Australian Chamber of Commerce and Industry

Privacy Act Review Report

Attorney-General's Department

ACCI Submission

31 March 2023

Australian Chamber of Commerce and Industry

Working for business.
Working for Australia

Telephone 02 6270 8000 | Email info@acci.com.au | Website www.acci.com.au

Media Enquiries
Telephone 02 6270 8020 | Email media@acci.com.au

Canberra Office
Commerce House
Level 3, 24 Brisbane Avenue
Barton ACT 2600
PO BOX 6005
Kingston ACT 2604

Melbourne Office
Level 2, 150 Collins Street
Melbourne VIC 3000

Sydney Office
Level 15, 140 Arthur Street
North Sydney NSW 2060
Locked Bag 938
North Sydney NSW 2059

Perth Office
Bishops See
Level 5, 235 St Georges Terrace
Perth WA 6000

ABN 85 008 391 795

Australian Chamber of Commerce and Industry

Table of Contents

Introduction

1. ACCI welcomes the opportunity to respond to the Privacy Act Review Report (**Report**).

2. ACCI's primary concern with the Report lies in the proposal to remove the small business exemption from the *Privacy Act 1988*. As will be discussed later in this submission, the small business exemption has a strong policy basis in the lesser capacity of small businesses to comply with privacy law.

3. In addition to the arguments that will be raised, ACCI stresses from the outset that the removal of this critical exemption while simultaneously adopting other proposals made in the Report will have significant consequences for small businesses in Australia. In effect, presently exempted small businesses in the future will face the risk of not only being required to divert substantial resources into privacy compliance generally, but also being required to comply with a privacy law framework that will become more complex and onerous than that which is presently faced by large corporations. This is an unreasonable challenge to impose on small business.

4. In a similar vein, the Commonwealth should be attentive to the ways in which each proposal interacts with one another prior to deciding to adopt any specific proposal. For instance, if the employee records exemption is not expanded to include the collection of information (as will be argued by ACCI), proposal 4.3 to extend the definition of 'collection' under the Act will mean that employers will bear greater obligations with respect to employees' information that could create challenges for workplace management.

5. Overall, ACCI remains concerned about some aspects of the proposals in the Report. Nevertheless, ACCI thanks the Attorney-General's Department for the opportunity to provide our feedback in response to the Issues Paper and Discussion Paper during the review in the preparation of the Report. ACCI would be very interested in engaging in future consultation regarding any of the proposals contained therein.

6. This submission will substantively address the following parts of the Report:

   a. Personal information, de-identification and sensitive information;

   b. Small business exemption;

   c. Employee records exemption;

   d. Consent and privacy default settings;

   e. Organisational accountability;

   f. A direct right of action; and

   g. A statutory tort for serious invasions of privacy.

7. The final section of this submission will then address the other parts of the Report in brief.

Australian Chamber of Commerce and Industry

Personal information, de-identification and sensitive information

Changes affecting the definition of sensitive information

1. Proposal 4.9 reads:

   Sensitive Information

   (a) Amend the definition of sensitive information to include 'genomic' information.

   (b) Amend the definition of sensitive information to replace the word 'about' with 'relates to' for consistency of terminology within the Act.

   (c) Clarify that sensitive information can be inferred from information that is not sensitive information

2. ACCI has concerns in relation to amending the definition of sensitive information, particularly part c and 'inferred' information.

3. These concerns arise from member feedback indicating that this proposal read in combination with other proposals could create compliance difficulties that do not produce significant benefit.

4. If this proposal is to be progressed, further guidance will be needed that clarifies the intent of these amendments and considers how these amendments are to be read in conjunction with other changes in section 4 for example.

Geolocation tracking proposal 4.10

5. ACCI has significant concerns in relation to the current wording of proposal 4.10, which reads:

   > 4.10 Recognise collection, use, disclosure and storage of precise geolocation tracking data as a practice which requires consent. Define 'geolocation tracking data' as personal information which shows an individual's precise geolocation which is collected and stored by reference to a particular individual at a particular place and time and tracked over time.

6. ACCI notes that the report indicated there was merit in including precise geolocation tracking data as a special category of personal information requiring express consent for tracking and storage over time to address concerns about risk to personal safety and lack of transparency. Previous respondents who flagged concerns did so mainly in relation to limited uses of location data which the report indicated are not intended to be captured.

7. ACCIs concerns are in relation to:

   - Where geolocation is used as a safety control for workers undertaking isolated or remote work
   - Where geolocation tracking is used in facility service and maintenance systems, and
   - We do not believe the 'employee record exemption' would cover these above situations/information as it does not necessarily directly relate to the employment relationship and is not information contained in an employee record held by the employer in relation to the individual.

Geolocation as a safety control for workers undertaking isolated or remote work

8. The key issue we see here is that work health and safety practices (and compliance) are informed by consultation and what is 'reasonably practicable' whereas the proposal above uses the concept of 'consent'.

9. Where workers are undertaking isolated work or are working alone, a reasonably practicable control that may have been identified through risk assessment and consultation with workers is the implementation of a communications or monitoring system for workers working alone.

