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.

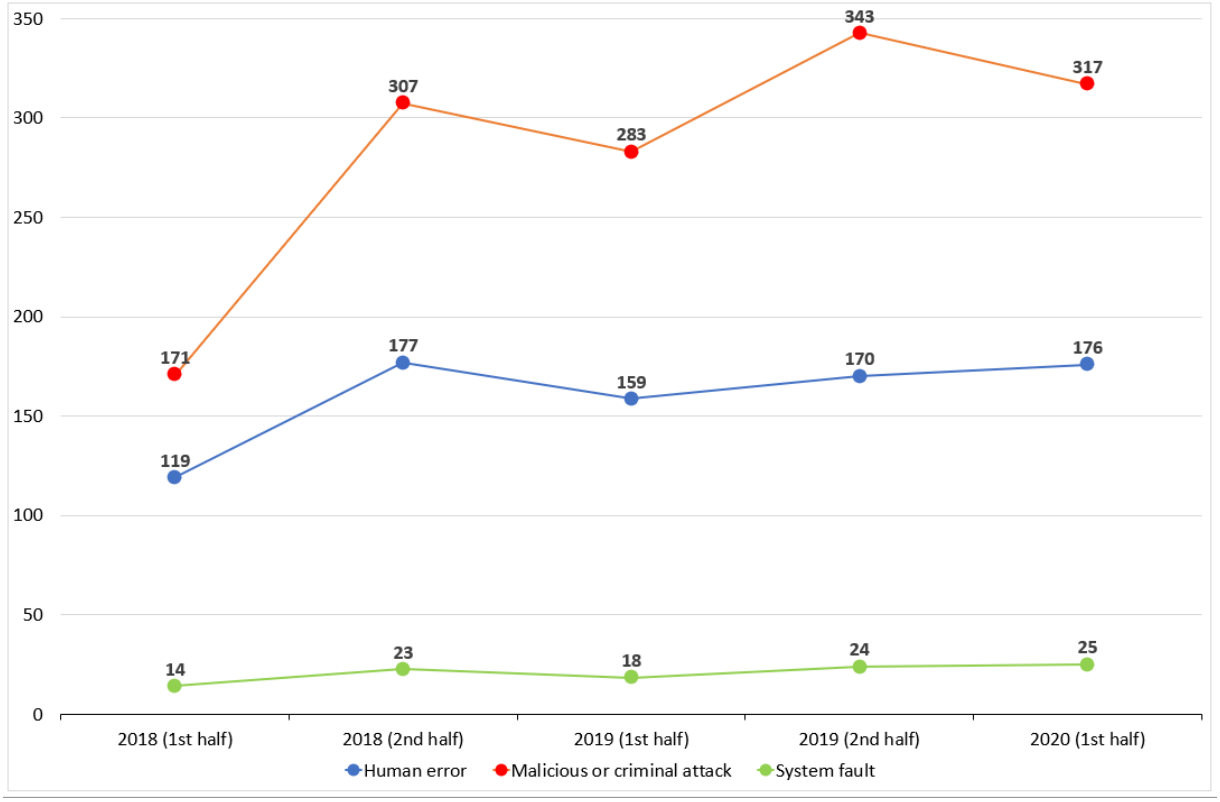
exercising reasonable use of personal information to effectively manage their workforce.

