employer obligations pertaining to employee records and pay slips are provided for under Division 3 of Part 3-6 of the *Fair Work Regulations 2009* (**Regulations**). The Regulations mandate the form and conduct of records relating to a specified list of matters including pay, overtime, averaging of hours and leave. These regulations also govern the employer's obligations concerning provision of such records to a 'new employer' in the context of a transfer of business in a manner which would arguably be contrary to APP 3 that generally, an APP entity must collect personal information about an individual only from the individual. The Regulations already provide employees with protected access to employee records, as defined, for the purpose of inspection or copying the relevant information.

Employers are also required to correct a record that the employer is required to keep under the Act as soon as the employer becomes aware of the error. Significant fines are available under the *Fair Work Act 2009* (Cth) (**FW Act**) for failing to correct the accuracy of a record.

Unlike under the Privacy Act, independent rights of action are available under the FW Act to employees over failure to abide by the record keeping requirements. The FW Act prohibits an employer from making or keeping an employee record that the employer knows is false or misleading.[10] However, this prohibition does not apply if the record is not false or misleading in a material particular.[11] No qualifier regarding the materiality of the false record applies under the Privacy Act.

In certain proceedings related to a contravention of a civil remedy provision under the FW Act, if an applicant makes an allegation relating to a matter about which an employer was required to keep an employee record and the employer failed to do so, the burden of disproving the allegation falls upon the employer. Separate provisions under Division 2 of Part 3-4 of the FW Act govern the right to access employee records by an employee organization. Although these rights and obligations arise under federal legislation, abolishing or watering down the employee records exemption calls into question the interaction between these separate and comprehensive provisions arising under workplace legislation and the Privacy Act. The provisions governing employee records in the FW Act and the associated Regulations were not drafted to operate in tandem with or intersect with the APPs. Apart from the obvious administrative and financial burden of applying the Principles, employers would be left in a state of legal uncertainty as to how the laws are to interact. This would

[10] *Fair Work Act 2009* (Cth) s. 535(4).
[11] *Fair Work Act 2009* (Cth) s. 535(5).

not be conductive to efficient and productive workplace relations.

Although Commonwealth legislation now governs much of the field of industrial relations, there remain an appreciable number of specific laws governing employee records which the APPs would cut across were the employee records exemption to be abolished or reduced. Additionally, State and Territory legislation restricting surveillance by employers of their employees at work restricts the use and disclosure of surveillance records.[12] The policy positions surrounding the treatment of such records cannot be divorced from the separate regulatory schemes governing the undertaking of workplace surveillance. Ai Group understands that the Queensland Government has asked the Queensland Law Reform Commission to review Queensland laws in respect of workplace surveillance. The Queensland Law Reform Commission is to report to the Queensland Government by 30 April 2021. Any reforms which may disturb these State or Territory laws should not be made in the context of the present review of the Privacy Act.

Numerous APPs would significantly restrict an employer's capacity to operate and engage in reasonable management action. For example, APP 3.2 would restrict an employer from collecting personal information unless it is reasonably necessary for one or more of the entity's functions or activities. It would be near impossible for employers to obtain much information concerning their staff with certainty that such was "reasonably necessary" for one or more of its functions or activities. APP 3.3 provides more significant restrictions regarding sensitive information, the collection of which, without the employee's consent, is prohibited unless one of a series of specified exceptions apply. This would be very difficult to apply consistently with an employer's need to investigate instances of bullying or misconduct. An open question may remain as to whether such collection would be otherwise authorized by or under an Australian law pursuant to APP 3.4. The prohibition under APP 3.6 from collecting information about an individual via any other source than the individual him or herself would cause significant issues with an employer's capacity to carry out staff development functions and identify training needs, identify deficiencies in an employee's performance or respond to employee claims under unfair dismissal, general protections, underpayment of wages, anti-discrimination, workers' compensation and other laws.

Significant restrictions on the use of unsolicited personal information under APP 4 would prevent an employer from appropriately dealing with inappropriate or unlawful behaviour by an employee or responding to deficiencies in an employee's performance. Were an APP entity to receive unsolicited personal information and the entity determine that it could not have collected the information under APP 3 if the entity had solicited the information, it must, where lawful and reasonable to do so, destroy the information or ensure that it is de-identified. Application of this principle would present employers with significant difficulties in dealing with information provided in the context of performance management where customer complaints are received or where another employee makes a bullying allegation. Requirements to notify an employee of the collection of personal information of this nature could limit employers' capacity to respond in the context of

[12] *Workplace Surveillance Act 2005* (NSW); *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 1998* (WA); *Workplace Privacy Act 2011* (ACT).

an ongoing dispute following termination of employment.

With the exception of the employee records dealt with under Division 3 of Part 3-6 of the Fair Work Regulations, there are a significant number of materials likely held by employers concerning issues of performance management which are of a personal and sensitive nature which should not be subject to access on request. Such records may, in some circumstances, have been collected in the course of investigations into employee misconduct. It would be inappropriate to limit the circumstances under which an employer is able to keep such records confidential. Currently APP 12.1 requires an APP entity to give an individual access to personal information held by the entity on request. The limited exceptions in APP 12.3 are insufficient to ensure employers are able to withhold access in appropriate circumstances.

The Issues Paper refers to the recent decision by a Full Bench of the Fair Work Commission in *Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946 in which the Commission held that the employee records exemption only applies once the record is created. As such the employer's direction to an employee to submit to finger print scanning contravened APP 3. This case demonstrates the folly of removing the employee records exemption and presents a strong argument for extending it to personal information requested in the context of an employment relationship. The COVID-19 pandemic has highlighted the need for employers to be capable of putting in place practices and procedures which enable employer oversight of employee attendance at each workplace and to obtain health related data. Some employers engaged in a practice of taking employees' temperatures before allowing their staff access to the workplace. Employers should not be prevented by the application of the Privacy Act to requesting personal information which is necessary to engage in reasonable management action.

A common practice which would place former employers at risk of contravening the APP relates to provision of employee references. If a past employer were to respond to a request from a prospective employer concerning an employee's performance or conduct during a period of employment, this would arguably contravene prohibitions on disclosure of personal information under APP 6 if the employee records exemption were removed. Even where an employee has consented to a prospective employer contacting a former employer, ambiguity may arise as to what information the employee had consented to the disclosure of.

The employee records exemption does not go far enough in protecting new employers from breaches of the Privacy Act in the context of a transfer of business. Provisions in the FW Act govern recognition of previous transferring employees' accumulated service for the purposes of leave and redundancy pay.[13] Application of the APP to employee records dealing with issues of service would conflict with these existing provisions in the FW Act which assume such records may be passed to a third party. In some cases, a prospective new employer would need to have a thorough knowledge of an existing company's employee obligations in order to assess whether an acquisition makes business sense. Such companies should not be prevented from accessing relevant information by the application of the APP. The limited application of the employee records exemption should not

[13] *Fair Work Act 2009* (Cth) ss. 69, 91 and 122.

restrict the ability of prospective employers to adopt sound recruitment and selection processes when engaging new staff, including enabling information to be obtained about job candidates from former employers.

The employee records exemption should be expanded to encompass host companies in the context of a labour hire arrangement. In many cases, a labour hire employer will deploy workers to a site operated and managed by another entity. In such circumstances, the limitation of the employee records exemption to acts done, or practices engaged in, by an organisation that is or was an employer of an individual limits the capacity for the host company to freely engage with an existing employer by providing and requesting relevant information regarding employee performance and conduct. Health and safety information must be freely exchanged between a host and an employer to ensure safety in the workplace is maintained. Restricting the application of the employee records exemption to employers and excluding entities supervising an employee in the context of a labour hire arrangement presents a significant risk that such arrangements would breach the APP.

The personal information of employees are adequately protected by the current scope of the employee records exemption. Employer practices in legitimately obtaining relevant information concerning the employment relationship must not be inappropriately prescribed by the APP. The employee records exemption should be expanded to encompass prospective new employers and the recipients of labour hire services.

6. NOTICE OF COLLECTION OF PERSONAL INFORMATION

The Issues Paper raises several questions relating to themes on improving awareness of relevant matters, third party collections and limiting information burden. It also refers to Recommendation 16(b) of the DPI Final Report. If Government decides to progress with this recommendation, we wish to reiterate our previous concerns that were raised during the DPI.

Recommendation 16(b) proposed that the collection of personal information should be accompanied by a notice from the APP entity collecting the personal information (whether directly from the consumer or indirectly as a third party) unless the consumer already has this information or there is an overriding legal or public interest reason. The ACCC suggested that this will address information asymmetries for consumers and better inform them. They also acknowledged that this can create the risk of information overload on consumers and suggested ways that this could be minimised.

As we stated in our submission to the DPI Final Report, if such notification requirements were to be introduced, there is a risk that these could lead to a cumulative increase in notifications (albeit shorter in length) from APP entities (including third parties) to consumers. Therefore, it is not clear how this recommendation will reduce information overload for consumers and be of material benefit to them.

As the DPI Final Report acknowledges with respect to the effect of information overload:[14]

> *Information overload may result in suboptimal outcomes such as:*
>
> - *consumers putting off making a purchase that would have made them better off*
> - *consumers remaining with their existing supplier when switching suppliers would have made them better off*
> - *low consumer awareness and understanding of product risks, for example the risk of data breaches or targeted advertising*
> - *consumers feeling anxious and stressed from information overload.*

Elaborating further on the above, while the Privacy Act currently allows notification to be provided after collection (where it is not practicable to do so before), the ACCC's recommendation, if adopted, would require notification to be given at the time of collection. While this might be achievable where the data controller is collecting information from sites it owns and operates, this is more difficult and less practical where data is collected from third party sites, particularly where multiple APP entities are collecting information via one site.

Where multiple APP entitles are collecting information from one site, imposing notification obligations at the time of collection could result in consumers receiving multiple simultaneous notifications. This would not only impose a complex regulatory burden on business, but would increase the risk of "information overload" leading to consumer confusion and ultimately disengagement, an outcome that appears disproportionate to any demonstrated consumer benefit. To address this concern, we suggest that instead of requiring each APP entity collecting information to notify customers at the time of collection, the Government could require the third party site operator to provide the relevant notice of the collection by the APP entity, via either their privacy notice or some other means.

If there is limited benefit to consumers in introducing this new notification requirement, it would be inappropriate to create a new regulatory burden on businesses. Nevertheless, the ACCC "considers that the regulatory burden from the strengthening of notification requirements is unlikely to outweigh the benefits, particularly as the size of the burden imposed by stricter notification requirements will be commensurate with the extent to which the APP entity collects, uses and discloses the personal information of Australian consumers".[15]

We consider that this reasoning is inadequate and requires more rigorous analysis and assessment (including a cost-benefit assessment). For instance, further work will be required to properly assess whether there is material consumer benefit from these proposed notification requirements. A proper assessment of options will also be required, including a cost-benefit assessment. Otherwise,

[14] ACCC, Final Report, Digital Platforms Inquiry, June 2019, p. 404.
[15] ACCC, Final Report, Digital Platforms Inquiry, June 2019, p. 462.

this recommendation will likely place an even greater regulatory burden on smaller businesses, not just larger businesses.

In the absence of substantiated evidence to the contrary, we consider that the current regime is operating adequately, striking the right balance between protecting the consumer without overloading them with information that may have limited value in practice, and not creating an unnecessary regulatory burden on businesses.

7. CONSENT TO COLLECTION AND USE AND DISCLOSURE OF PERSONAL INFORMATION

The Issues Paper raises several questions associated with consent to collect, use and disclose personal information. It also refers to Recommendation 16(c) of the DPI Final Report. If the Government decides to progress with this Recommendation, we wish to reiterate our previous concerns raised during the DPI.

Recommendation 16(c) proposed to require consent to be obtained whenever a consumer's personal information is collected, used or disclosed by an APP entity, unless the personal information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason. The recommendation goes to both the circumstances in which consent is required for data processing under Australian law, and the requirements for obtaining a valid consent. The ACCC suggested that this will improve consumer choice over their information, as well as suggesting this will closely follow current non-binding APP guidelines and the GDPR.

Similar to our concern with Recommendation 16(b) of the DPI Final Report, creating a new consent requirement for APP entities will likely create information overload for consumers – in this case, consent fatigue – as well as practical implementation issues for businesses to seek consent. Consumers will also be likely to miss out on benefits as a consequence of opt-in consent. In this respect, consumer expectations need to be properly considered, including the benefit that they may receive from having opt-out consent. For example, consumers do benefit from targeted advertising through improved customer experience and service.

While the ACCC suggested that the Recommendation aligned with the GDPR, it recommended that Australia not adopt the GDPR principle that processing of data is also lawful if undertaken for the legitimate interest of the data controller. This is because it considered that the GDPR was too wide and flexible with respect to consent requirements. The recommendation therefore sought to import a regime similar to that included in the GDPR without the inclusion of a critical component of that regime. As a result, the Recommendation is not aligned with the GDPR. On this basis, there will likely be a regulatory burden for any business if this new requirement were to be introduced, with a greater burden felt by smaller businesses.

Exploring this further, the GDPR legitimate interest exception gives data controllers the ability to process data without obtaining the consent of the data subject where the data processor's

legitimate interest in processing the data does not override the fundamental freedoms of the data subject. For example, the organisation may have a legitimate interest in processing personal data to enforce a legal claim, prevent fraud, or manage information security.

In this way, the GDPR attempts to strike a balance between the legitimate interests of the data processor (or a third party) and the fundamental privacy rights of individuals. This approach encourages data processors to think more about the impact of processing on individuals and the safeguards required to minimise undue impact on the data subject. Having a balanced legitimate interest exception also reduces the need to burden consumers with intrusive and repeated consent requests, particularly where the impact on the individual is limited or negligible. For example, balancing the privacy interests of users who want and expect to receive interest-based ads that help connect them to relevant products or services, and who have not opted out for such services, can be achieved through privacy safeguards to ensure the end result of processing does not produce legal or similarly significant effects on the data subjects. Such safeguards may include pseudonymising and segregating data and minimising retention periods where possible.

The ACCC's recommendation removed the balance struck by the GDPR where the privacy impact to individuals is minimal. The only reason given by the ACCC for rejecting the "legitimate interests" exception was its view that "there is considerable uncertainty and concern surrounding the relatively broad and flexible definition of the 'legitimate interests' basis for processing personal information under the GDPR". This is not a valid reason to remove an element critical to the workings of the GDPR regime. While the ACCC acknowledged the real possibility of consent fatigue, no clear mechanism was proposed to deal with it. Without this, there is a risk of creating a more cumbersome, confusing and intrusive experience for consumers while bringing no meaningful improvement to their understanding of data practices.

Before radically departing from the GDPR's legitimate interest test, the Government should carefully weigh the consumer benefits of this approach against the risk of consent fatigue and the impacts on the data management and privacy collection practices of Australian business across the economy.

Even in the event of there being sufficient evidence to support proceeding with Recommendation 16(c), entities should not be expected to obtain consent for data already obtained prior to this new requirement and should be exempted from the effect of this recommendation. That is, the recommendation should not have a retrospective effect.

We understand that collections required to perform a contract are excluded from Recommendation 16(c). However, if such collections were not excluded and the definition of personal information were also broadened to include online identifiers, Recommendation 16(c) could be expected to seriously impact online data collection practices as online identifiers will be required to perform a contract in order to engage in data processing.

If Government decides to progress with the Recommendation 16(c), further work will be required to properly assess whether there is material consumer benefit from these proposed consent

requirements. A proper assessment of options will also be required, including a cost-benefit assessment.

8. CONTROL AND SECURITY OF PERSONAL INFORMATION

The Issues Paper raises the concept on the "right to be forgotten", and includes references to Recommendation 16(d) of the DPI Final Report and the international example of the concept's implementation under the GDPR.