10. For example:

    - *Man Down App* – this system buddies up and individual with service controllers or a work colleague spotter that is remote to the person working alone. If action is not taken within a nominated period of time then alerts are generated to action search and rescue.

    - *After Hours Service Desk* – technicians are date and time stamped when receiving an afterhours service call. The technician must respond to time limits (dead man actions). Failure to do so results in search and rescue action.

11. It is unclear how you would address inconsistencies between the pieces of legislation and the concepts of 'consent' and 'consultation' and the extent of the consequences on the business as well as the safety of individuals of needing to comply with 'consent' in implementing these controls. This recommendation would also interact with the other 'consent' related proposals and should be examined together.

Geolocation tracking used in facility service and maintenance systems

12. Geolocation tracking is used in everyday services for trades and other industries in relation to facility service, maintenance scheduling and asset management systems. We are concerned that this proposal would result in significant business interruptions and costs as well as unintended consequences such as breach of legislative and insurance requirements.

13. For example:

    - Proprietary facility service, maintenance scheduling and asset management systems use geolocation tracking for assets and service and maintenance data collection throughout the life of the asset. This is achieved by geolocation tags on assets. As work is assigned to the asset it tags the technician, date, time that the technician attends, the 'take 5' (safety process) prior to commencement of work, the work carried out and the tag off time. These records are kept for the life of the building to demonstrate, contract and legislative mandatory inspection compliance. Administration rights to the systems allow tracking of the technician throughout the course of the day, week, month, year. It may also interface with time sheet and pay role systems. Without this capability companies would not be able to operate as they currently are.

    - In the Plumbing industry, geolocation tracking is used for multiple purposes:

        - Geolocation of business assets. Utes, machinery, trailers, equipment etc not only for security but for insurance as well.

        - Geolocation for maintenance plumbing businesses for easy allocation of emergency plumbing jobs to nearest staff member.

- Geolocation for client asset service reports. Logs the exact location of the asset, date time, technician etc.
- Logging of job records which shows proof that worker has attended a site. Great for invoicing queries.
- Safety for employees, as it shows their location of where they are working or last known location. Especially for isolated workers.
- Job management software utilises Geolocation tracking to be able to locate job sites more accurately, or areas within the sites the works are being undertaken.

- Geolocation tracking is also used in the fire protection industry, where it is integral to the tracking of attendance to critical fire safety issues (e.g. fire alarm system malfunctions in schools, hospitals, and aged care facilities as well as high density apartment living and office spaces, and special hazard system malfunctions – 'special hazards' are the special systems set up to respond to particularly niche fire hazards such as at airports, for example – and can be exceptionally costly and dangerous if a system malfunctions). Given much of this work can occur while technicians are on call, the linkage to payroll and timesheets is also important. In addition, given the fire protection industry is strictly regulated in most jurisdictions in terms of licensing, certification, and registration, it's also important for employers to be able to demonstrate that the specific person who attended a job was suitably licensed to perform that work.

Unclear if the 'employee record exemption' would cover these situations.

14. Some of the uses of geolocation data mentioned above to not directly relate to the employment relationship and is not information contained in an employee record held by the employer in relation to the individual. We would need clarity on how employee record exemptions would apply in these instances or not.

Small Business Exemption

15. In relation to the small business exemption, the Privacy Act Review Report recommended that:

> 6.1 Remove the small business exemption, but only after:
>
> (a) an impact analysis has been undertaken to better understand the impact removal of the small business exemption will have on small business - this would inform what support small business would need to adjust their privacy practices to facilitate compliance with the Act
>
> (b) appropriate support is developed in consultation with small business
>
> (c) in consultation with small business, the most appropriate way for small business to meet their obligations proportionate to the risk, is determined (for example, through a code), and
>
> (d) small businesses are in a position to comply with these obligations.

16. ACCI resolutely opposes the proposal to remove the long-standing small business exemption from the Privacy Act. Small business owners are facing mounting costs, labour shortages and ongoing regulatory changes. This proposal would be onerous and costly for smaller entities. There is no widespread evidence of data breaches by small businesses that would justify the removal of this exemption.

17. ACCI submits that small businesses would be disproportionately impacted by the onerous burden of additional regulatory requirements and the cost of privacy law compliance. Harming small businesses or risking their viability through an unnecessary intensification and extension of the regulatory demands upon them hurts not only small business families and employees, but also the communities in which they operate.

18. We acknowledge and welcome the substantial contributions that have been made to the discourse from the 'diverse range of stakeholders including government agencies, academics, research centres, private sector organisations and consumer advocates' on the appropriateness of whether small businesses should be subject to privacy law obligations.[1]

19. Nevertheless, ACCI encourages the Attorney-General to give foremost consideration to the representatives of businesses, whom this change will ultimately and significantly burden.

20. Many of the other interests, however eminent, are engaging with this academically or on a basis of principle, and not through sufficient consideration or understanding of the capacities and circumstances of small businesses, nor the impact upon them of being subject to Commonwealth privacy law.