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

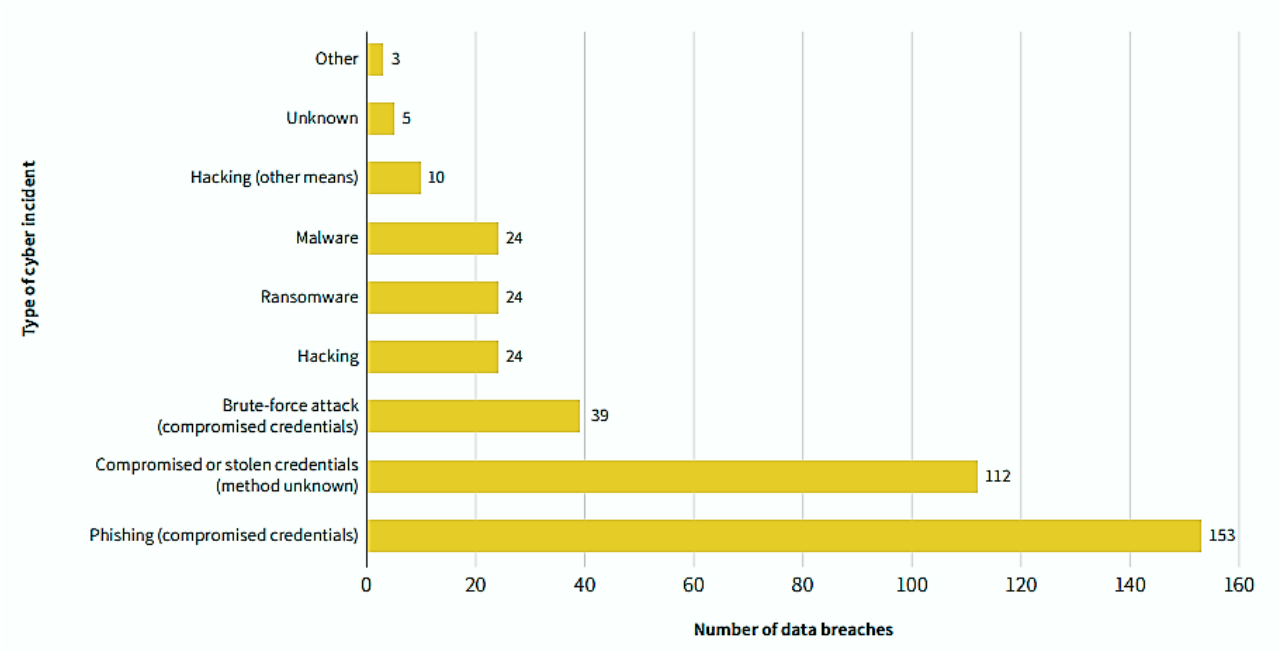
By the end of June 2020, there were over 2,320 data breaches reported to the OAIC since the NDB Scheme commenced.[23] Over this period, malicious or criminal attacks greatly contributed to these data breaches (61%), followed by human error (34%). System faults (4%) were rarely a factor.

[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]

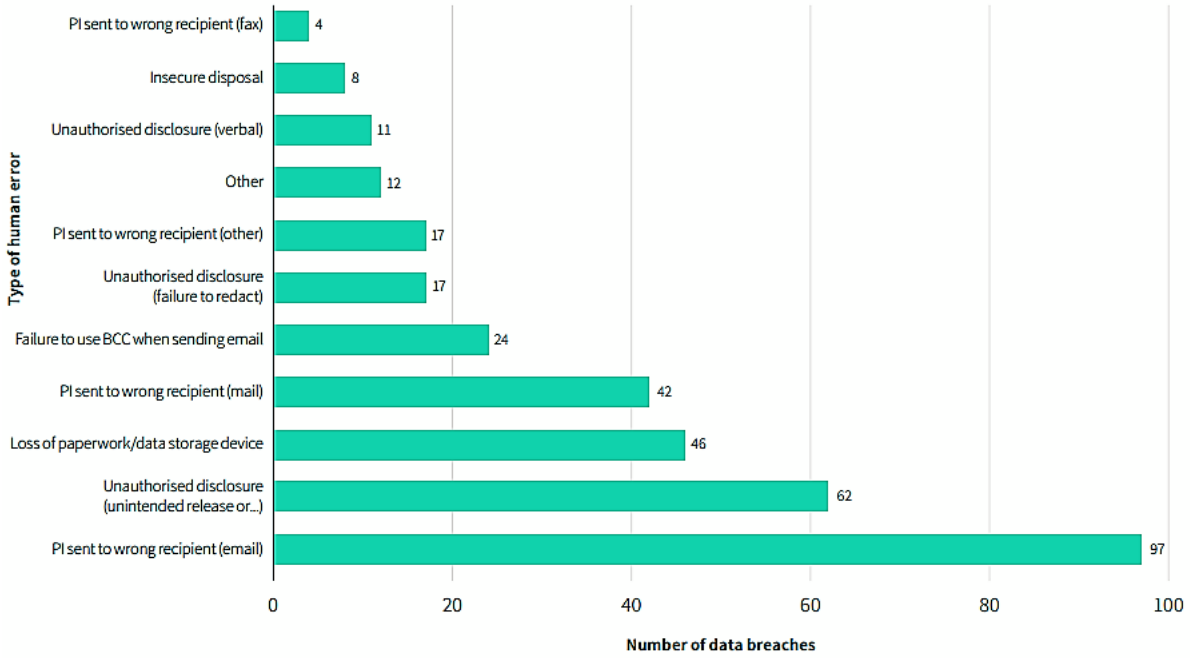
Chart 2: Notifiable data breaches caused by cyber security incidents, 1 April 2018 – 31 March 2019