Recommendation 16(d) proposed to amend the Privacy Act to give an individual the ability to request APP entities to erase that individual's personal information, without delay. The ACCC suggested that this will help mitigate the bargaining power imbalance for consumers and give them greater control over their personal information.

In our submission to the DPI Final Report, several Ai Group members identified a number of issues with this ACCC recommendation.

The recommendation is akin to the GDPR's "right to be forgotten". While this concept has been implemented in the EU, the relatively new GDPR is not without its challenges, as highlighted earlier. There are important lessons for Australia if a similar requirement were to be contemplated.

One Ai Group member, while not opposed to the concept, is currently subject to the GDPR and shared their own practical problem in complying with this GDPR requirement. For their business, they are placed in a position where they have to determine whether it is in the public interest to remove content about an individual if requested. In this example, inclusion of judicial oversight to make this determination would help this company resolve this matter, which is not currently available under the GDPR.

Another member is not legally obliged to erase personal information. However, in practice they may receive fewer than five requests of this nature from their Australian customers every year. Where they legally can, the member will endeavour to accept the customer's request, although it takes significant time for the company to process it. The limited number of requests that this company receives raises questions regarding the actual materiality of the need for consumers to seek erasure of their personal information, which will likely create a regulatory burden on businesses should they be required to comply with such a legal requirement.

If IP addresses and other metadata are defined in the Act as "personal information", and consumers were to be given the right to request deletion of their personal information (and for entities to be required to delete it unless an exception applies), there is a potential that individuals could misuse this right. The ACCC had proposed exceptions to this requirement to delete personal information relate only to information that is:

- required for the performance of a contract to which the consumer is a party;
- required under law; or

- otherwise necessary for an overriding public interest reason.

These exceptions should be expanded (or the public interest exemption clarified) to cover situations where the information is required to be retained in order to safeguard customer privacy or security or to prevent fraudulent activity. For example, a customer who asks one of our members to delete their metadata (after they have ceased to be a customer) – including device information and IP address – may do so in order to engage in fraudulent activity without our member knowing who they are. More work needs to be undertaken on considering the consequences of allowing individuals to request that this data (if defined as personal information) be deleted from an entity's records.

There are also potential privacy risks that might arise with the proposed right to erasure. Therefore, such a proposed right needs to be clarified and carefully considered with a focus on ensuring privacy protection. For example, requiring APP entities to erase personal data that has been rendered pseudonymous may require an APP entity to reattribute full personal data such as name and email address to pseudonymous data to enable erasure. This could undermine the privacy protection offered by pseudonymisation in general, and increase the privacy risk to both the individual requiring erasure and other data subjects whose data is pseudonymised under the reattribution key. Careful consideration should be given to the ways privacy risk can be minimised without unintentionally jeopardising the individual's and other individuals' personal information. It should also be acknowledged that in some cases, there will be legitimate business requirements for APP entities to retain data, and in these circumstances, the focus should be on the use of effective privacy safeguards to minimise any risk.

In addition, the CDR may also include a requirement to erase personal information. As discussed above, consideration needs to be given as to how new requirements under the CDR interact with a proposed right to erasure, including whether this proposed right is necessary.

9. DIRECT RIGHT OF ACTION

The current avenues for enforcing the provisions of the Privacy Act are fit for purpose and do not currently require amendment. If a direct right of action is ultimately pursued by the Government, this should not result in extending a class action scheme to enable representative proceedings to be brought for breaches of the Privacy Act.

Direct right of action for individuals and a statutory tort for serious invasions of privacy are closely related. We note that these proposals were recommended in the DPI Final Report (Recommendations 16(e) and 19), which we also previously commented on.

The ACCC suggested that recommendation 16(e) will empower consumers and give them greater control over their personal information by giving them another avenue for redress, and will incentivise APP entities to comply with the Privacy Act. For recommendation 19, the ACCC suggested that the new cause of action relating to a statutory tort for serious invasions of privacy will lessen the bargaining power imbalance for consumers, address existing gaps in the privacy framework and

increase the deterrence effect on businesses. While it is important for consumers to have access to an avenue to seek redress for breaches of the Privacy Act, caution needs to be taken when considering creating any new forum or cause of action.

We consider that the forum with the appropriate expertise lies with the OAIC to assess breaches relating to privacy and act on an affected individual's behalf. If there are concerns that the OAIC has insufficient resources to undertake its responsibilities or expeditiously resolve matters, a more appropriate response would be to increase the OAIC's resources.

Creating another avenue and action for redress through the courts may create other problems, including shifting the administrative burden from the OAIC to the courts, duplicating the OAIC's function, and potentially opening up the floodgates to a litigious culture. Such an outcome would be an administratively inefficient use of public resources and would most likely harm many businesses.

There may be a false economy created for the consumer in seeking legal action through the courts. There will be legal costs for consumers and businesses in using this avenue which need to be accounted for.

Part V of the Privacy Act provides a comprehensive regime in dealing with complaints and investigations about acts or practices that may be an interference with the privacy of an individual. Division 1 of this Part establishes an avenue for complaints brought to the Information Commissioner by an individual about an act or practice that may be an interference with the privacy of the individual and for an investigation to be undertaken by the Commissioner in response. The Commissioner can also initiate an investigation into an act or practice which may be an interference with the privacy of an individual or a breach of APP 1. The Commissioner may decide to conciliate a matter, conduct a hearing or conference. The Commissioner has power to obtain information and documents or examine witnesses. At the finalisation of an investigation, the Commissioner may either dismiss a complaint or make a determination that includes a declaration that the conduct constituted an interference with the privacy of an individual and/or:

- a declaration that the respondent must take specified steps within a specified period to ensure that such conduct is not repeated or continued;
- a declaration that the respondent must perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant;
- a declaration that the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint;
- a declaration that it would be inappropriate for any further action to be taken in the matter.

Division 3 of Part V outlines the process for proceedings to be brought in the Federal Court or the Federal Circuit Court to enforce a determination. The Information Commissioner is an authorised applicant in relation to civil remedy provisions under the Privacy Act. A framework is in place for

accepting and enforcing undertakings or using injunctions in relation to compliance with the Privacy Act in Divisions 2 and 3 of Part VIB.

The OAIC Annual Report for 2019/20 recorded that in the 2019-20 reporting period, the OAIC closed 3,399 privacy complaints which was a 15% improvement upon the 2019/18 reporting period. The OAIC finalised 87% of all privacy complaints within 12 months of receipt. The OAIC delivers guidance for regulated entities to improve awareness and practices regarding its regulatory functions. In this reporting period, for the first time, the OAIC utilised its powers under the Privacy Act to initiate proceedings in the Federal Court against Facebook Inc and Facebook Ireland for alleged serious and/or repeated interferences with privacy in contravention of Australian privacy law. The OAIC has reported that 77% of privacy complaints closed in the 2019/20 reporting period were resolved in what was termed the 'early resolution approach' where the complaints were assessed against the OAIC's jurisdiction and informal resolution is attempted. In 2019/20 the OAIC conciliated 175 complaints with 59% successfully resolved. Following the implementation of this tiered response mechanism, the majority of matters are dealt with via informal mechanisms or via conciliation with only 4 determinations being ultimately issued by the OAIC in the 2019/20 reporting period.

The above outline of the OAIC's performance over the previous financial year suggests that the enforcement framework available under the Privacy Act is working.

It is essential that the Government not pursue any avenue which would allow for representative proceedings to be brought under the Privacy Act. Contrary to the ACCC's rationale for its recommendation in the Final Report from the DPI that a direct right of action for individuals be introduced, class actions do not provide individual applicants with greater control over proceedings, particularly where the action is financed by a litigation funder. Litigation funders lack the same duties to group members which law firms ostensibly are required to uphold. This problem has been exacerbated by the exclusion of litigation funders from the general regulatory oversight which applies elsewhere in the financial services industry. The recent announcement of licensing requirements for litigation funders is a welcome reform but will only go part way toward addressing the issue. The interests and positions of individual class members may be overlooked where a litigation funder exerts control over positions taken and arguments pursued by, lawyers in the proceedings.

In some circumstances, class actions have been used as an avenue for litigation funders and plaintiff law firms to make an unreasonable profit at the expense of business and nominal group members genuinely seeking redress. In his ex-tempore reasons for approving a recent settlement of three class actions regarding the Commonwealth's use of allegedly toxic firefighting foam, Lee J acknowledged the value of the availability of class actions but noted that the phrase 'access to justice' is often misused by funders to justify "what at bottom is a commercial endeavour to make money out of the conduct of litigation".

A significant proportion of the funds which have been extracted from businesses as a result of class action disputes is paid to law firms to satisfy high legal fees and to discharge a contractual obligation to pay a return to litigation funders rather than to the group members themselves. The diversion of

these financial resources to entities which take advantage of an unregulated system merely drains value from the economy and minimises the return available to group members seeking justice.

The financial benefits to a litigation funder may be at the expense of class members in representative proceedings. In a keynote address to then one of Australia's largest litigation funders IMF Bentham, Hon Michael Lee criticised the practice of calculating a litigation funder's minimum return on the basis of legal costs. He said:[16]

> *…speaking frankly there are people who are participants in the industry. Or likely participants in the industry where I've seen funding agreements which frankly are hard to justify including those funding agreements which have a return which is struck by reference to a multiple of legal costs as a minimum. Well you know that just can't work.*
>
> *…*
>
> *It is rightly a scandal for there to be situations where group members in proceedings where there has not been a massive change in prospects since the commencement of proceedings recovering only a very very small return for their claim and in circumstances where legal costs have become extraordinarily large. And and funding commission taking on top of that means they're recovering very little. Now one hopes that you have practitioners people who a duties to the Court that makes sure make sure that that doesn't happen or seek to minimise the prospect of that happening. And one I'm sure the Court would expect that certainly senior practitioners involved in those sort of cases would be saying they're not putting things up for approval unless things change. But those sort of matters are ones that candidly the Court would expect to see put before it on a settlement approval.*

The disproportionately high returns due to litigation funders in funding agreements are such that the entities often receive an unfair share of litigation proceeds. In one case which was referred to the Victorian Law Reform Commission in its inquiry into litigation funding and group proceedings, once costs were paid out of the awarded amount, class members received nothing of the proceeds. The case concerned a claim made by trustees for former employees of Huon Corporation Limited against CBL Insurance Ltd. The action was initiated on behalf of 336 former employees with final orders made in May 2015. Out of the final settlement amount of $5,107,259 ($4,132,232 was the principle sum based on employee entitlements), the litigation funder received 36.3% of the award. Once legal fees, accounting and administrative assistance and the liquidator's fee were taken out, no part of the award was available for the benefit of class members on whose behalf the action was brought.

In representative proceedings, the interests of group members are at times opposed to their legal representatives. The presence of a litigation funder introduces an additional element whereby the matter, ostensibly brought in the group members' interests is financed on the speculative

[16] IMF Bentham, 'Keynote Address, The Hon Justice Michael Lee', 27 June 2017, https://www.imf.com.au/newsroom/blog/blog-full-post/class-action-centre/2017/06/27/imf-class-action-conference-keynote-address-the-hon-justice-michael-lee-(federal-court-of-australia).

assumption that a return will be available to the funder. As the initiation of funded proceedings depends on the funder's interests being satisfied, it is not difficult to imagine a scenario where group members' interests are overlooked or watered down to ensure funding will be available

Allowing for representative proceedings to be initiated for alleged breaches of the Privacy Act would encourage speculative litigation and ultimately result in less control over proceedings for individual applicants, particularly where litigation funding agreements are signed. On 13 May 2020, the Commonwealth House of Representatives referred an Inquiry to the Parliamentary Joint Committee on Corporations and Financial Services into Litigation funding and the regulation of the class action industry. The Committee is due to table its report by 7 December 2020. Currently, the class action regime in Australia provides inadequate oversight of litigation funders and insufficient safeguards for class members in representative proceedings. It would be inappropriate to introduce a mechanism for initiating class actions for breaches of the Privacy Act particularly while this remains the case.

10. A STATUTORY TORT

The introduction of a statutory tort for invasion of privacy would amount to a significant change to the enforcement regime pertaining to privacy breaches that is not justified by any apparent shortcomings in the existing avenues available for enforcing individual rights to protection from invasion of privacy.

The potential existence of a common law tort regarding invasion of privacy has been explored by the judiciary. Perry J of the Federal Court of Australia recently made the following comments in a decision issued on 10 September 2020 (references omitted):[17]

> *The door has not been closed to the possibility that a tort of privacy might develop in Australia following the decision in Lenah Meats, even though it has been cautioned that "the statements of the majority in Lenah do not support the suggestion that the High Court in Lenah held out any invitation to intermediate courts in Australia to develop the tort of privacy as an actionable wrong."*

Perry J referred to comments made by Basten JA in the New South Wales Court of appeal[18] that the absence from the common law of an established tort for unjustified invasion of privacy has been noted on more than one occasion and that such cases "may well lay the basis for development of liability for unjustified intrusion on personal privacy, whether or not involving breach of confidence". The current uncertainty regarding the development of a tort of privacy across all jurisdictions in the Commonwealth is harmful in that it leaves businesses in a state of uncertainty regarding their liabilities in the realm of privacy. It would be beneficial for any reforms to the Privacy Act to confirm that the enforcement avenues available under the Act cover the field and any overlapping common law torts which may exist are not available.

[17] *DOQ17 v Australian Financial Security Authority* (No 3) [2019] FCA 1488, [222]-[223].
[18] *Maynes v Casey* [2011] NSWCA 156, [34] – [35].

The fault element for any proposed statutory tort should not extend to strict or negligence-based liability. Ai Group considers that opening an avenue for prosecution on the basis of recklessness to be oppressive and likely result in businesses taking an excessively risk averse stance with respect to the treatment of employee information. In many cases, the communication of private information concerning employees would be welcome. This may be the case in the context of a medical emergency, where an employee would like an employer to provide a reference following termination of employment or where a financial services provider seeks an employer to provide some evidence regarding an employee's financial status. It is not in the interests of employers or employees to introduce a statutory tort relating to privacy, particularly if the fault element extends to negligence as disclosure of private information in the ordinary conduct of business would place employers at undue risk of prosecution. Establishing strict liability or negligence as the requisite fault element in a statutory tort would place employers in a very difficult position where required to disclose information in a court of law. Employers should not be placed in the position of risking breaching a statutory tort by disclosing excessive information where responding to a court request or being found in contempt of court for failing to disclose all relevant information requested. The introduction of a statutory tort of invasion of privacy should not be pursued, however it is particularly urgent that any fault element not extend to negligence on the part of the defendant.

It should be acknowledged that in many circumstances businesses are compelled to provide private information to various regulatory bodies. For example, Division 2 of Part 3-4 of the FW Act provides avenues for access to records or documents held by employers in the context of right of entry exercised by an industrial association. The Fair Work Ombudsman retains a separate right to require employers to produce records or documents.[19] Pursuant to the *Building and Construction Industry (Improving Productivity) Act 2016* (Cth) (**BCCI Act**), authorised officers have the power to require employers to provide records which may contain private information concerning employees.[20] Separate provisions are provided under the BCCI Act regarding the confidentiality of information obtained under an examination notice.[21] Entities covered by the Commonwealth Building Code are already required to ensure that personal information concerning subcontractors is dealt with in accordance with the Privacy Act.[22] Any tort of privacy introduced should ensure an exemption applies which is at least as broad as that applicable under the existing employee records exemption under the Privacy Act.