21. ACCI views assertions about an absence of comparable exemptions overseas and Australia's exemption being 'an international anomaly' as extraneous to a question that must be about whether subjecting small businesses to a greater regulatory burden will benefit or harm their viability, employment, and contribution to our economy.[2] We note the comments around Australian small businesses exemptions as unique, however the Privacy Act allows for sectors which are considered to be a higher privacy risk to be covered by the Act.

[1] www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf, p. 60
[2] Attorney-General's Department, *Review of the Privacy Act 1988* (Discussion Paper, October 2021) 43.

22. ACCI believes the proposal at 6.1 should instead recommend that an impact analysis on removal of the small business exemption be conducted by sector to determine if removing the exemption is required. This will continue to allow sectors to be exempt should the Act have no relevance to them, and those sectors deemed high risk should be covered by the Act.

23. If the Government proceeds with removing the exemption altogether for small businesses, a comprehensive impact analysis must be undertaken across sectors. This will inform an understanding of the impact of the removal of the exemption on small businesses including financial requirements and the resources needed to assist in the implementation of the Privacy Act requirements.

24. A clear understanding of the financial implications of the removal of the exemption on small businesses must be undertaken prior to it being removed entirely. In the Privacy Act review there is a figure on potential cost, which converts an estimate from 2008 into 2021 figures, with the financial impact estimated at $292.87 for a start-up and $391.79 for ongoing annual costs.[3] It is extremely unlikely the costs will be this low, the impact analysis must develop estimates of the initial cost of compliance and the ongoing costs for different sectors.

25. We note that in the European Union, over 40% of small businesses reported spending at least €10,000 (AUD $15,657 as of 1/1/2022) on GDPR compliance.[4] Further, 18% of small businesses reported spending over €50,000 (AUD $78,284) on compliance.[5] GDPR rules are of course more stringent than those in Australia or those proposed in the Discussion Paper, however privacy regulation advocates generally support greater symmetrisation with that framework[6] and it is valid to assess European compliance costs in assessing proposals to have Australia move in the European direction. These costs are simply unmanageable for most small businesses.

26. In the EU, nearly half of small businesses were reported to be often failing to comply with GDPR obligations.[7] This presents a serious problem in itself — due to the sheer cost and burden of compliance, small businesses can become unable to cope with their obligations and resultantly run the risk of illegal activity. An extraneous, unbalanced or impractical obligation that is ignored in practice is not protecting anyone or changing the management of information in any way, it is just endangering vulnerable small business owners to whom the obligation should never have been imposed.

27. The outcome of the impact analysis should be used to inform the development of the resources needed to assist small businesses. These resources must be developed with input from small business representatives and industry associations. Consulting the ACCI network and working with our members, will be a central to attracting interest and cooperation from small businesses. There will need to be the development and appropriate funding of a comprehensive support and education programs. The development of resources for small businesses could see the creation of privacy audit list, template privacy policies and advice for small business owners prior to the removal of the exemption.

28. Additionally, a framework such as small business privacy guidelines may be useful to improve the information collection and handling practices of small businesses.

---

[3] https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf p.67
[4] GDPR.EU, *2019 GDPR Small Business Survey* (Report, May 2019) 5.
[5] See Ibid.
[6] Attorney-General's Department, *Review of the Privacy Act 1988* (Discussion Paper, October 2021) 8.
[7] GDPR.EU, *2019 GDPR Small Business Survey* (Report, May 2019) 3.

29. Small businesses will face significant and ongoing expenses in order to comply with the Privacy Act. This will entail various "soft costs" such as training staff, setting up data breach procedures, and designating a team member responsible for ensuring compliance with the Act, including addressing requests for the retrieval and de-identification of personal information collected by the business. These additional expenses related to processes and information systems could amount to thousands of dollars, which may be difficult for small businesses to absorb.

30. To assist small businesses transition, a key trusted adviser for small businesses will be through the role of the Australian Small Business and Family Enterprise Ombudsman (ASBFEO). This body should receive additional funding to provide practical advice and assistance to small business which should be delivered and coordinated with supporting engagement from the Privacy Commissioner. ASBFEO position in the small business community makes it an ideal reference point for assistance and information provision. It is crucial that agencies are sensitive and supportive of small businesses provide any lead in this area

31. Small businesses will need assistance to improve their rate of digitalisation as they look to meet Privacy Act requirements. It is estimated that close to half a million Australian SMEs have no or little engagements with digital tools.[8] The *Technology Investment Boost* and *Skills and Training Boost* Measures announced in the 2022-23 federal budget, provide an additional tax deduction of 20 per cent for small businesses, with an annual turnover of less than $50 million, to invest in external training of staff and business expenses and depreciating assets that support digital uptake. It will be funding of programs like these that will assist small business owners increase their digitalisation ability to meet privacy requirements.

32. Other methods such as various financial aid to small businesses or industry-specific employer associations to run and implement privacy programs may also be useful.

33. The federal government should take a lead role in harmonising existing state and territory privacy regimes, there are instances where the Consumer Data Right Rules may have some intersection with the APP's.