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



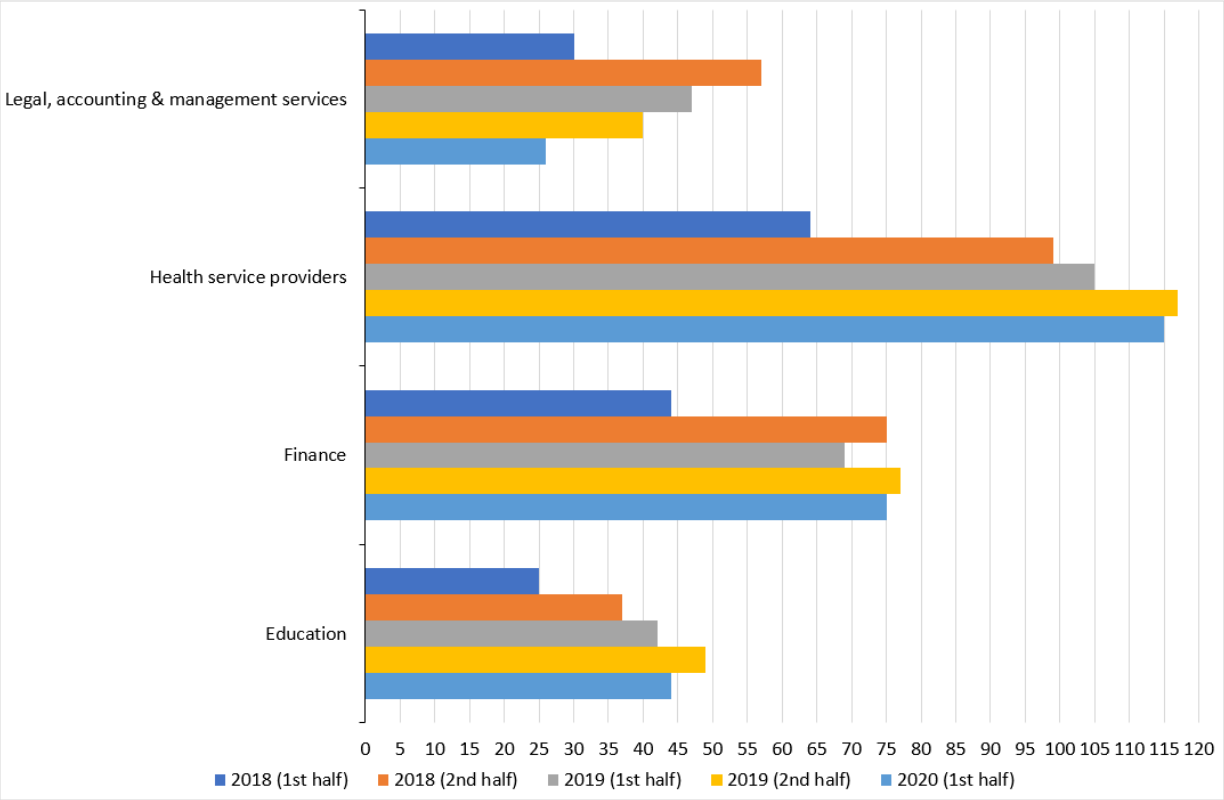
Source: OAIC, Insights Report, 2019

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