The nature of a tort, by focussing on redress by way of an award of damages, is unsuitable to breaches of privacy in the context of employment. Employers typically keep personal records with a view to ensuring the efficient running of a business or compliance with obligations under workplace legislation which may relate to matters including industrial relations, work health and safety and anti-discrimination. Although an individual may consider retention or use of personal information in the employment context to infringe a right to privacy, the prospect of compensation being ordered by way of damages is inappropriate considering the public interest in employers

[19] *Fair Work Act 2009* (Cth) s. 712.
[20] *Building and Construction Industry (Improving Productivity) Act 2016* (Cth), Chapter 7, Part 3 Division 3.
[21] *Building and Construction Industry (Improving Productivity) Act 2016* (Cth), Chapter 9, Part 2, Division 2.
[22] Code for the Tendering and Performance of Building Work 2016, cl. 13.

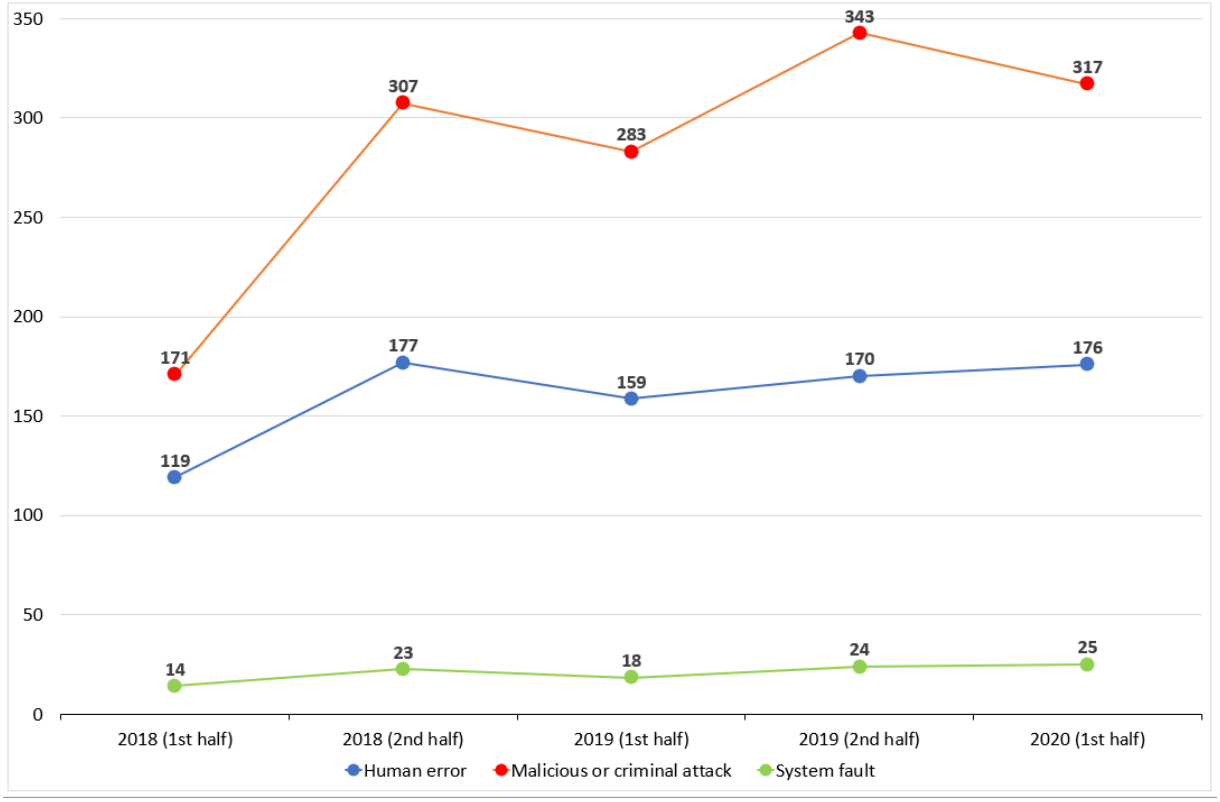
exercising reasonable use of personal information to effectively manage their workforce.

The emphasis on damages and compensation in tort law may encourage speculative litigation by individuals claiming mental distress. Vicarious liability for the wrongs of an employee presents a significant risk for employers in the context of tort law. The various risk mitigation strategies and the litigation insurance costs which would be necessitated by the establishment of a privacy tort would not be in the public interest. An actionable tort *per se* (i.e. where there is no need for the claimant to establish any form of damage) would expose employers to an even greater risk which is not counterbalanced by any public benefit from introducing a tort of privacy.

11. NOTIFIABLE DATA BREACHES SCHEME IMPACT AND EFFECTIVENESS

Chart 1 below shows the number of data breaches reported to the OAIC since the NDB Scheme commenced in February 2018.

Chart 1: Notifiable data breaches since NDB Scheme commenced (by breach category)



Source: OAIC

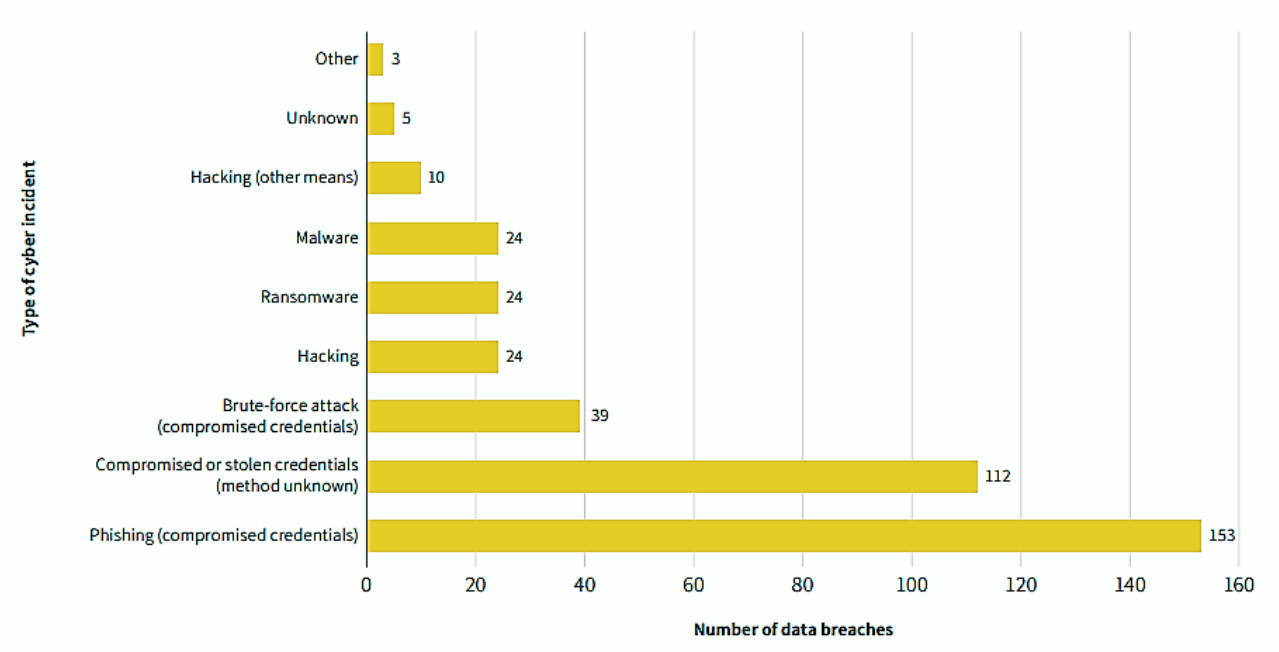
By the end of June 2020, there were over 2,320 data breaches reported to the OAIC since the NDB Scheme commenced.[23] Over this period, malicious or criminal attacks greatly contributed to these data breaches (61%), followed by human error (34%). System faults (4%) were rarely a factor.

[23] OAIC, Notifiable Data Breaches Quarterly Statistics Reports (January 2018 – March 2018, 1 April – 30 June 2018, 1 July – 30 September 2018, 1 October – 31 December 2018, 1 January 2019 – 31 March 2019, 1 April 2019 – 30 June 2019, 1 July 2019 – 31 December 2019, 1 January 2020 – 30 June 2020).

Delving deeper into the data, the OAIC provided a breakdown of the types of cyber security incidents that gave rise to data breaches from the period of 1 April 2018 to 31 March 2019 (see Chart 2).[24] For the same period, the OAIC also categorised the type of human errors and system faults that resulted in data breaches (see Chart 3).[25]

These causes for data breaches point to the need for cyber security hygiene within organisations, as well as more general improvements in internal management of personal data to minimise human errors. And according to a Telstra report, human errors were "often caused by inadequate business processes and employees not understanding their organisation's security policies".[26]

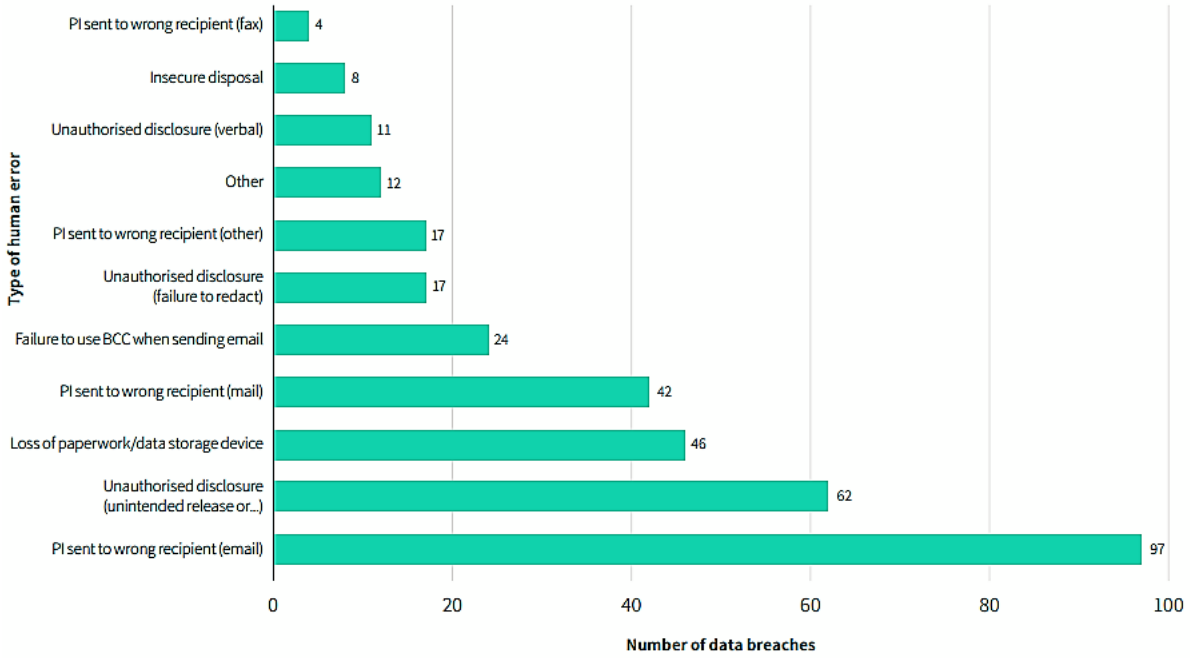
Chart 2: Notifiable data breaches caused by cyber security incidents, 1 April 2018 – 31 March 2019



Source: OAIC, Insights Report, 2019

[24] OAIC, "Notifiable Data Breaches Scheme 12-month Insights Report" (Report, May 2019), p. 10.
[25] Ibid, p. 12.
[26] Telstra, "Breach expectation: the new mindset for cyber security success" (Article on Telstra website, April 2019).

Chart 3: Notifiable data breaches caused by human error and system faults, 1 April 2018 – 31 March 2019



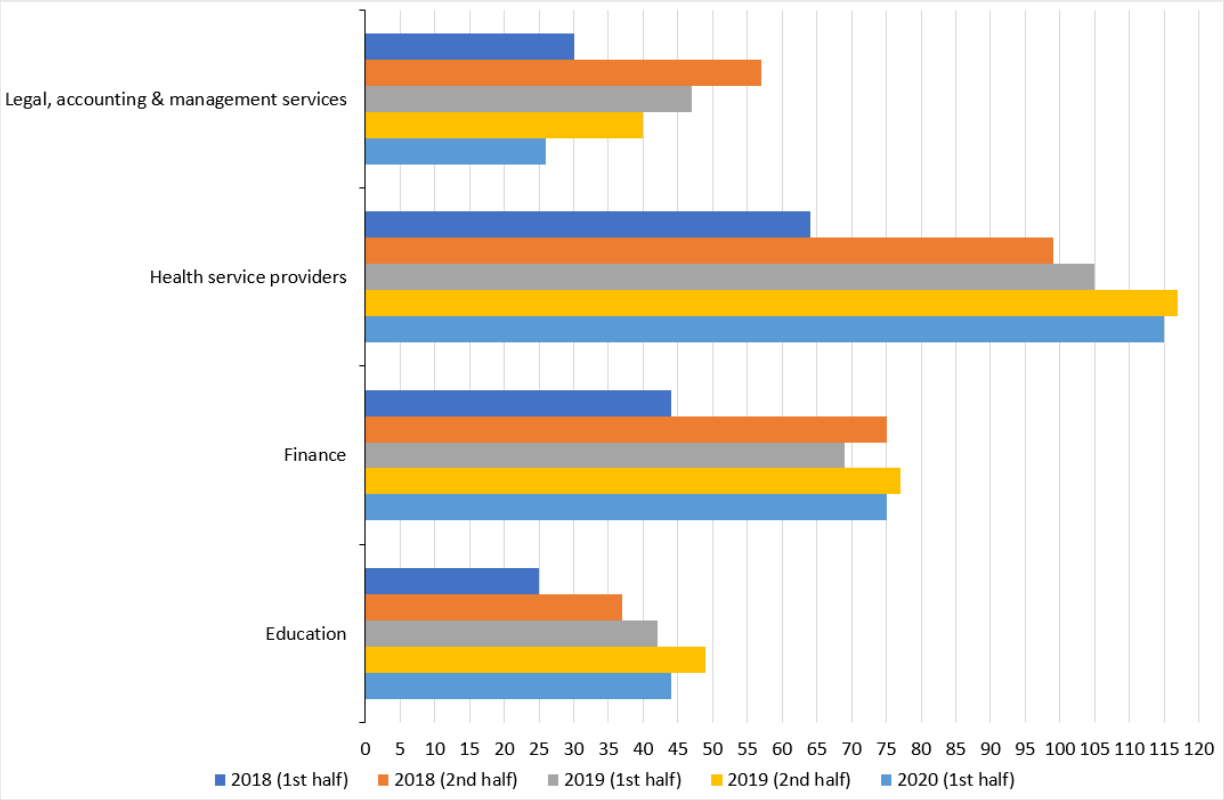
Source: OAIC, Insights Report, 2019

Of the breaches reported to the OAIC since the NDB Scheme commenced, industries that have regularly appeared included: health service providers (21%); finance (15%); professional services (legal, accounting and management) (9%); and education (8%). Chart 4 provides a half-yearly breakdown of notifiable data breaches reported for these sectors.[27] Given how much personal data are handled in these respective industries, this should be no surprise. Of greater concern was that these sectors service other industries so others were not immune.

The fact that there was a steady rate of data breaches being reported from a diverse range of industries highlight the need for additional government support.

[27] OAIC, Notifiable Data Breaches Quarterly Statistics Reports (January 2018 – March 2018, 1 April – 30 June 2018, 1 July – 30 September 2018, 1 October – 31 December 2018, 1 January 2019 – 31 March 2019, 1 April 2019 – 30 June 2019, 1 July 2019 – 31 December 2019, 1 January 2020 – 30 June 2020).

Chart 4: Notifiable data breaches since NDB Scheme commenced (by top sectors)



Source: OAIC

As discussed above, the latest NDB data breach analysis shows that a high proportion of data breaches were due to human error. Therefore, it is not only about having cyber security technology to mitigate data breaches.