34. Non-regulatory methods of improving privacy protections in small businesses must be considered before the removal of the exemption. This could include online training courses for small business owners. Ultimately, ACCI supports the intentions of improving privacy outcomes, but the means of achieving these objectives—removing the small business exemption—is ill-considered and costly.

35. If the exemption is removed, ACCI recommends a two-year transition process in order to ensure all businesses have the opportunity to equip themselves and implement the required changes. This will ensure business have the opportunity to adjust to practices to meet privacy standards and to address unforeseen issues that may arise. During this time, OAIC could take a more educative approach to enforcement. This would allow small businesses sufficient time to adopt the appropriate information collection and handling practices, which may require significant investment and alterations to existing commercial arrangements.

36. ACCI believes that if pecuniary penalties for small businesses are introduced, the Act must be amended and consideration provided to the size and resources of an entity when determining a penalty.

37. A review of any changes to the Act must be undertaken within two years of implementation.

[8] MYOB, Australia's SMEs: A Snapshot, 2022

Australian Chamber of Commerce and Industry

Employee Records Exemption

Introduction

38. In relation to the employee records exemption, the Privacy Act Review Report recommended that:

> 7.1 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.

39. In response to the Discussion Paper released in the review, ACCI submitted that the employee records exemption should be retained because the personal information of employees should be protected under workplace relations legislation, which primarily governs and regulates the employment relationship, rather than under privacy law. ACCI maintains this position.

40. Employee records are fundamentally different to other information protected by privacy law. Integrating employee records within the scope of the *Privacy Act 1988* would require a unique framework of rules to reflect these inherent differences, which would both complicate privacy law, due to the added complexity in the legislation, and workplace relations law, due to the potential for overlapping of regulation.

41. The decision to not recommend an outright abolition of the employee records exemption is therefore welcome. ACCI appreciates the concerns underpinning the position that further enhancements to the privacy protections of employees' personal information may be justified and looks forward to engaging in further consultation with the Government on the Report's proposal, should they decide to accept it, on the basis that these changes are contemplated within the workplace relations legislative framework.

42. This part of the submission will first discuss the existing privacy protections for employee records and then address each of the four aims listed in Proposal 7.1 sequentially.

43. In summary, ACCI:

    a. contends that the existing patchwork approach to the protection of employee records, with the collection of information for their creation regulated under privacy law while they are otherwise regulated under workplace relations, suggests that the employee records exemption should not only be retained but expanded;

b. remains unconvinced that the existing privacy protections are wholly inadequate, but nevertheless would be willing to engage in consultation and a review of the regulations, on the condition that any further protections are introduced within the workplace relations framework; and

c. considers that any reviews of the privacy regulations for employee records should be primarily guided by the need to protect their information rather than a desire to create new rights for individuals.

Existing Privacy Protections of Employee Records

44. If the existing privacy protections of employee records are to be reviewed, ACCI submits that they should be done so with the objective of merging them all into a single regime under the workplace relations framework, in recognition of their idiosyncrasies (which are described in respect of each aim of Proposal 7.1 below). This would entail the extension of the employee record exemption to the collection of information for the creation or amendment of employee records, while strengthening those that exist under the *Fair Work Regulations 2009*.

45. This approach would significantly assist employers, particularly those smaller businesses who narrowly fall outside the scope of the small business exemption (or all small businesses, were Proposal 6.1 to be adopted), in complying with and understanding their privacy obligations in relation to employee records. It would also mean that the purpose of the Australian Privacy Principles that already apply to the collection of information for employee records could be fulfilled in a way that minimises adverse impacts on the management of the employment relationship.

46. As noted in the Report,[9] in *Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946 (***Lee***), the Full Bench of the Fair Work Commission held that the employee records exemption does not apply to employee records that are yet to be in the possession or control of an employer.[10] Accordingly, the Australian Privacy Principles will generally apply to the collection of employee records.[11]

47. Consequently, the employee records exemption fails to exclude employee records from a significant proportion of the Australian Privacy Principles. Under APP 1, an employer may need to specify what kinds of personal information of their employees they collect, how they do so, and for what purposes.[12] Under APP 3, as was in dispute in *Lee*, an employer may require consent for the collection of sensitive information from employees. Other APPs are likely to apply, such as APP 5.

48. This means that the *collection* of information for the creation of employee records are largely regulated in the same way as the collection of this information for other purposes; however, the *use* of this information does fall within the exemption.

49. Under the workplace relations framework, employers bear other obligations in relation to employee records. For instance, employers are prohibited from making or keeping an employee record that they know is false or misleading.[13] Employers must also make a copy of an employee record available for inspection and copying on request by the employee or former employee to whom the record relates.[14]

---

[9] Report 66.
[10] *Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946 [56].
[11] Ibid [57].
[12] *Privacy Act 1988* (Cth) sch 1 cls 1.4(a)-(c).
[13] *Fair Work Act 2009* (Cth) s 535(4).
[14] See *Fair Work Regulations 2009* reg 3.42.

50. This melange of privacy protections detracts from compliance. Following *Lee*, the degree to which employers are aware of their obligations under the *Privacy Act 1988* with respect to the collection of information for employee records may still remain limited. It is on this basis that ACCI contends that, not only should any future new privacy protections for employees records be introduced solely withing the workplace relations framework, but also that the employee records exemption should in fact be extended to cover the collection of information, thereby excluding employee records from the scope of the *Privacy Act 1988* entirely.

51. As ACCI and other parties submitted in the Privacy Act Review,[15] the application of APP 3 risks interference with the legal duty of employees to obey lawful and reasonable directions of their employers to provide information that is necessary for the performance of management action or the operations of a business. For example, complications could arise in the collection of information that arguably falls within the definitions of "religious beliefs" or "political opinions" during a workplace investigation into a discrimination complaint, which may need to be discrete and would be inhibited by the requirement to obtain consent. This is not to say that future privacy protections of employee records should never involve consent requirements; rather, by consolidating all privacy protections of employee records into the workplace relations framework, the protections could be designed in a manner that is bespoke to the employment relationship and provides for sufficient carveouts that are deemed necessary.

Objectives of a review of the privacy protections of employee records

52. The existing privacy protections of employee records under both privacy law and workplace law have not been demonstrated as wholly inadequate. However, ACCI acknowledges that improvements could be made and, pursuant to the proposal, would be very interested in engaging in any consultation regarding future changes, as long as it occurs with the intention of confining them to the workplace relations system.

53. If the privacy protections of employee records are to be reviewed, ACCI has the underlisted views with respect to each of the objectives listed in paragraphs (a)-(f) of Proposal 7.1.

Aim of review of privacy protections	**ACCI Position**
(a) providing enhanced transparency to employees regarding what their personal and sensitive information is being collected and used for	In some circumstances, requiring employers to be fully transparent about the collection or use of employee information could impair legitimate management actions or business functions. One area where this issue may arise is with respect to workplace investigations, where employers may need to collect information in a non-transparent way to protect the confidentiality of complaints and procedures. For example, an employer may need to examine and collect information from the work email logs of an employee who is an alleged perpetrator of workplace bullying, without notifying them. It is crucial that any requirements imposed on employers to provide employees with greater transparency about the collection and use of their personal information enable employers to carry out these important functions unimpeded.

[15] Report 66.

(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	ACCI strongly supports this objective because the administration of the employment relationship and operation of businesses requires the treatment of information is unique ways. Unlike the collection and use of consumers' information, there may be legitimate reasons for the collection or use of employees' information that is contrary or tangential to that particular employees' interests. As noted above, one example where this would apply is in workplace investigations. Another example could be where employers are required to collect employees' information to comply with public health orders, such as a vaccine mandate, irrespective of whether an employee wishes this information to be collected.
(c) ensuring that employees' personal information is protected from misuse, loss or unauthorised access and is destroyed when it is no longer required	While ACCI does not consider the existing privacy protections for employee records wholly inadequate, it is acknowledged that there may be some room for improvement. If the privacy protections for employee records are reviewed, ACCI contends that this principle of "ensuring that employees' personal information is protected" should be given primacy over other considerations. Fundamentally, privacy regulations that apply to employee records are about privacy *protection*. They are not and should not be focussed on providing individual rights to employees, which is what rules relating to consent and transparency are premised on.
(d) notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm	ACCI is willing to engage on practical proposals that would facilitate the notification of data breaches involving employee's personal information which are likely to result in serious harm. If such changes are introduced, they should be accompanied by guidance resources for businesses.

Consent and privacy default settings

54. Section 11 outlined proposals in relation to consent and privacy default settings. ACCI and our members have significant concerns about the consent proposals, particularly when read in conjunction with each other and other proposals.

55. Proposal 11.1 is to 'amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous'.

56. ACCI is concerned about the ambiguity of the words, in particular the word "current." It implies that consent can expire but does not specify any timeframes. Any changes to the definition should provide greater clarity and not create uncertainty.

57. Any future legislation that seeks to introduce this definition should be accompanied by explanatory material that indicates an intention for the threshold for each aspect of this definition to be low. This would mitigate risks of potential complications that could arise were the requirements for consent to be "informed" and "specific" to denote a high threshold.

58. Proposal 11.3 is to 'expressly recognize the ability to withdraw consent, and to do so in a manner as easily as the provision of consent. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.'

59. This proposal should only be further contemplated with substantial carveouts or exceptions.

60. One of our concerns is businesses ability to retain data originally collected with consent that is needed for legitimate commercial and public interest purposes and to allow for compliance with other legislative regimes that require retention of information in certain circumstances as set out in legislation.

61. Here we refer back to our concerns with proposal 4.10 and in that example the need to maintain data collected in relation to facilities asset and maintenance systems for legal and insurance compliance purposes.

62. These matters are already contemplated under the GDPR, where the controller of information can refuse to cease processing data upon the exercise of the right to object by the data subject if "the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims": Article 21 GDPR. These two exceptions—compelling legitimate grounds, and the establishment, exercise or defence of legal claims—would also need to be included alongside any right to withdraw consent.

63. Proposal 11.4 would require APP entities that provide online services to ensure that any privacy settings are "clear and easily accessible for service users". ACCI is not opposed to this proposal.