We have received anecdotal feedback from businesses, especially SMEs, about the costs arising from new legislation such as the NDB Scheme. Other data and privacy legislations such as the EU GDPR and CDR (which is being developed for specific sectors), as well as the controversial TOLA Act, also present an additional regulatory burden and challenge for a range of businesses. Government support for businesses to meet these obligations may be required.

Notwithstanding the above, we have seen improvements in business investment in cyber security. Of businesses previously surveyed by Ai Group, 79% indicated that they invested in cyber security measures in 2018.[28] While our survey did not explore other drivers for cyber security investment, the higher proportion of businesses proactively investing in cyber security compared to our previous survey suggested a dramatic shift in business attitudes. This may possibly be due to increasing awareness about cyber management hygiene, and compliance with new privacy and data breach legislations such as the NDB Scheme and EU GDPR.

The NDB Scheme was introduced with an intention to reduce data breaches. While well intentioned, we consider that the Scheme may only promote a compliance culture, as opposed to a proper

[28] Ai Group, Fourth Industrial Revolution: Australian Businesses in Transition (August, 2019), https://cdn.aigroup.com.au/Reports/2019/AiGroup_Fourth_Industrial_Revolution_Report.pdf.

proactive leadership and risk management culture. There are still questions as to how integrity and privacy measures can be put in place to mitigate data breaches from occurring in the first instance.

In this regard, a policy or regulatory response is only effective if it properly identifies and targets the problem that it is trying to address. Automatically reaching for penalties may not be the most effective solution, and potentially creates a compliance-only mindset.

And this is especially the case when a business is a victim as well. The Government has stated that cyber security incidents cost Australian businesses up to $29 billion each year, with almost one in three Australian adults impacted by cybercrime. Recent reports released by the ACSC and ACCC highlight the impact of cyber security incidents. According to the ACCC, Australians lost over $634 million to scams in 2019.[29] The ACSC indicates that it received almost 60,000 reports a year, or one report every 10 minutes – and bearing in mind those are only reported incidents, noting that cybercrime within Australia is underreported.[30] We therefore support the Government's recently announced investment in cyber security related measures to assist businesses and individuals in its 2020 Cyber Security Strategy and affirmed in the Federal Budget. Nevertheless, these various reports also highlight the importance of proper coordination between Government agencies to assist businesses and individuals that are victims of cyber security related incidents.

In other forms of regulation such as safety, business and governments have evolved over decades from pure compliance and concerns about over-regulation to a culture of risk management – this was partly driven by customer and supply chain expectations as they became more informed about safety.

Rather than automatically reaching out for new regulatory instruments, further collaboration will be needed between industry and governments to explore workable and practical remedies such as technological solutions.

Bodies such as the ACSC should be commended for working closely with organisations affected by data breaches. However, as the ACSC has noted, this is help after the fact.[31]

Given that a large proportion of data breaches under the NDB Scheme have been triggered by malicious or criminal attacks, or human error, it is important to tackle these causes and prevent breaches from occurring in the first place. For instance, while the OAIC suggested that awareness of the NDB Scheme appeared to be high, there remains a potential gap in awareness about mitigating data breaches, as well as responding to them effectively if they do arise.[32]

As noted earlier, industries that regularly appear in the NDB reporting include health service providers, finance, professional services (legal, accounting and management) and education. This suggests a targeted approach to cyber security awareness raising is worth considering – sometimes referred to as a "public health" approach where those most vulnerable are targeted with

[29] ACCC, "Targeting scams 2019: A review of scam activity since 2009" (June 2020).
[30] ACSC, "Annual Cyber Treat Report, July 2019 to June 2020" (September 2020).
[31] OAIC, "Notifiable Data Breaches Scheme 12-month Insights Report" (Report, May 2019), p. 19.
[32] Ibid.

appropriate messaging. In this case, a specific awareness campaign could be developed that targeted the industries that most often appear on the NDB reporting.

12. INTERACTION BETWEEN THE ACT AND OTHER REGULATORY SCHEMES

We consider that there are various government consultations and initiatives that are relevant for consideration in relation to this review. We note that some of these interrelated consultations are occurring concurrently with similar tight deadlines, particularly towards the end of the year (e.g. Home Affairs' consultation on *Protecting Critical Infrastructure and Systems of National Significance* Exposure Draft Bill, and DISER's consultation on its AI Action Plan). In terms of process, we recommend that better coordination should be undertaken by the AGD and other relevant Government agencies to enable for proper consultation for both this review and others underway.

Below is a non-exhaustive list. Where possible, we have also referenced our previous submissions covering similar issues that may also be relevant to this review:

- DITRDC's consultation on a new Online Safety Act – online safety proposals in this consultation may be relevant to privacy under consideration.[33]

- Home Affairs' *Voluntary Code of Practice: Securing the Internet of Things for Consumers* – a range of matters with respect to the proposed Code of Practice that may be relevant to this consultation.[34]

- Home Affairs' consultation on *Protecting Critical Infrastructure and Systems of National Significance* – our submission raises several issues including details that currently remain unclear and require further consultation such as the nature of the reforms, scope, definitions, measures and cost-benefit impact.[35]

- Home Affairs' consultation on its draft Critical Technology Supply Chain Principles – a range of matters including principles that may be applicable to this consultation.[36]

- Treasury's consultation on *Major reforms to the Foreign Investment Review Framework* – we consider that there are potential interactions between Home Affairs' critical infrastructure security reforms and Treasury's reforms. In particular, Treasury's proposed changes to the

[33] Ai Group submission to Commonwealth Department of Infrastructure, Transport, Regional Development & Communications, *Consultation on a new Online Safety Act* (February 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/New_Online_Safety_Act_Proposals_21Feb_2020.pdf.
[34] Ai Group submission to Home Affairs (February 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/Securing_IoT_for_Consumers_Voluntary_Code_of_Practice_Feb_2020.pdf.
[35] Ai Group submission to Home Affairs (September 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/Dept_Home_Affairs_Critical_Infrastructure_Security_Reforms_Sept2020.pdf.
[36] Ai Group submission to Home Affairs (November 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/Home_Affairs_Critical_Technology_Supply_Chain_Principles_Discussion_Paper_12Nov.pdf.

Foreign Acquisitions and Takeovers Act 1975 (Cth) (FATA) would subject any business responsible for, or with a significant stake in, critical infrastructure covered by the *Security of Critical Infrastructure Act 2018* (Cth) (SCIA) to substantial new obligations and powers under the FATA. Thus decisions about the scope of the SCIA will have larger implications that need to be fully considered in regulatory impact analysis.[37]

- Treasury's consultation on its *Inquiry into Future Directions for the Consumer Data Right* – we raised several interrelated issues including on privacy, data protection and cyber security.[38]

- Treasury's consultation on *Improving the Effectiveness of the Consumer Product Safety System* – insofar as privacy relates to the consumer, privacy may also fall under the scope of Treasury's consultation if it leads to consumer safety issues.[39]

- Parliamentary Joint Committee on Intelligence and Security (PJCIS) and Independent National Security Legislation Monitor (INSLM) reviews relating to the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (TOLA Act) – there are concerns about the potential negative impact of this Act on cyber security and privacy of products and services.[40] We have recently made a supplementary submission supporting the INSLM's recommendations.[41]

- The PJCIS review into the effectiveness of the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020* – we consider this Bill is interrelated with the TOLA Act review.[42]

---

[37] Ai Group submission to Treasury (September 2020), Link: https://cdn.aigroup.com.au/Submissions/Trade_and_Export/Submission_FATA_reforms_September_2020.pdf.
[38] Ai Group submission to Treasury (June 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/Treasury_CDR_Inquiry_5 Jun_2020.pdf.
[39] Commonwealth Treasury, *Improving the Effectiveness of the Consumer Product Safety System*, Link: https://consult.treasury.gov.au/market-and-competition-policy-division-internal/main-consultation.
[40] Joint submission to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS), *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA Act)* (Submission No. 23, July 2019), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Submissions; Joint submission to the Independent National Security Legislation Monitor (INSLM), *Review of the TOLA Act* (Submission No. 15, September 2019), Link: https://www.inslm.gov.au/submissions/tola; Ai Group submission to the INSLM, *Review of the TOLA Act* (Submission No. 12, September 2019), Link: https://www.inslm.gov.au/submissions/tola; Australian Strategic Policy Institute (ASPI), *Perceptions survey: Industry views on the economic implications of the Assistance and Access Bill 2018* (December 2018), p. 3.
[41] Ai Group supplementary submission to PJCIS (Submission No. 23.1, July 2020), Link: https://www.aph.gov.au/DocumentStore.ashx?id=d40979d1-6ce6-4460-a6d5-bd903f757cb8&subId=668167.
[42] Ai Group submission to PJCIS (Submission No. 32, May 2020), Link: https://www.aph.gov.au/DocumentStore.ashx?id=f73c608e-f21d-42a0-972d-56aebbcd7d57&subId=682819.

- The Standing Committee on Communications and the Arts Inquiry into 5G in Australia – while cyber security has been excluded from this Inquiry, there are interrelated considerations with respect to the operation of 5G and IoT.[43]

- The Australian Human Rights Commission's (AHRC) consultation into Human Rights and Technology – as the title suggests, the AHRC have been exploring the impact of emerging technologies on human rights.[44]

- DISER's AI initiatives such as the AI Ethics Framework, and its recently commenced consultation on an AI Action Plan.[45]

- The Ambassador for Cyber Affairs and Critical Technology within DFAT has been consulting on Australia's International Cyber and Critical Technology Engagement Strategy, which may be potentially be relevant to this consultation.[46]

- With respect to standards, there already exists standards (especially international) and initiatives to support industry standards relevant to privacy that may address or respond to the issues raised in AGD's Issues Paper. For instance, Standards Australia's AI Standards Roadmap includes references to standards.[47] Also, Ai Group is involved in a partnership with the NSW Government, Standards Australia, AustCyber and other key industry stakeholders to harmonise cyber security standards across several key sectors. There is an opportunity for the scope of this work to be expanded to other sectors.

[43] Ai Group submission to Standing Committee on Communications and the Arts, *Inquiry into 5G in Australia* (Submission No. 356, November 2019), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Communications/5G/Submissions.
[44] Ai Group submission to AHRC, *Discussion Paper on Human Rights and Technology*, Link: https://cdn.aigroup.com.au/Submissions/Technology/AHRC_Human_Rights_and_Technology_Discussion_Paper_26Mar_2020.pdf.
[45] DISER, *AI Action Plan*, Link: https://www.industry.gov.au/news-media/australias-ai-action-plan-have-your-say.
[46] DFAT, *International Cyber and Critical Technology Engagement Strategy*, Link: https://www.dfat.gov.au/international-relations/themes/cyber-affairs/public-consultation-international-cyber-and-critical-technology-engagement-strategy.
[47] Standards Australia, *Artificial Intelligence Standards Roadmap: Making Australia's Voice Heard* (March 2020), Link: https://www.standards.org.au/news/standards-australia-sets-priorities-for-artificial-intelligence.

ABOUT THE AUSTRALIAN INDUSTRY GROUP

The Australian Industry Group (Ai Group®) is a peak employer organisation representing traditional, innovative and emerging industry sectors. We are a truly national organisation which has been supporting businesses across Australia for nearly 150 years.

Ai Group is genuinely representative of Australian industry. Together with partner organisations we represent the interests of more than 60,000 businesses employing more than 1 million staff. Our members are small and large businesses in sectors including manufacturing, construction, ICT, transport & logistics, engineering, food, labour hire, mining services, the defence industry and civil airlines.

Our vision is for thriving industries and a prosperous community. We offer our membership strong advocacy and an effective voice at all levels of government underpinned by our respected position of policy leadership and political non-partisanship.

With more than 250 staff and networks of relationships that extend beyond borders (domestic and international) we have the resources and the expertise to meet the changing needs of our membership. Our deep experience of industrial relations and workplace law positions Ai Group as Australia's leading industrial advocate.

We listen and we support our members in facing their challenges by remaining at the cutting edge of policy debate and legislative change. We provide solution-driven advice to address business opportunities and risks.

OFFICE ADDRESSES

NEW SOUTH WALES

Sydney
51 Walker Street
North Sydney NSW 2060

Western Sydney
Level 2, 100 George Street
Parramatta NSW 2150

Albury Wodonga
560 David Street
Albury NSW 2640

Hunter
Suite 1, "Nautilos"
265 Wharf Road
Newcastle NSW 2300

VICTORIA

Melbourne
Level 2 / 441 St Kilda Road
Melbourne VIC 3004

Bendigo
87 Wil Street
Bendigo VIC 3550

QUEENSLAND

Brisbane
202 Boundary Street Spring Hill
QLD 4000

ACT

Canberra
Ground Floor,
42 Macquarie Street
Barton ACT 2600

SOUTH AUSTRALIA

Adelaide
Level 1 / 45 Greenhill Road
Wayville SA 5034

WESTERN AUSTRALIA

South Perth
Suite 6, Level 3 South Shore Centre 85
South Perth Esplanade
South Perth WA 6151

www.aigroup.com.au

Appendix B

Ai GROUP SUBMISSION

Australian Government
Attorney-General's Department

Review of the Privacy Act 1988 – Discussion Paper

January 2022

Table of Contents

1. Introduction

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission on the Discussion Paper for the Review of the *Privacy Act 1988* (Cth) by the Attorney-General's Department (AGD). This submission follows on from our previous submission on the Issues Paper to the AGD in November 2020.

We note that the Issues Paper stage provided the AGD with an opportunity to start the conversation regarding areas in which the Privacy Act Review could cover in a holistic way. The Discussion Paper has now been released which includes potential options to reform the Privacy Act.

However, at this time we have not yet been provided with a Regulation Impact Statement (RIS) and details of the proposed timeline for implementation of the proposed reforms. Given the extensive nature of the proposed reforms and wide-ranging impact on businesses, we submit that a significant transition period will be required should these reforms proceed.[1]

In reviewing the Discussion Paper, including various proposals and questions, we consider that the volume of material needs to be properly worked through with stakeholders.

Given the extensive review and wide implications that proposals arising from the review could have on many businesses, we propose that the AGD consider breaking down their proposals into a more digestible and manageable manner, to allow sufficient time to be considered practically. This will ensure that stakeholders are properly engaged.

For instance, we suggest the consultation could be structured and coordinated by the AGD along the following lines:

- Categorise the different areas in which the AGD considers should be prioritised in its review and consult in a more structured manner. This should also take account of appropriate sequencing of related proposed amendments including the Exposure Draft of the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* (OP Bill) and associated OP Code.

- Develop a consultation schedule including timeline and action plan to address specific areas. This should include a clear statement detailing the proposed lead time for implementation by regulated entities. Timelines should recognise the continuing impact of COVID-19 on regulated businesses.

- Walk through the issues and associated proposals, which can be undertaken via stakeholder workshops for example. This should assist the AGD to properly categorise and prioritise the issues and their potential options, as noted above.

- Following proper stakeholder consultation, the AGD could provide a RIS and undertake targeted consultations focused on specific areas and proposals that arise from the Privacy Act Review.

As a matter of good policy and regulatory practice, this consultation should be based on proper identification, analysis and assessment of issues, underlying causes, options to address these issues, as well as a robust and considered cost-benefit assessment for any proposed regulatory or legislative change. We consider the above steps will be strongly contingent on these conditions. At this stage, we maintain that this work still needs to be done.

[1] As a comparison, we note that a two-year period was provided for the EU General Data Protection Regulation (GDPR).

In contrast, we do not consider that the concurrent Exposure Draft of the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* (OP Bill) is an appropriate option at this stage. For various reasons stated in our submission to the AGD on the OP Bill, matters raised in the OP Bill should be considered as part of the broader umbrella of the Privacy Act Review, rather than in a separate and concurrent consultation.[2]

At this stage of the review, we maintain our positions in our previous submission to the Issues Paper. These are briefly discussed in our submission, as well as additional comments arising since our last submission in November 2020.