Australian Chamber of Commerce and Industry

Organisational Accountability

64. Proposal 15.1 would require APP entities to determine and record the purposes for which it will collect, use and disclose personal information at or before the time of collection. ACCI is not necessarily opposed to this proposal if the threshold for satisfying the requirement is low. APP entities should not be required to record the purposes for which personal information is being collected, used, or disclosed, in a separate or isolated document. It should be sufficient to have in writing somewhere a clear indication of the intended purpose. For example, this could be merely an email between two senior employees when the decision to interact with the personal information is made.

65. Proposal 15.2 is to 'expressly require that APP entities appoint or designate a senior employee responsible for privacy within the entity. This may be an existing member of staff of the APP entity who also undertakes other duties.'

66. We are opposed to this and primarily concerned with the practicality and the impact this proposal will have on SMEs and emphasise the report's assertion that "consideration should be given to excepting or modifying this requirement for some small APP entities that are covered by the Act where they are less able to absorb its associated regulatory costs."

67. We would propose that small businesses be exempted from this proposal.

68. If the proposal progresses as articulated, then we would encourage further consultation on how best this could be implemented for small businesses with a sufficient transitional period applied and additional guidance.

Direct Right of Action

69. In relation to a direct right of action, the Privacy Act Review Report recommended that:

> 26.1 Amend the Act to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy. The model should incorporate the appropriate design elements discussed in [Chapter 26].

70. Chapter 26 proposed the following design elements of this right of action:

> The Act should be amended to permit individuals to apply to the courts for relief in relation to an interference with privacy with the following design elements:
>
> (a) The action would be available to any individual or group of individuals who have suffered loss or damage as a result of privacy interference by an APP entity. This would include claims by representative groups on behalf of members affected by breaches of the Act.
>
> (b) Loss or damage would need to be established within the existing meaning of the Act, including injury to the person's feelings or humiliation.
>
> (c) The action would be heard by the Federal Court or the FCFCOA.
>
> (d) The claimant would first need to make a complaint to the OAIC and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme.
>
> (e) Where the IC or an EDR is satisfied there is no reasonable likelihood that the complaint will be resolved by conciliation or the IC decides a complaint is unsuitable for conciliation, the complainant would have the option to pursue the matter further in court.
>
> (f) In cases where the IC has decided that a complaint is unsuitable for conciliation on the basis that the complaint does not involve an interference with privacy or is frivolous or vexatious, the complainant should be required to seek leave of the court to bring an application in the court.
>
> (g) The OAIC would have the ability to appear as amicus curiae or to intervene in proceedings instituted under the Privacy Act, with leave of the court.
>
> (h) Remedies available under this right would be any order the court sees fit, including any amount of damages.
>
> Appropriate resources should be provided to the Courts to deal with these new functions.

71. This part of the submissions will first address the overall policy intent of the direct right of action, followed by an examination of each design element of the proposal.

72. In summary, ACCI:

a. remains unpersuaded that the introduction of a direct right of action has been sufficiently justified;

b. contends that the priority for improving the privacy enforcement framework should be to increase the resourcing of the OAIC;

c. contends that if the proposal to introduce a direct right of action is adopted, the proposal to introduce a statutory tort cannot be simultaneously adopted; and

d. considers that the primary flaw with the design elements of the proposed direct right of action is the gateway which would enliven the right, which could be improved by requiring the complaint to be first investigated by the OAIC and determined as possessing some evidentiary basis.

Policy intent

73. The introduction of a direct right of action for individuals has not been justified. While the potential benefits of a direct right of action would include that it would perhaps "enhance individuals' control of their personal information", "reflect current community expectations", "increase the avenues available to individuals who suffer loss as a result of an interference with privacy to seek compensation", "increase consumers' bargaining power with businesses that collect and use their personal information" are acknowledged, ACCI is unconvinced that these arguments outweigh the problems with the proposal.

74. Introducing a direct right of action for individuals will increase the privacy law compliance costs for businesses. It will heighten the risk of litigation for breaches of privacy law for businesses. Employers will be more exposed to unmeritorious or speculative claims, given that they are more likely to be pursued by individuals than the OAIC. These factors tend strongly against any supposed justification for the introduction for a direct right of action and it is not clear that they have been adequately taken into account.

75. Additionally, it has not been shown that the existing system, whereby the regulator plays the central role in enforcement and the pursuit of claims, is inadequate. Significant flaws in the existing system of allowing the Commissioner to make determinations following investigated complaints,[16] which are enforceable by the courts,[17] have not been identified. Importantly, this system prevents vexatious or frivolous claims from being pursued.

76. If the deficiency in the existing system is that the regulator is not sufficiently pursuing its own actions or investigation complaints, then this should be rectified without an overhaul of the enforcement framework. This failure of the regulator to pursue claims, if factual, is likely due to inadequate resourcing. The Information Commissioner reportedly requested greater funding from the Attorney-General in September last year.[18]

77. ACCI contends that given this problem should be rectified before the introduction of a direct right of action is considered. Followingly, ACCI would be interested in engaging with detailed consultation about the proposal and the purported bases as to why the right of action should be introduced, in spite of the increased costs to businesses.

78. Nevertheless, ACCI will engage with the various design elements below but stresses that, as is discussed in the next section, a direct right of action cannot be introduced in addition to a statutory tort. There should only be one new cause of action introduced and the direct right of action is a far more manageable avenue for businesses because it will only be enlivened following breaches to their obligations under the *Privacy Act 1988*, rather than "cover the field".

[16] *Privacy Act 1988* (Cth) s 52.
[17] Ibid s 55A.
[18] Sean Parnell, '"Unable to keep up": Information Commissioner issues budget warning', *Brisbane Times* (online, 2 September 2022).

Standing to exercise the right

79. Were a direct right of action to be introduced, ACCI has reservations about representative groups bringing claims on behalf of individuals; however, the consent requirement expressed in the Report mitigates some of these concerns. All representative actions under the direct right of action must operate on an 'opt-in' basis, even if affected individuals are financial members of the representative body.

Forum

80. ACCI agrees with the Report's proposal that, were a direct right of action to be introduced, the Federal Court or the FCFCOA would be the appropriate forums.

Gateway to enliven right

81. The Report proposes that the gateway to enliven the direct right of action should be that a complaint must be first made to the OAIC, which is then assessed for conciliation, after which the individual could elect to initiate court action either:

- instead of pursuing conciliation
- after conciliation has proven unsuccessful
- where the OAIC has determined the matter not suitable for conciliation, or
- where the OAIC has terminated the matter

82. ACCI sees issues with this proposed gateway. This process would allow the individual to commence litigation too quickly without the merits of the claim being first assessed. This would potentially expose businesses to vexatious, frivolous and unmeritorious claims.

83. Instead, individuals should only be able to exercise the direct right of action after the complaint has been investigated by the OAIC and the claim determined as possessing some evidentiary basis. Once this has occurred, the individual should only then have the option of commencing court action. This would prevent unmeritorious claims from being pursued and ensure that the OAIC's investigative functions are exercised.

Harm threshold

84. ACCI has concerns about a requirement that injury to an individual's feelings or humiliation would be sufficient to constitute loss or damage for which the direct right of action could be pursued. The effect of this would be that remedies sought by the plaintiff would be entirely for non-pecuniary losses. The financial cost of emotional distress is difficult to quantify and risks resulting in awards of damages that far exceed what a business would reasonably expect.

Role of the OAIC

85. ACCI agrees that the OAIC should be permitted to appear as either amicus curiae or an intervener in a claim brought under direct right of action.

Remedies

86. ACCI contends that the courts should only be able to award amounts of damages under a direct right of action that compensate individuals for pecuniary losses, for the reasons mentioned above.

87. Otherwise, ACCI is not opposed to the court having a wide discretion with respect to what remedies can be awarded.

Statutory Tort

88. In relation to a proposed statutory tort, the Privacy Act Review Report recommended that:

> 27.1 Introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123. Consult with the states and territories on implementation to ensure a consistent national approach.

89. This part of the submission will respond to the purported justification for the introduction of a statutory tort for serious invasions of privacy.

90. In summary, ACCI contends that the proposal for the introduction a statutory tort has not been justified and should not be considered, particularly in light of the proposal to introduce a direct right of action.

Purported need

91. The need for a statutory tort of privacy has not been justified. Unlike for the direct right of action, ACCI does not believe that the statutory tort should be given further consideration, even after other improvements are made to the existing system.

92. The case for the statutory tort was not made out by the Privacy Act Review Report. Even if strong arguments were advanced in its favour, ACCI would oppose its introduction given that another cause of action—the direct right of action—is being considered and is more appropriate.

93. The context within which various law reform commissions recommended the introduction of a statutory tort must be recalled. The ALRC's report that designed the model of the statutory tort which the Privacy Act Review Report recommends "was asked to design a cause of action, rather than to determine whether it is needed or desirable".[19]

94. The introduction of a statutory tort was deemed desirable by three prior law reform inquiries. In each of those inquiries, the statutory tort was considered in isolation from recommendations to introduce a direct right of action, even if comparisons between the two as different options were made. As such, the conclusion that a statutory tort was necessary was inevitably impacted largely by the lack of a right of action for individuals to pursue claims in response to breaches of their privacy.

95. In contrast, the Privacy Act Review Report recommends the introduction of *both* a direct right of action and statutory tort. This is unnecessary. The introduction of a direct right of action fulfills the central purpose of a statutory tort for invasions of privacy, which is to provide a cause of action for individuals; the model of a broad tort was simply considered the best means for achieving this. For example, the ALRC's report, *For Your Information*, consistently discussed the proposal for a "statutory cause of action" generally, rather than precisely a statutory *tort* throughout.[20]

[19] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Final Report, No 123, June 2014) ("ALRC 123") [1.17].
[20] See generally Australian Law Reform Commission, *For Your Information* (Report,

96. It may be accepted that these law reform inquiries primarily examined statutory causes of action that would 'cover the field' in terms of the protection gaps that exist under the *Privacy Act 1988*; nevertheless, they were not considered with an understanding that a direct right of action would be introduced. If proposal 26.1 is to be accepted, even if in a modified form, and a direct right of action is introduced, the justification for a statutory tort will be significantly mitigated.