2. Issues and proposals for further consideration

The following is a list of key issues and considerations that Ai Group raised in our submission to the Issues Paper, which we continue to stand by, including with respect to:

- Definition of personal information:[3]
    - There should be caution against shifting emphasis of protecting consumers under the current regime to data protection under the EU GDPR. The EU GDPR is a complex scheme with qualifications and exceptions that operate to ensure that its requirements are capable of practical implementation. Adoption of definitions and other individual features of the EU GDPR risks over-inclusiveness and unworkability.
    - Consideration should be given to the impact of multiple forms of regulation in this area such as Consumer Data Right and industry specific regulations. Over-regulation has the potential to chill innovation and add costs to business.
    - Appropriate assistance should be provided for industry, including additional guidance and other ways to alleviate regulatory compliance burdens for businesses.
- Flexibility of the APPs:[4]
    - We consider the current principles-based privacy regime to be appropriate, given its flexibility to enable future proofing and therefore technology neutrality in a rapidly changing environment.
    - Government should be aware of various issues associated with adopting an EU GDPR approach. For instance, international experience suggests that the EU GDPR has been highly prescriptive, with certain provisions introducing significant burdens on regulated businesses without necessarily providing demonstrable benefit to individuals. Retaining the flexibility of the APPs would mitigate the risk of a similar outcome in Australia.
- Notice of collection of personal information:[5]
    - Government should be cognisant of the risk of cumulative increase of notifications and information overload for consumers associated with notice of collection requirements.

[2] We refer the AGD to our separate submission on the Online Privacy Bill for further information: https://www.aigroup.com.au/news/submissions/2021/online-privacy-bill-exposure-draft/.

[3] Ai Group submission to AGD (November 2020), pp. 5-6, https://www.ag.gov.au/sites/default/files/2020-12/ai-group.PDF.

[4] Ai Group submission to AGD (November 2020), pp. 7-9.

[5] Ai Group submission to AGD (November 2020), pp. 14-16.

- Government should properly assess whether there are material consumer benefits from expanding the range of requirements for giving of notice of collection requirements, and as to the content of these notices.

- Government should consider alternative options and assess their relative costs and benefits. A RIS would be of assistance in this regard.

- Consent to the collection, use and disclosure of personal information:[6]

  - Similar to the issue of notice of collection requirements, Government should be cognisant of the risk of creating information overload or consent fatigue for consumers with consent requirements.

  - There are practical implementation issues for businesses if the statute expands the range of requirements for obtaining of consent, or the form of requests for consent.

  - Opt-in consent should only be required where this has a real identified benefit to individuals and does not materially impact on the ability of businesses to continue to provide innovative services to the benefit of consumers and the broader Australian economy.

  - Government needs to properly understand the EU GDPR approach to consent. This includes the many exceptions and limitations to those consent requirements, including the legitimate interest exceptions.

  - Government should be cautious to not add a costly regulatory burden to businesses by requiring the retrospective operation of consent requirements in relation to already obtained data.

  - A proper assessment (including cost-benefit) of material consumer benefits should be undertaken with respect to any proposed consent requirements. A RIS would be welcome.

- Right to erasure or be forgotten:[7]

  - There is no evidence of consumer need for this right (over and above existing disposal requirements under APP 11), or that any need outweighs the significant regulatory burden, technical implementation issues, and substantial costs for entities that would be required to implement such a scheme.

  - Consideration should also be given to how erasure rights would impact insights that businesses develop through their own methods (e.g. inferences).

  - Proper consideration of public interest exemptions should be given to the right to erasure to ensure proper consumer safeguards are factored in and not inadvertently impacted such as in terms of ensuring privacy and security, preventing fraudulent activity and resolving later complaints or litigation.

  - Introducing this right could create a conflict with providing incentives to entities to ensure effective anonymisation of personal information to better protect against privacy risks.

  - Introducing this right could also conflict with mandatory regulatory requirements for retention of personal data.

[6] Ai Group submission to AGD (November 2020), pp. 16-18.

[7] Ai Group submission to AGD (November 2020), pp. 18-19.

- Unlike under the EU GDPR, the proposed right is not qualified through judicial oversight and ability to make public interest considerations. This should be taken into account and amended.

The above matters were discussed more comprehensively in our previous submission to the Issues Paper. We strongly encourage Government to review our previous submission regarding the above matters.

In addition, we would also like to build further in this submission on our previous views regarding:

- Definition of personal information;
- Notice of collection, use and disclosure of personal information;
- Consent of collection, use and disclosure of personal information;
- Employee records exemption;[8]
- A direct right of action;[9]
- A statutory tort of privacy;[10]
- Notifiable Data Breaches (NDB) Scheme;[11] and
- Interactions with other schemes.[12]

There are also other matters which we would like to discuss further relating to:

- The small business exemption;
- Direct marketing, targeted advertising and profiling;
- Automated decision-making; and
- Enforcement.

These matters are discussed in further detail in the remainder of this submission.

We would welcome discussing these issues and associated proposals in further detail as these matters progress further as part of the consultation process.

3. Definition of personal information

3.1 Scope

The Discussion Paper proposes various ways in which the definition of personal information in the Privacy Act could be potentially amended under Proposals 2.1 to 2.4 by:

- changing the word "about" in the definition of personal information to "relates to";

[8] Ai Group submission to AGD (November 2020), pp. 10-14.

[9] Ai Group submission to AGD (November 2020), pp. 19-23.

[10] Ai Group submission to AGD (November 2020), pp. 23-25.

[11] Ai Group submission to AGD (November 2020), pp. 25-30.

[12] Ai Group submission to AGD (November 2020), pp. 30-32.

- including a non-exhaustive list of the types of information capable of being covered by the definition of personal information;

- defining "reasonably identifiable" to cover circumstances in which an individual could be identified, directly or indirectly, and including a list of factors to support this assessment; and

- amending the definition of "collection" to expressly cover information obtained from any source and by any means, including inferred or generated information.

There is a real risk that these proposals would create a significant and inadvertent negative regulatory impact on entities and the possibilities of innovation, without necessarily providing material benefit to consumers. We note similar issues could arise if the definition of sensitive information were to be amended. These will also depend on the context and it will be important that proper consideration be given to such circumstances. For instance, it would be concerning if a changed definition unintentionally interfered with the normal operation of critical infrastructure, as well as any other service or system, that required access to such information.

Proposed amendments that expand the definition also pose risks, including information saturation where meaningful information would be lost through increased notice obligations, the inability to conduct meaningful analytics that would stifle innovation, and generally practical difficulties with notifying individuals when technical identifiers alone are collected and no further attributes are known.

As noted in our previous submission, the current definition of personal information provides for flexibility to include things like IP addresses, for example, in situations where they can reasonably identify someone (or are associated with other information that is about someone or which could reasonably identify someone). The OAIC has also pointed out in their own guidance, whether a person is reasonably identifiable "is an objective test" which depends on the "context in which the issue arises".[13] If the information could reasonably identify someone, it is already covered by the definition; and if it cannot reasonably identify someone (for example, an IP address taken in isolation), then it does not require the same level of protection as personal information.

Therefore, contextual evaluation will be critical and cannot be avoided with any proposed amendment in the definition of personal information. Such an evaluation may entail consideration of the particular circumstances of that entity, that entity's reasonable access to other information, the nature of the relevant information, and the data situation in which that relevant information is collected and handled.

It is also unclear how some of the APPs would apply to technical information. For example, data quality obligations (APP 10) and correction rights (APP 13) may not make sense in the case of technical information.

3.2 De-identification, anonymisation and pseudonymisation

Under the Privacy Act, de-identified information is not regarded as personal information and therefore not subject to the legislation. Proposal 2.5 in the Discussion Paper proposes to differentiate between de-identified information and anonymised information by requiring personal information to be anonymous before it is no longer protected by the Act. This proposal effectively means that de-identified information could become subject to the legislation.

We note that the AGD suggests that this proposal "would not impose an absolute or unworkably high standard on APP entities that use data for research or service delivery".[14] However, members

[13] OAIC, Australian Privacy Principles Guidelines, Chapter B: Key Concepts (July 2019), p. 20.

[14] AGD Discussion Paper, p. 31.

suggest that a goal to achieve complete anonymisation of consumer data is not possible in practice. For instance, the uniqueness of every individual would not preclude an individual ultimately being re-identified if other datasets (from other sources) were combined, not to mention the impact of technological advances that could enable re-identification. This issue will be further compounded if the definition of personal information were to be broadened, leading to a greater compliance burden for managing such information and inhibiting innovation. A significant investment will be required from businesses to ensure that the risk of de-identification remains unrealised.

If there were to be a delineation between de-identified and anonymised personal information, as proposed in the Discussion Paper, this also raises the question as to whether there should be a distinction made with pseudonymisation. Pseudonymisation is another safeguard for protecting personal information that we discussed in our previous submission in relation to issues associated with the AGD's proposal for a right to erasure or be forgotten.

We suggest that further assessment is needed for the practical considerations that such a proposal would introduce. We welcome further consultation for the technical standards if the Government wishes to proceed with this proposal.

4. Notice of collection, use and disclosure of personal information

4.1 Reducing matters to be notified under APP 5.2

Proposal 8.2 of the Discussion Paper proposes that APP 5 notices be limited to the following matters under APP 5.2:

- *the identity and contact details of the entity collecting the personal information;*
- *the types of personal information collected;*
- *the purpose(s) for which the entity is collecting and may use or disclose the personal information;*
- *the types of third parties to whom the entity may disclose the personal information;*
- *if the collection occurred via a third party, the entity from which the personal information was received and the circumstances of that collection;*
- *the fact that the individual may complain or lodge a privacy request (access, correction, objection or erasure); and*
- *the location of the entity's privacy policy which sets out further information.*

In principle, we support the policy objective of providing consumers with transparency to better inform them regarding their privacy. Such an objective should avoid creating consent and notice fatigue on consumers. We would also support this proposal if it were to deliver such an objective, while providing entities with sufficient flexibility, simplicity and reduced burden and costs, especially those with complex operations. This could be achieved in part by limiting the amount of information provided to consumers under this proposal. However, this could be complicated if the definition of personal information were to be broadened under the proposals in the Discussion Paper, as discussed above. A proper assessment, including a cost benefit assessment, will also need to be undertaken.

We previously raised the issue of complexities and information overload for consumers associated with proposed notification obligations. For example, this could arise as a result of notifications from multiple APP and third party entities, which could be burdensome for the notifying entity as well as

providing limited value for affected individuals. Matters listed under Proposal 8.2 need to avoid creating such a scenario. For example, the items referring to third parties (fourth and fifth items) may need to be reviewed including on whether they should be removed if they do not offer any material consumer benefit. Similarly, if the purpose of personal information to be collected, used or disclosed is reasonably expected by the consumer, it may also provide no material benefit for them to be notified of such information.

In addition, standardised collection notices and templates under Proposal 8.3 may be difficult to implement for some entities and may not offer material benefit to consumers if they already have templates which are compliant.

Finally, further consideration should also be given to the practical value in treating the use of hyperlinks (as suggested in the Discussion Paper) as a potentially legitimate way for entities to provide individuals with sufficient notice to an entity's privacy policy including APP 5.[15]

4.2 Strengthening requirement for APP 5 notice

Proposal 8.4 in the Discussion Paper proposes to strengthen the requirement for when an APP 5 collection notice is required – that is, require notification at or before the time of collection, or if that is not practicable as soon as possible after collection, unless:

- the individual has already been made aware of the APP 5 matters; or
- notification would be *impossible* or would involve *disproportionate effort*.

For the sake of strengthening the requirement for notifications, we would be concerned if consumers were overloaded with information, such as a consequence of a cumulative increase in notifications (albeit reduced in matters under Proposal 8.2) from APP entities (including third parties). And if there were limited benefits to consumers in introducing such a new notification requirement, it would be inappropriate to create a new unreasonable regulatory burden on businesses. Therefore, regard needs to be given as to whether such a proposal will reduce information overload for consumers and be of material benefit to them. Associated with this, sufficient guidance will also be needed to clarify the meaning of "disproportionate effort", which should include a cost benefit assessment.

Setting aside this concern, we note that the exceptions under this Proposal appear to be limited and it may be worth expanding these to take into account other reasonable exceptions. For example, "lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety" is commonly referred to as a permitted general situation in several APPs that may warrant further consideration.[16]

5. Consent of collection, use and disclosure of personal information

In addition to matters that we have previously discussed regarding consent of collection, use and disclosure of personal information, we would be concerned if consent requirements were to be expanded or introduced without proper assessment of the problem, as well as material consumer benefit and cost impact on entities.

For instance, it is important to ensure that consent fatigue be avoided in a similar manner that it should be avoided through privacy notification fatigue. There may also be benefit in considering whether transparency measures such as through privacy disclosures and user empowerment can provide consumer benefit without creating unnecessary new regulatory obligations. There should

[15] AGD Discussion Paper, p. 69.

[16] Section 16A of Privacy Act.

also be an appreciation of the diversity of ways in which consent can be reasonably provided without needing to be overly prescriptive.

6. Direct marketing, targeted advertising and profiling

6.1 Definition of direct marketing

The Discussion Paper refers to OAIC guidance for the definition of "direct marketing", which "involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services".[17]

In contrast, Proposal 16.2 in the Discussion Paper applies a different definition for "direct marketing": "The use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions must be a primary purpose notified to the individual when their personal information is collected". Associated with this, Proposal 10.4 proposes to: define a "primary purpose" as the purpose for the original collection, as notified to the individual; and define a "secondary purpose" as a purpose that is directly related to, and reasonably necessary to support the primary purpose. This expansion of the definition of "direct marketing" will have far reaching implications and lead to notification fatigue for individuals. If this proposal were to be adopted alongside Proposal 11.1, which concerns prohibited acts and practices, businesses will be less inclined to invest in innovative services that benefit customers through providing timely and targeted information (e.g. through location data).

Where entities must provide notices to individuals of the use or disclosure of personal information for the purpose of influencing their behaviour or decision as a primary purpose, additional risks emerge when coupled with Proposal 8.1, which provides that notices must be clear, current and understandable. Without further direction as to a reading comprehension threshold, businesses are at risk of failing to cater to a wide range of Australians. Further, providing concise explanations of technically complex information exposes regulated entities to risk. Guidance from the OAIC would greatly benefit businesses, or the inclusion of a legislative safe harbour would also address this risk.

Taken together, Proposal 16.2 effectively departs from the meaning of "direct marketing" provided in OAIC guidance and broadens its scope, which can lead to unintended consequences for entities. We therefore suggest applying a consistent definition, as provided by the OAIC.

6.2 Right to object to collection, use or disclosure for direct marketing

Proposal 16.1 in the Discussion Paper proposes that:

> *The right to object … would include an unqualified right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing. An individual could still request not to receive direct marketing communications from an organisation. If an organisation provides marketing materials to an individual, it must notify the individual of their right to object in relation to each marketing product provided.*
>
> *On receiving notice of an objection, an entity must stop collecting, using or disclosing the individual's personal information for the purpose of direct marketing and must inform the individual of the consequences of the objection.*

We appreciate the intention behind the proposal is aimed to ultimately assist individuals in enhancing their awareness and understanding about the use of information for direct marketing. However, the proposal does not contemplate that such information is collected for other various legitimate reasons that would also be in the individual's interest. For instance, consumers could

[17] AGD Discussion Paper, p. 124.

reasonably expect information to be collected to enable better customer service, improve products or services, communication of targeted non-marketing information such as invoices, and protect against fraud. In this regard, loyalty schemes should benefit from being considered for exemption as an example. Such applications are not always completely known at the time of collection, which could evolve over time to meet consumer expectations.

If consumer benefit is the main objective, then allowing consumers the ability to opt-out of receiving direct marketing could be a better alternative to be considered further, as opposed to automatically adopting Proposal 16.1 and Proposal 10.4 more broadly. However, a global opt out of direct marketing with a single click mechanism as in Proposal 12.1 for example may not meet the needs of consumers and create confusion. An example of this would be a business with multiple products and services, and the consumer opts out of all direct marketing when the consumer would still like to receive offers on certain products and services. Even where a consumer may opt out of receiving direct marketing, ads may still be shown indirectly via other platforms. This could lead to blow-back on businesses even where opt outs are offered to consumers.

Careful consideration should be given to any opt out settings so that consumers and businesses can continue to benefit.

7. Automated decision-making

Proposal 17.1 in the Discussion Paper proposes that privacy policies be required to include information on whether personal information will be used in automated decision-making (ADM) which has a legal, or similarly significant effect on people's rights.

Should this proposal proceed further, clarification will be needed:

- Regarding the threshold of "legal, or similarly significant effect". The risk of non-compliance by entities due to unclear criterion should be addressed, particularly where entities will utilise artificial intelligence (AI) to support decision making in the realm of employment and recruitment.

- To ensure that both business and individuals understand the scope of information included. For instance, the language in Proposal 17.1 should be clarified and there is merit in considering that it applies only in those instances where personal information is inputted into ADM and that it does not apply more generally e.g. the use of anonymised information derived from personal information.

We note that the Discussion Paper particularly notes the use of AI for implementing ADM and also cites the AHRC's report on Home Rights and Technology, which included a number of recommendations on how Australia should regulate AI and other emerging technologies that can be used to make automated decisions.[18]

Overall, we agree that privacy is a relevant consideration in a discussion about AI and other emerging technologies, such as in Proposal 17.1. However, there are a range of dimensions and activities related to AI, not limited to privacy and human rights. We appreciate diversity of perspectives that need to be properly captured and would be concerned about the potential for fragmented and conflicting regulation or legislation that could arise in absence of proper coordination between multiple bodies on this subject. There would be benefit if privacy and other matters associated with AI were considered as part of coordinated discussion between the various Federal departments, agencies, authorities and stakeholders around policy issues that arise from new and emerging technologies such as AI. This will help to ensure that government's potential role in promoting AI

[18] AGD Discussion Paper, p. 137.

investment and uptake is not inadvertently stifled by other government activities that may inhibit it. This valuable coordinating role would also ensure consistent policy, efficient use of stakeholder resources, and helping to connect industry capability.

These are matters that we have previously raised in various submissions including to the AHRC and Department of Industry, Science, Energy and Resources (DISER).[19] Subsequent to this, we note that the Government released its AI Action Plan, and more recent Critical Technologies Blueprint and Action Plan. These and other government activities are also more broadly relevant to our point in this submission regarding the need for better coordination across Federal departments, agencies and authorities around interrelated reforms.

8. Controllers and processors of personal information

While not currently a proposal, the Discussion Paper discusses the concepts of data controllers and data processors. According to the Discussion Paper, there may be benefits in introducing such a concept in Australia, where it could clarify entities' accountability such as with the NDB Scheme, and align with international data protection and privacy regimes. However, the Discussion Paper also notes that there may be challenges in its implementation such as how it might apply to small businesses with an annual turnover of less than $3 million (which is in contrast to how these concepts have been adopted overseas).

As a general comment, to the extent that the Privacy Act review can assist with the facilitation of effective and efficient cross-border disclosure, this may be valuable for certain large entities, particularly given the nature of many of their services which require transfer of data. This is also important in terms of enabling regulatory coherence.

While we have noted caution needs to be given regarding a proposed adoption of the EU GDPR (discussed earlier in this submission), there may be benefit in reviewing further and consulting on the concept of data controllers and data processors, including a cost benefit assessment and whether they are appropriate in the Australian context. A RIS would be of assistance in this regard.

9. NDB Scheme

In our previous submission, we shared our views regarding the NDB Scheme since its commencement in February 2018.[20] Subsequent to this consultation, we provided updated views regarding the Scheme to Home Affairs in response to Home Affairs' Discussion Paper on Strengthening Australia's Cyber Security Regulations and Incentives.[21]

Overall, while the Scheme may have been a useful source for analysing reasons for data breaches, more can be done to assist businesses in mitigating them from occurring in the first place.

[19] Ai Group submission to DISER (1 December 2020), https://www.aigroup.com.au/globalassets/news/submissions/2020/diser_ai_action_plan_dec2020.pdf; Ai Group submission to AHRC (26 March 2020), https://www.aigroup.com.au/globalassets/news/submissions/2020/ahrc_human_rights_and_technology_discussion_paper_26mar_2020.pdf.

[20] Ai Group submission to AGD (November 2020), pp. 25-30.

[21] Ai Group submission to Home Affairs (September 2021), pp. 16-21, https://www.aigroup.com.au/news/submissions/2021/home-affairs-discussion-paper-on-strengthening-australias-cyber-security-regulations--incentives/.

Of particular interest to the AGD's consultation, the NDB Scheme has highlighted a number of issues which we believe requires Government actions or assistance and we recommend the following:

- Address the source of malicious or criminal attacks that lead to data breaches
- Publish more frequent OAIC NDB Scheme insights reports (e.g. annually) that may help to better inform policymakers with respect to privacy and cyber security policy.
- Fund businesses with transition support to meet regulatory obligations associated with cyber security including NDB Scheme.[22]
- Develop policy options to assist businesses to mitigate data breaches from occurring in the first instance, including awareness and effective responses. This could entail further collaboration between industry and governments to co-design workable and practical remedies to increase cyber security capability, such as technological solutions and education and training programs.
- Proper coordination between Government agencies to assist business victims of data breaches and cyber security incidents.
- Ensure the ACSC is sufficiently resourced to meet the cyber security demands of industry and the community.
- Undertake a public health approach through specific awareness campaigns targeted at industries that most often appear in the NDB Scheme reports.

10. Interactions with other schemes

In our previous submission to the AGD, we noted the various government consultations and initiatives that are relevant for consideration in relation to this review. Complexity of parallel and overlapping reform initiatives continues to be a problem and in fact appears to be increasing. In our most recent submission to the AGD on its OP Bill, we raised this issue again, noting further issues that have since arisen and wish to reiterate these points for the purposes of this consultation.

In addition to the Privacy Act Review, there are a range of other reforms, legislations and regulations that Government needs to be mindful of and avoid potential scope creep, overlap and duplication. And there is a larger impact on affected stakeholders that the RIS for the OP Bill may not fully appreciate, which is the cumulative impact of multiple forms of regulation in relation to online activities.

Without properly considering these other reforms more holistically, there will likely be similar problems as running concurrent privacy reforms as discussed above. It would also be an administratively inefficient outcome and inappropriate use of public resources if there were to be overlapping regulations and therefore overlapping responsibilities between regulators. Such complexities in overlapping regimes will also more likely lead to inadvertent non-compliance and confusion for consumers seeking to exercise their rights.

Given the interactions between these areas of reform, we also recommend that consideration be given to improved coordination within Government on these matters. It also raises the broader

[22] For example, this could include providing cyber security uplift such as education and training, compliance assessment, cyber security assessment, and cyber security investment. Such a cyber security support scheme could offer a range of security services and capabilities that can be accessed by businesses at a subsidised cost (i.e. either no or minimal cost).

question of how these fit under the Government's various strategies including the Digital Economy Strategy, Australian Data Strategy and Cyber Security Strategy.

We therefore recommend that:

- Government should give proper consideration to the interrelated reforms, legislations and regulations relevant to this consultation, and their impact on businesses including uncertainties that may be introduced, chilling investment and innovation.

- Government should improve coordination between government agencies and departments with respect to this consultation and other interrelated reforms, legislations and regulations.

10.1 Online Privacy Bill

The AGD has acknowledged that there are interactions between its OP Bill and the Privacy Act Review. However, the AGD has suggested that the OP Bill "addresses the pressing privacy challenges posed by social media and other online platforms", while the Privacy Act Review "seeks to build on the outcomes of the OP Bill to ensure that Australia's privacy law framework empowers consumers, protects their data and best serves the whole of the Australian economy".[23]

However, we consider that the issues raised and solutions proposed in the OP Bill are intertwined with the wider Privacy Act Review. We are concerned if the Online Privacy Code (OP Code, arising from the OP Bill) were to be developed ahead of completion of the Privacy Act Review, without proper consideration of the practical challenges and other options including amending the Bill.

We strongly encourage the AGD to refer to our submission on its OP Bill, which goes into comprehensive detail regarding the overlap between its OP Bill and the Privacy Act Review, including practical challenges with the concurrent consultations and recommendations.

Below is a summary of our issues and recommendations in response to the OP Bill.

Issues	**Recommendations**
1. Problem and rationale for regulation	• A more detailed analysis of the problem statement should occur before proceeding with the OP Bill. The Privacy Act Review provides the perfect platform for this.
2. Interactions with Privacy Act Review	• The Privacy Act Review should take precedence over the OP Bill to ensure proper analysis, assessment and consultation of the issues and underlying causes (if any), as well as options to address these. • Sufficient time and consultation stages need to be allocated for providing proper stakeholder consultation on the AGD's concurrent privacy reform consultations, including the proposed approach for development of the OP Code. • If it were not possible to pause the OP Bill to allow for the Privacy Act Review to take precedence, the scope of the OP Bill should be limited to those aspects requiring Government's critical attention and subject to further consultation.
3. Interactions with other interrelated reforms	• Government should give proper consideration to the interrelated reforms, legislations and regulations relevant to this consultation, and their impact on businesses including uncertainties that may be introduced, chilling investment and innovation.

[23] See: https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/.

Issues	Recommendations
	• Government should improve coordination between government agencies and departments with respect to this consultation and other interrelated reforms, legislations and regulations. • Government should review the interactions between the CDR and Privacy Act more broadly with the objective of reducing regulatory duplication and red tape. • Government should explore other options to enable sharing of information between the OAIC and eSafety Commissioner to avoid regulatory duplication and overlap. • An alternative option could include establishing a central regulatory body (such as under the PM&C) for coordinating between the various regulators with respect to online activities.[24]
4. Overly broad and disproportionality in scope of targeted businesses	• Subject to properly assessing the issues and underlying causes, Government should further clarify the businesses that it intends to target under the OP Bill. • Based on clearly defined targeted businesses under the OP Bill, Government should undertake a proper assessment of the impact on targeted businesses including cost-benefit assessment and other relevant implementation considerations (e.g. compliance time and assistance).
5. Lack of consideration of other options and solutions	• Government should explore other options to the OP Bill and these should be considered as part of the Privacy Act Review, including: ○ Providing sufficient resources to the OAIC funded by Government in the first instance; ○ Reviewing the effectiveness of the APPs; and ○ Providing businesses with transition assistance such as an industry engagement plan for enabling business privacy capability uplift, Government funding to support business uplift, and providing industry with a reasonable timeframe to meet any new compliance requirements.

10.2 Consumer Data Right

In our submission to Treasury on its Consumer Data Right (CDR) Strategic Assessment Consultation Paper, we suggested that it would be prudent for Treasury to consider integrating or aligning its CDR Review with the Privacy Act Review, especially as there are interrelated privacy and data protection regulation considerations.[25] This would benefit consumers and industry by ensuring a more integrated approach – as opposed to creating multiple and overlapping privacy regimes.

In this regard, we welcome the AGD's consideration of the potential overlap between the OP Code (as proposed in the OP Bill) and the CDR regime, with the AGD having consulted with other Government Departments on these reforms, according to the RIS.[26]

However, we would like to see more integration and coordination between Treasury and the AGD to ensure there is proper alignment of activities associated with the CDR and Privacy Act more generally. For example, as we previously raised with Treasury and the AGD, the CDR has effectively created a dual privacy regime with regulatory oversight of the CDR Privacy Safeguards by the ACCC

[24] The UK Centre for Data Ethics and Innovation is an example of a coordinating central body, https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation/about.

[25] Ai Group submission to Treasury (September 2021), https://www.aigroup.com.au/news/submissions/2021/treasury-consultation-paper--strategic-assessment-on-implementation-of-an-economy-wide-consumer-data-right/.

[26] AGD RIS for the OP Bill (October 2021), p. 25.

and OAIC for sectors subject to the CDR. Such an outcome creates complexity and compliance costs for businesses that have to comply with both regimes, and also for small businesses that may not currently be subject to the Privacy Act and therefore not familiar with privacy regulatory regimes. Here, there would be benefit in reducing regulatory duplication and associated red tape.

We therefore recommend that Government should review the interactions between the CDR and Privacy Act more broadly with the objective of reducing regulatory duplication and red tape.

10.3 Landscape of regulatory processes relating to online activities

We note that there are several concurrent regulatory processes initiated by government agencies and departments with a focus on online activities where these processes appear to be targeting so-called digital or online platforms. However, as noted earlier, many businesses have the capability of having an online business or platform, with online services delivered via various digital media (e.g. websites, social media, apps and other digital or online platforms) which are B2C or B2B in nature, and affect businesses of all sizes. In fact, there are only low barriers to an online presence and it is common for even small businesses today to have any online presence.

For example, in addition to the proposed OP Code:

- The eSafety Commissioner is currently overseeing industry codes being developed under the *Online Safety Act 2021* (Cth);[27]
- The eSafety Commissioner is also consulting with industry on a roadmap for the introduction of mandatory age verification and the Restricted Access Systems Declaration;[28]
- The Department of Infrastructure, Transport, Regional Development and Communications is currently consulting on the Basic Online Safety Expectations;[29]
- Home Affairs has put forward a proposal for a new cyber security code under the Privacy Act as part of its Strengthening Australia's Cyber Security Regulations and Incentives Discussion Paper;[30] and
- Most recently, the AGD has initiated consultation on its Exposure Draft of the Social Media (Anti-Trolling) Bill 2021.[31]

These concurrent activities suggest a lack of coordination across Federal departments, agencies and authorities, and a lack of appreciation by at least some of them of the potential negative cumulative impact that this could have for a wide range of businesses, not just for large technology companies.

To reiterate, there would be a greater benefit if there could be better coordination between Federal departments, agencies and authorities in relation to multiple industry codes and regulations relating to online activities that are becoming an overcrowded landscape of regulation for a wider range of businesses.

---

[27] See: https://www.esafety.gov.au/about-us/consultation-cooperation/industry-codes-position-paper.

[28] See: https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification; https://www.esafety.gov.au/about-us/consultation-cooperation/restricted-access-system.

[29] See: https://www.infrastructure.gov.au/have-your-say/draft-online-safety-basic-online-safety-expectations-determination-2021-consultation.

[30] Ai Group submission to Home Affairs (August 2021), https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australias-cyber-security-submissions/australian-industry-group.pdf.

[31] See: https://www.ag.gov.au/legal-system/publications/exposure-draft-social-media-anti-trolling-bill-2021.

10.4 Overlapping regulatory bodies and functions

In addition to concurrent interrelated government activities with respect to the online domain, there is a consequential risk of overlapping regulatory bodies and functions in regulating this area.

An option that has been put forward in the OP Bill is to empower the eSafety Commissioner to be an alternative complaints body to the OAIC. The rationale provided in the Explanatory Paper is to "allow information sharing to occur in the event of overlap between privacy complaints and complaints to the eSafety Commissioner – such as cyberbullying, cyber abuse and image-based abuse complaints".[32]

Another example of overlap with questionable public benefit relates to the section 52A(1)(c) of the Bill, whereby the Commissioner can require the publication or communication of a statement in those cases where there has been an interference with the privacy of an individual. This overlaps with the NDB Scheme and may cause information that is harmful to the relevant entity to be published e.g. notification of weaknesses in systems may be exploited by malicious actors if made public.

In principle, we support administrative efficiency that enables information sharing between government bodies (subject to appropriate regulatory safeguards) and reduces regulatory red tape for businesses. However, we would be concerned if the eSafety Commissioner were to be given powers that extended beyond its remit of promoting online safety and duplicating the regulatory responsibilities and functions of the OAIC with respect to privacy related matters. There should be other options explored, without necessarily expanding the eSafety Commissioner's powers that could risk creating regulatory uncertainty, overreach and duplication. It should be made clear that the eSafety Commissioner will only deal with online safety matters and the OAIC deal with privacy matters.

For instance, where privacy related complaints are determined by one regulator, the complainant should not be able to make the same or similar complaint to another regulator. This protects against regulatory double dipping and forum shopping. Anecdotal feedback from an industry member indicates that they have experienced this problem with two regulators (namely, the Telecommunications Industry Ombudsman (TIO) and OAIC). This can arise where a complainant is unhappy with a TIO decision regarding their complaint so they subsequently file that same complaint with the OAIC.

Further exploration of other options through proper stakeholder consultation could include assessing the merits of establishing a central regulatory body (under a central government department such as the Department of the Prime Minister and Cabinet (PM&C)) that can properly coordinate between the various regulators responsible for developing codes and regulations. This could enable a more holistic consideration including understanding the cumulative regulatory impacts and costs on affected stakeholders who may be subject to multiple regulations related to online activities. The PM&C also plays an important role, providing oversight of the Digital Economy Strategy, Australian Data Strategy and most recently Critical Technologies Blueprint and Action Plan, so this coordinating approach could be another advantage.

We therefore recommend that:

- Government should explore other options to enable sharing of information between the OAIC and eSafety Commissioner to avoid regulatory duplication and overlap.

[32] AGD Explanatory Paper for the OP Bill (October 2021), p. 22.

- An alternative option could include establishing a central regulatory body (such as under the PM&C) for coordinating between the various regulators with respect to online activities.

- Privacy complaints should be handled by one regulator, with the OAIC a likely choice given its privacy expertise.

11. Enforcement and regulation

In our submission to the AGD on its OP Bill, we commented on its proposals to strengthen regulatory enforcement powers and penalties that we consider also pertinent to the review of the Privacy Act.

Setting aside our issues with the OP Bill, we were also concerned regarding the lack of options presented in the RIS for that Bill to demonstrate that the solution offered (including the introduction of an OP Code) was the most appropriate response. This was acknowledged in the RIS where only one option had been put forward, indicating that it was to meet Government's commitment to strengthen the Privacy Act by introducing reforms to amend the Act, centred around introducing a binding OP Code and strengthening enforcement measures and penalties.[33]

We consider that good policy and regulatory practice should entail a proper consideration of various options once the problem has been properly assessed, rather than immediately leaping to one solution. This is more reason why the Privacy Act Review should take precedence over the OP Bill and properly consulted upon.

11.1 Providing sufficient resources for the regulator

We are cautious with proposals to strengthen regulatory enforcement powers and penalties without a proper assessment of whether the regulator (in this case, OAIC) has the sufficient resources funded by Government to execute its functions. For instance, there may be adequate regulations in place, but the regulator may have insufficient resources. If the regulator were to be provided with sufficient resources that contributed to addressing an identified issue, then this suggests that the regulations in place are sufficient. We suggest this would be a more prudent step rather than immediately resorting to legislative reforms associated with enforcement (such as the ones proposed in the Discussion Paper) in the first instance.

11.2 Providing business transition assistance

While the OP Bill heavily focused on traditional regulatory approaches such as amending legislation, creating new regulations, and increasing enforcement powers and penalties, there lacked alternative solutions that may be more productivity enhancing and effective. For example, there is an important role that the Government or OAIC can provide through developing business uplift with respect to privacy.

Consider the NDB Scheme under the Privacy Act as an example. While the OAIC produces half-yearly reports about the Scheme, it would be useful for the OAIC to develop with industry more proactive initiatives to help mitigate such breaches occurring in the first place, as noted earlier. The introduction of the mandatory NDB Scheme left many businesses stranded with a compliance mindset as opposed to providing them with adequate uplift support – this is likely to be an even more significant issue for SMEs. While the RIS for the OP Bill briefly mentioned about how businesses may benefit from improved OAIC education material and programs based on the OAIC's increased ability to understand emerging systemic privacy issues, it would be useful to see an industry engagement plan developed that clearly spelt out meaningful actions (including resourcing, scheduled initiatives and collaboration with key stakeholders) and measures of success. This could

[33] AGD RIS for the OP Bill (October 2021), p. 13.

be co-designed with industry to develop a genuinely effective and mutual outcome that benefits the Australian community. Again, this is an example of a matter that should be considered as part of the broader Privacy Act Review.

If it were decided to proceed with an amendment to the legislation that could lead to some form of OP Code for example, it will be important that companies are provided with proper transition support from Government to meet these new compliance requirements. This will be especially important for companies that are not traditionally subject to these types of online activity reforms. These companies will need as much assistance as possible to ensure that they are properly accounted for. This includes Government funding and being provided a reasonable timeframe to meet any new compliance requirements. It is important to note that this is not necessarily about providing funding support for large technology businesses, but about SMEs and wider industry that may be captured under these requirements with practical uplift support. Related to this, relevant industry associations that might be required to develop industry codes should be properly identified, consulted with and appropriately supported by Government (including funding and resources) to undertake such activities.

12. Small business exemption

The small business exemption in the Privacy Act remains a necessary part of the regulatory system and should be neither removed nor narrowed. The exemption serves a necessary purpose in ensuring businesses are not overly burdened by the compliance measures necessary to satisfy the APPs.

Small businesses would benefit from being provided with assistance in terms of "best practice" in safeguarding personal information. However, the Australian Government should not impose strict requirements which small businesses may struggle to implement.

The *Privacy Amendment (Private Sector) Act 2000* (Cth) which extended coverage of the Privacy Act to some parts of the private sector included the limited exemption for small businesses from application of the APPs. The rationale for the inclusion of the exemption is clear from the explanatory memorandum which provided (emphasis added):[34]

> *All small businesses will be exempt from the operation of the legislation for a period of 12 months after the commencement of the legislation. This delayed application is designed to allow small business extra time to ensure compliance with the legislation. After the initial period it is intended that small business be exempt from the legislation unless there is a privacy risk.* ***This is in accordance with Government policy to minimise compliance costs for small business****.*

It was recognised by the drafters of the legislation that the compliance costs for small businesses would likely be exorbitant. This is also reflected in the second reading speech by the then Attorney-General in favour of the Bill:

> *Similarly, while protecting privacy is an important goal****, it must be balanced against the need to avoid unnecessary costs on small business****. For this reason, only small businesses that pose a high risk to privacy will be required to comply with the legislation.*
>
> *Small business is defined in the legislation as a business with an annual turnover of $3 million or less. Such businesses will be exempt unless they hold personal health information and provide a health service, trade in personal information, are a Commonwealth contracted service provider or are prescribed by regulation.*

[34] Explanatory Memorandum, *Privacy Amendment (Private Sector) Bill 2000*, p. 5.

The power to prescribe small businesses, or particular acts or practices of small businesses, provides a flexible way to ensure that other risks to privacy can be brought within the legislation where that is necessary and in the public interest. In considering whether the circumstances justify bringing small businesses within the regulatory scheme, the Privacy Commissioner must be consulted. I also intend to consult with the minister for small business before making a decision on such a regulation.

In addition, small businesses will not be subject to the legislation for a period of 12 months after it comes into force. The government appreciates that small business needs to focus on implementing the new tax system. The extra time given to small business will provide ample opportunity for them to implement the changes to the tax system before turning to how they will handle personal information.

Even so, with the increasing demands from consumers and larger business partners for greater respect for privacy, more small businesses are recognising that good privacy practices are good business practices. The bill provides an excellent foundation for Australian small businesses to take the initiative voluntarily in relation to privacy. This will allow them to capitalise on the increased consumer and business confidence that results from proper practices.

The concerns expressed by the Attorney-General continue to be relevant today. Smaller businesses lack dedicated staff with an in-depth knowledge of privacy law to assist in ensuring full compliance with the APPs. For "micro-businesses", the burden of understanding and executing obligations under the Privacy Act would be substantial. With the continued COVID-19 pandemic, smaller businesses have been required to devote significant resources to ensuring State and Federal regulations, aimed at controlling the spread of the virus, are complied with. The last few years have been particularly burdensome for businesses confronted with a patchwork of mandatory control measures which have impacted their operations.

Small businesses currently in the grip of significant difficulties brought on by the current pandemic should not be subject to increased layers of regulation. More benefit is likely to result from encouraging businesses to pursue best practice outcomes in their dealings with personal information. Educative programs are a preferable strategy to encourage best practice information collection and handling.

13. Employee records exemption

For the reasons outlined in section 5 of Ai Group's November 2020 submission, we oppose any proposed narrowing of the employee records exemption. Handling of employee records is best dealt with under current workplace legislation and employers should not be subject to multiple layers of regulation pertaining to the same subject matter.

Any watering down of the employee records exemption in the Privacy Act is likely to cause significant confusion regarding the interaction with existing controls in workplace legislation and will potentially put employers at risk of contravening the Privacy Act in the ordinary course of administering the employment relationship. The ongoing pandemic has demonstrated to employers the need to procure information from workers in the form of taking temperatures or ascertaining vaccination status in order to mitigate the risk of spreading the virus. Additional restrictions pertaining to dealing with such information will further impede employers in taking such reasonable management action.

Rather than being narrowed, as proposed in our November 2020 submission there is a need to ensure that the employee records exemption is extended to cover host employers engaging in labour hire arrangements. Such businesses are not covered by the exemption and, as a result, encounter significant difficulties in dealing with personal information which is necessary to undertake reasonable management action. Host employers often need to procure health information regarding

workers to properly undertake COVID-19 containment measures. The employee records exemption needs to be extended to ensure that labour hire operations are not obstructed by the inability of host employers to deal efficiently with records pertaining to staff that are not directly engaged.

The imposition of a "fair and reasonable" test would not assist employers in retaining current administrative flexibilities regarding the treatment of employee records. The term "fair and reasonable" in the context of employee records is untested and its inclusion would encourage litigation to determine its parameters. Although a concept of fairness is currently contained in APP 3.5, any existing guidance on this term would likely be of limited assistance with respect to employment records given the unique nature of the employment relationship. Employers will be unable to efficiently discharge their obligations to their employees without retaining existing flexibilities regarding usage of personal information regarding their staff.

As outlined in our November 2020 submission, the Decision of the Full Bench of the Fair Work Commission in *Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946 exposed a significant shortcoming in the existing exemption in that it did not apply to records before they were held by the employer. The Decision highlighted that the employee records exemption is excessively narrow in that it restricts employers from directing their employees to provide essential information which may be necessary to implement appropriate COVID-19 protections. Ai Group urges the Australian Government to address this gap in the exemption to ensure that employers are able to request that their staff submit to temperature checks and provide vaccination status without requiring consent.

Modification of APPs 12 and 13 to provide a limited right to access or correct employee records is unnecessary and potentially opens a conflict with regulations 3.42, 3.43 and 3.44 of the Fair Work Regulations which already impose obligations upon employers and former employers regarding disclosure and accuracy of employee records. Significant penalties apply for breaching these regulations. The confusion and detriment which would arise from narrowing or removing the employee records exemption would not be ameliorated by providing a limited restriction on the application of APPs 12 and 13. Such modifications would merely overlap with existing regulation and open the way to litigation over the extent of the rights under APPs 12 and 13 in the employment context.

Introducing an additional requirement to take reasonable steps to protect employees' personal information from misuse, interference or loss would unhelpfully cover the same ground as existing requirements under reg 3.44 of the Fair Work Regulations which restricts alteration of employee records and imposes a positive obligation upon employers to ensure that certain employee records are not altered by another person except where provided for under the Regulations or the *Fair Work Act 2009* (Cth) (FW Act). Regulation 3.44(6) also prohibits a person making use of an entry in an employee record if the person does so knowing that the entry is false or misleading. Additional obligations imposed upon employers under the Privacy Act are unnecessary given the existing protections in the FW Regulations.

Any productive debate concerning the privacy obligations in place to protect employee records need to take place within the confines of workplace relations legislation which comprehensively deals with this area. Investigation and enforcement of breaches of existing record requirements are already dealt with within the framework of the FW Act. It is not appropriate for duplication to occur by removing or narrowing the employee records exemption.

14. Direct right of action

In Ai Group's November 2020 submission to the Inquiry, we opposed the introduction of a direct right of action for individual claimants and for groups instituting representative proceedings. The model proposed in recommendation 25.1 of the Discussion Paper does not constitute an appropriate regulatory response to the issues surrounding enforcement of the Privacy Act. The existing enforcement options available under the Privacy Act remain fit for purpose. Any perceived

deficiencies in the current enforcement framework should be addressed by ensuring adequate resources are available to the OAIC. Given the ongoing reform efforts by the Federal Government to regulate the class action industry, caution is needed before expanding the class action system to encompass proceeding instituted by groups under the Privacy Act.

The OAIC is well placed to evaluate contraventions of privacy legislation and take appropriate action on behalf of persons impacted by a potential breach. Any asserted deficiencies in the present enforcement framework should be addressed within the parameters currently set by the Privacy Act with the OAIC as the entity responsible for initiating such action.

Complaints and investigations relating to interferences with an individual's privacy are appropriately dealt with under Part V of the Privacy Act. Complaints may be brought to the Information Commissioner or an investigation conducted on the Commissioner's own motion. The Commissioner may take action that includes conducting a hearing or conference or making a determination which is enforceable in the Federal Court or Federal Circuit Court. The Commissioner's powers are broad and encompass a capacity to accept an enforceable undertaking or seek an injunction to prevent further breaches of the Privacy Act.

The OAIC has demonstrated capability to deal with the quantity of matters to which it is referred. In its Annual Report for the 2020/21 reporting period, the OAIC reported that it had made 17 privacy determinations, more than in any previous year. It also resolved 94% of privacy complaints within a 12-month period (more than the previous reporting period). The OAIC's most recent annual report demonstrates that 93% of privacy complaints are closed through early resolution and conciliation. The report notes that during the 2020/21 reporting period, the OAIC "introduced process improvements which resulted in reduced handling times for complaints referred for further investigation, including faster up-front assessments, streamlined investigation processes, and an increased focus on early resolution and conciliation". The Australian Government should not divert complaints away from the OAIC and toward the Court system. Regulatory responses to challenges in relation to privacy should centre on appropriate resourcing and empowerment of the OAIC.

The proposed model is not an appropriate reform in that it would enable representative proceedings to be initiated under the Privacy Act. Class action proceedings are currently beset by numerous failings which encourage speculative litigation and inflate legal costs at the expense of defendants and class members. In Ai Group's November 2020 submission, we outlined the regulatory challenges which were being examined as part of the Parliamentary Joint Committee on Corporations and Financial Services' Inquiry into litigation funding and the regulation of the class action industry. Since that submission was filed, the Committee has tabled its report which concluded that recent case law suggests that the present regulation of the class action industry is inadequate.[35] The report said:[36]

> *The growth in the scale of litigation funding, the participation of international litigation funders in the Australian market, and the frequency of windfall profits, highlights the need to reassess whether representative plaintiffs, class members and defendants are achieving reasonable, proportionate and fair outcomes.*

The Committee identified a number of areas where it saw significant value in reforming the current class action regime. In seeking to address some of those areas, the Treasury released an exposure draft of the *Treasury Laws Amendment (Measures for Consultation) Bill 2021: Litigation funders*. A consultation process in relation to that Bill took place from 30 September 2021 to 6 October 2021. The Bill formed the framework for the *Corporations Amendment (Improving Outcomes for Litigation*

[35] Parliamentary Joint Committee on Corporations and Financial Services, "Litigation funding and the regulation of the class action industry" (Report, 21 December 2020), p. xv.

[36] Parliamentary Joint Committee on Corporations and Financial Services, "Litigation funding and the regulation of the class action industry" (Report, 21 December 2020), p. xv.

Funding Participants) Bill 2021 (Litigation Funding Bill) which was also subject to a Parliamentary Joint Committee Inquiry and remains before Parliament. The Litigation Funding Bill imposes express obligations regarding the constitution of class action litigation funding schemes and sets appropriate parameters regarding claims proceeds distribution methods. The Litigation Funding Bill also places necessary restrictions on common fund orders.

The Australian Government should not institute reforms allowing privacy matters to be pursued as representative proceedings while significant problems remain in the class action system.

It is also notable that in the 2020/21 reporting period, the OAIC resolved 1,746 matters through a representative complaint finalised in January 2021. This demonstrates that multiple complainants can effectively pursue redress through the OAIC under the current regulatory system.

15. Statutory tort of privacy

A number of detriments in introducing a statutory tort for invasion of privacy were comprehensively outlined in Ai Group's November 2020 submission. The current regulatory regime is sufficient to ensure that complainants have sufficient avenues available for redress in the event that they are impacted by a privacy breach. Introduction of a statutory tort would invariably lead to an increase in litigation with associated legal and insurance costs for business, particularly if such a tort were to encompass damages for emotional distress. Businesses should not be faced with the prospect of damages pursuant to a statutory tort where appropriate recourse is currently available through the complaints mechanisms under the Privacy Act.

In the event that a statutory tort is legislated for, despite Ai Group's opposition, it is essential that an exemption for employee records is maintained given the specific complications which arise in the workplace context. For example:

- In the event that such reforms extend liability on the basis of negligence or recklessness, employers may be forced to take an overly cautious approach in dealing with employee records – for example, in the event of a medical emergency requiring the provision of an employee's health information or where a financial service provider seeks information from an employer regarding an employee's financial status;

- Employers are subject to obligations under the FW Act to provide information to certain bodies such as the Fair Work Ombudsman and registered organisations; and

- The *Building and Construction Industry (Improving Productivity) Act 2016* (Cth) (BCCI Act) empowers authorised officers to require employers to provide information which may include personal information about an employee.

There is a public interest in ensuring that employers are able to effectively manage their workforce through the reasonable use of personal information.

Present uncertainty regarding whether the common law will develop of tort of invasion of privacy over time leaves businesses in a difficult position as to determining the degree of risk to which they are exposed in dealing with information. Any proposed reforms to the Privacy Act should confirm that the legislation covers the field with respect to recourse available to a complainant and rule out the possibility of a common law tort emerging.

.

ABOUT THE AUSTRALIAN INDUSTRY GROUP

The Australian Industry Group (Ai Group®) is a peak employer organisation representing traditional, innovative and emerging industry sectors. We are a truly national organisation which has been supporting businesses across Australia for nearly 150 years.

Ai Group is genuinely representative of Australian industry. Together with partner organisations we represent the interests of more than 60,000 businesses employing more than 1 million staff. Our members are small and large businesses in sectors including manufacturing, construction, ICT, transport & logistics, engineering, food, labour hire, mining services, the defence industry and civil airlines.

Our vision is for thriving industries and a prosperous community. We offer our membership strong advocacy and an effective voice at all levels of government underpinned by our respected position of policy leadership and political non-partisanship.

With more than 250 staff and networks of relationships that extend beyond borders (domestic and international) we have the resources and the expertise to meet the changing needs of our membership. Our deep experience of industrial relations and workplace law positions Ai Group as Australia's leading industrial advocate.

We listen and we support our members in facing their challenges by remaining at the cutting edge of policy debate and legislative change. We provide solution-driven advice to address business opportunities and risks.

OFFICE ADDRESSES

NEW SOUTH WALES

Sydney
51 Walker Street
North Sydney NSW 2060

Western Sydney
Level 2, 100 George Street
Parramatta NSW 2150

Albury Wodonga
560 David Street
Albury NSW 2640

Hunter
Suite 1, "Nautilos"
265 Wharf Road
Newcastle NSW 2300

VICTORIA

Melbourne
Level 2 / 441 St Kilda Road
Melbourne VIC 3004

Bendigo
87 Wil Street
Bendigo VIC 3550

QUEENSLAND

Brisbane
202 Boundary Street Spring Hill
QLD 4000

ACT

Canberra
Ground Floor,
42 Macquarie Street
Barton ACT 2600

SOUTH AUSTRALIA

Adelaide
Level 1 / 45 Greenhill Road
Wayville SA 5034

WESTERN AUSTRALIA

South Perth
Suite 6, Level 3 South Shore Centre 85
South Perth Esplanade
South Perth WA 6151

www.aigroup.com.au

Appendix C

Ai GROUP SUBMISSION

Australian Government
Attorney-General's Department

Response to the Privacy Act Review Report

March 2023

The Australian Industry Group (Ai Group®) is a peak national employer organisation representing traditional, innovative and emerging industry sectors. We have been acting on behalf of businesses across Australia for 150 years.

Ai Group and partner organisations represent the interests of more than 60,000 businesses employing more than one million staff. Our membership includes businesses of all sizes, from large international companies operating in Australia and iconic Australian brands to family-run SMEs. Our members operate across a wide cross-section of the Australian economy and are linked to the broader economy through national and international supply chains.

Ai Group supports the need to provide the public with confidence that their privacy and their data is being handled safely and responsibly. We advocate for the principle of Data Stewardship, which reflects the obligations and responsibilities of business of all sizes and industries in managing data collected in the usual course of business or as part of the business model. It reflects both the governance requirements and responsible utilisation of data and covers technological and behavioural strategies. It also addresses the safe disposal of data at the end of its usefulness.

Consideration should be given to the impact of multiple forms of regulation in this area such as Consumer Data Right and industry specific regulations. Over-regulation has the potential to chill innovation and add costs to business.

There are two significant changes presented in the report that business must grapple with:

- the inclusion of SMEs and
- the closer alignment with GDPR rules.

We maintain our objection to removal of the exclusion of SMEs. We acknowledge that there is support being offered to assist SMEs to comply with new regulations, however, it needs to be recognised that compliance to these rules is an ongoing adaptive process as technology and business practices change. Support cannot be regarded a 'set and forget' proposition, rather Government and industry must work in partnership for the long term to support privacy considerations without stifling innovation.

Ai Group has long advocated for international regulatory cohesion in digital and privacy rules. We welcome the attempt to align with the rules of our trading partners, however, there is a risk that we make limited facsimiles of external rules, with far reaching consequences in the Australian context, without achieving the benefit of automatic reciprocal coverage. The justified and welcome exceptions for employee data may risk the desired outcome.

Similarly, there should be caution against shifting emphasis of protecting consumers under the current regime, to data protection under the EU GDPR. The EU GDPR is a complex scheme with qualifications and exceptions to ensure practical implementation. Adoption of definitions and other individual features of the EU GDPR risks over-inclusiveness and unworkability.

Government should be aware of various issues associated with adopting an EU GDPR approach. International experience suggests that the EU GDPR has been highly prescriptive, with certain provisions introducing significant burdens on regulated businesses without necessarily providing demonstrable benefit to individuals. Retaining the flexibility of the APPs would mitigate the risk of a similar outcome in Australia.

Of particular concern is the introduction of a requirement of a **Data Protection Officer and a Data Impact Statement** and the risk of increasing the regulatory burden on Australian businesses, especially public facing businesses. As the OAIC prepares its guidance, we encourage lengthy consultation with a wide range of organisations to avoid regulatory overreach.

- Notice of collection of personal information:
    - Government should be cognisant of the risk of cumulative increase of notifications and information overload for consumers associated with notice of collection requirements.
    - Government should properly assess whether there are material consumer benefits from expanding the range of requirements for giving of notice of collection requirements, and as to the content of these notices.
- Consent to the collection, use and disclosure of personal information:
    - Government should be cautious to not add a costly regulatory burden to businesses by requiring the retrospective operation of consent requirements in relation to already obtained data.
    - Similar to the issue of notice of collection requirements, Government should be cognisant of the risk of creating information overload or consent fatigue for consumers with consent requirements.
    - There are practical implementation issues for businesses if the statute expands the range of requirements for obtaining of consent, or the form of requests for consent.
    - Opt-in consent should only be required where it is a real benefit to individuals and does not materially impact on the ability of businesses to provide and develop innovative services to the benefit of consumers and the broader Australian economy.
    - Government needs to properly understand the EU GDPR approach to consent. This includes the many exceptions and limitations to those consent requirements, including the legitimate interest exceptions.
    - Proposal 13.4 can be problematic for logistics service providers. They receive personal information about an individual from a third party (e.g. receive consignees' personal information from shippers). The proposal may have unintended consequences and/or burden for logistics service providers who have hundreds of thousands of consignments per week where the customer/shipper provides the personal information of the consignee/receiver to facilitate delivery. A requirement that the third party would need to verify consent could create a diffusion of responsibility and practical implications to the transfer of personal data.
- Right to erasure or be forgotten:
    - Consideration should be given to how erasure rights would impact insights that businesses develop through their own methods (e.g. inferences).
    - Proper consideration of public interest exemptions should be given to the right to erasure. This should ensure proper consumer safeguards are considered and not inadvertently impacted, such as ensuring privacy and security, preventing fraudulent activity and resolving complaints or litigation.
    - Introducing this right could create a conflict with providing incentives to entities to ensure effective anonymisation of personal information to better protect against privacy risks.
    - Introducing this right could also conflict with mandatory regulatory requirements for retention of personal data.
    - Unlike under the EU GDPR, the proposed right is not qualified through judicial oversight and

ability to make public interest considerations. This should be taken into account and amended.

- Direct marketing, targeted advertising and profiling

We appreciate the intention behind the proposal is aimed at assisting individuals in enhancing their awareness and understanding about the use of information for direct marketing. However, the proposal does not contemplate that such information is collected for other various legitimate reasons that would also be in the individual's interest. For instance, consumers could reasonably expect information to be collected to enable better customer service, improve products or service customisation, communication of non-marketing information such as invoices, and to protect against fraud. In this regard, loyalty schemes should benefit from being considered for exemption as an example. Such applications are not always known at the time of collection, which could evolve over time to meet consumer expectations. Careful consideration should be given to any opt out settings so that consumers and businesses can continue to benefit.

- Proposed removal of the small business exemption

Ai Group opposes the proposed removal of the small business exemption as identified in the Review Report at recommendation 6.1. The removal of the current exemption would impose a significant cost and compliance burden on small business that in many instances would be disproportionate to the incidence and scale in which personal information is collected.

The Review Report proposes that consultation with an impact analysis should occur before the current statutory exemption is removed. It is apparent that any impact analysis would only be accounted for in designing support measures as a result of the exemption's removal rather than in the design of an alternative or more narrow exemption. While consultation is welcome, this provides little comfort to small business operators, who would be greatly concerned about the magnitude of the compliance cost and viability of their operations.

Ai Group contends that the removal of the exemption would present very significant challenges for small business and their capacity to comply with the APPs. Small businesses cannot simply adopt the technological and digital infrastructure to comply as larger organisations. Similarly, the need to upskill and/or hire new staff to assist in the implementation of the APPs would be an essential step that many small businesses would not be in a financial position to take.

The removal of the current exemption would also be a strong barrier to small business creation and will no doubt create constraints on the ability of small business to grow and employ.

If, despite Ai Group's objection, the proposal proceeds, it is essential that consideration be given to an alternative level of privacy regulation that may go to modifying the exemption rather than its complete removal.

The Review Report's proposal at 6.2 states:

In the short-term:

- *prescribe the collection of biometric information for use in facial recognition technology as an exception to the small business exemption, and*

- *remove the exemption from the Act for small businesses that obtain consent to trade in personal information.*

While Ai Group consider these measures to be far more targeted and less disruptive to small

business across the board, the introduction of any new obligation on small business should be preceded by adequate consultation and with extensive transitional arrangements.

- Employee records exemptions

The Review Report proposes an increase in privacy protections for employees but acknowledges that "further consideration is required as to how the privacy and workplace relations laws should interact."

Specifically, the Review Report makes recommendation 7.1 in relation to the employee records exemption.

Enhanced privacy protections should be extended to private sector employees, with the aim of:

a) providing enhanced transparency to employees regarding what their personal and sensitive information is being collected and used for

b) ensuring that employers have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship, including addressing the appropriate scope of any individual rights and the issue of whether consent should be required to collect employees' sensitive information

c) ensuring that employees' personal information is protected from misuse, loss or unauthorised access and is destroyed when it is no longer required, and

d) notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm.

Further consultation should be undertaken with employer and employee representatives on how the protections should be implemented in legislation, including how privacy and workplace relations laws should interact. The possibility of privacy codes of practice developed through a tripartite process to clarify obligations regarding collection, use and disclosure of personal and sensitive information should also be explored.

Ai Group supports the retention of the current employee records exemption in the Privacy Act 1988 (Cth) (Privacy Act) and strongly opposes its removal.

Further, Ai Group does not support narrowing the employee records exemption (or the effect of the exemption) such that it would create additional obligations on employers that not only carry an added regulatory burden but constrain employers from acting in compliance with other workplace laws.

Ai Group refers to its earlier submissions regarding the importance of retaining the employee records exemption and its essential role in enabling employers to manage matters arising from the employment relationship and obligations under a variety of workplace laws.

If anything, under current Australian Government labour standards and gender equity policy, the need for employers to collect employee personal information relating to the workplace is growing. This reflects the intended outcomes of Government policy in often requiring higher levels of employer intervention and control into various workplace matters, rather than any commercial motivation of the employer.

For instance, recent legislative developments in the areas of workplace sexual harassment, workplace gender diversity reporting and foreshadowed reform concerning employer obligations relating to the underpayment of wages, same job same pay, labour hire licensing and modern slavery

due diligence all elevate the need for employers to be collecting employee information to help satisfy new and specific legal obligations.

It is essential that privacy reforms relating to employee information travel cohesively with current Government workplace reform -particularly given its magnitude.

Accordingly, it would be inappropriate and would add to the fragmenting of privacy obligations (as they relate to employers and employees) if any further reform around employee privacy protection was solely dealt within the Privacy Act. As referred in our earlier submissions, the Fair Work Act 2009 (Cth) regulates employer obligations in relation to employee and employment records, in addition to various state and territory workplace surveillance legislation.

If the Government is minded to engage in further consultation about modifying, or modifying the effect of the current employee record exemption, it is essential that it squarely focus on the impact of any proposed modification as it relates to the employment relationship, and employer (and employee) obligations under workplace laws.

The specific formulation of considerations in recommendation 7.1 would create a raft of problems for employers in managing matters arising in the employment relationship and workplace law obligations. What may be seen as a modest and targeted modification to the employee exemption may still have profound adverse and unintended consequences on a range of matters, such as employee and community safety.

For instance, we envisage that additional employer obligations arising from legislating matters in 7.1(a), (b), (c) and (d) would have the potential to significantly impede the ability to conduct workplace investigations (including work, health and safety) or other disciplinary matters employers may be required to act upon.

The role of privacy codes of practice may be a more appropriate and targeted alternative to new legislative obligations on employers. Ai Group would not support codes of practice if they were intended to add a further regulatory layer to any new legislative obligations on employers in respect of employee records and employee information. This would be of limited utility to employers and employees and would only add to the complexity of privacy regulation generally.

Ai Group would not be opposed to a tripartite consultation process given that the issues for consideration need to be properly understood as they apply to employers, employees and workplace laws.

It is essential that the workplace relations legislative framework remain the appropriate framework for any further assessment by the Government relating to privacy protections for employee records.

Louise McGrath

Head of Industry Development and Policy

Australian Industry Group.