97. In that context, the entire purpose of the statutory tort will be to fill the "gaps" left by the *Privacy Act 1988*. ACCI submits that a cause of action introduced solely for this purpose is unwarranted.

98. The "gaps" in the coverage of the *Privacy Act 1988* have a strong policy basis, which is why they exist in the first place. For example, despite proposal 6.1 recommending its removal, the "gap" created by the small business exemption is justified by the lesser capacity for compliance with complex privacy law that is characteristic of small businesses. The "gap" created by the employee records exemption has a sound policy basis in the more appropriate statutory regime for regulating the protection of this information existing under the workplace relations system. ACCI does not agree that, were the direct right of action to be introduced, a second cause of action that will distinctively apply to employee records, small businesses, and other actions excluded from the coverage of the *Privacy Act 1988*, ought to be introduced.

99. Furthermore, a cause of action that is "designed to cover the field" and operate adjacently to existing privacy law will be highly challenging for businesses. There should not be a risk that, were a business to be fully compliant with the *Privacy Act 1988*, state and territory privacy laws, and the common law (such as the doctrine of breach of confidence), it could still be found liable for breaches of privacy. Businesses need to be able to identify and understand its compliance obligations, which will be undermined by a statutory tort that exists alongside these legislative regimes.

100. These challenges are compounded by the constantly evolution of the digital systems for which businesses are required to manage their privacy obligations. Businesses, particularly those of a smaller size, are unlikely to be capable of contemplating and then managing all risks of liability under a statutory tort that "covers the field" for new digital systems, in addition to those that exist due to potential breaches of the *Privacy Act 1988*.

101. For these reasons, a statutory tort for breaches of privacy cannot be considered alongside the introduction of a direct right of action under the *Privacy Act 1988*. The choice must be between the two causes of actions and the Commonwealth should prefer a cause of action that works in tandem with, not adjacent to, businesses' obligations under the *Privacy Act 1988*. Only the direct right of action is able to do so.

Other proposals

Objects of the Act

102. ACCI supports amending the objects of the *Privacy Act* 1988 to clarify that it is about the protection of personal information and to recognise the public interest in protecting privacy.

Flexibility of the APPs

103. ACCI is broadly supportive of proposals 5.1, 5.2, 5.3, 5.4, and 5.5. Improvements to the APP codes should assist APP entities in their compliance with the privacy regime.

Political exemption

104. ACCI does not represent political entities. ACCI does not therefore wish to make any submissions in respect of the proposals relating to the political exemption.

Journalism exemption

105. ACCI does not represent journalistic organisations. ACCI does not therefore wish to make any submissions in respect of the proposals relating to the journalism exemption.

Privacy policies and collection notices

106. Proposal 10.1 recommends to "Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise, and understandable." ACCI does not oppose this proposal and welcomes the decision to substitute the phrase "up-to-date" in place of "current", noting the issues raised in the Report relating to the intention for collection notices to only need to be updated when practices change.[21]

107. Proposal 10.2 recommends that the following new matters should be included in a collection notice:

- if the entity collects, uses or discloses personal information for a high privacy risk activity —the circumstances of that collection, use or disclosure
- that the APP privacy policy contains details on how to exercise any applicable Rights of the Individual, and
- the types of personal information that may be disclosed to overseas recipients.

108. ACCI is unconvinced that these new matters to be included in collection notices are entirely necessary. Nevertheless, ACCI does not oppose this proposal given that the additional regulatory burden is unlikely to be significant and sees some added utility in bringing businesses' attention to these aspects of privacy law when preparing the collection notice.

[21] Report 96.

109. Proposal 10.3 recommends the development of standardised templates and layouts for privacy policies and collection notices. ACCI strongly supports this recommendation and contends that it will significantly assist businesses in their compliance. This is particularly the case in light of proposal 10.2 which will impose greater obligations on employers with respect to the content of collection notices.

Fair and reasonable personal information handling

110. Proposals 12.1, 12.2, and 12.3 would introduce a "fair and reasonable" test for the collection, use and disclosure of personal information.

111. Given that both "fairness" and "reasonableness" are prevalent concepts in Australian law, ACCI is not overly concerned with these proposals.

112. ACCI considers proposal 12.2, which would introduce a non-exhaustive list of factors which would be considered when determining whether a collection, use or disclosure is fair and reasonable in the circumstances, to be of great utility. This will help guide laypersons in understanding how these terms may be understood and interpreted by the courts.

Additional protections

113. ACCI supports proposal 13.3 which would require the OAIC to develop practice-specific guidance for new technologies and emerging privacy risks.

Research

114. ACCI does not wish to make any submissions in respect of the proposals relating to the conduct of research.

Children

115. ACCI supports proposals 16.1, 16.2, 16.3, 16.4, and 16.5, which would improve privacy protections for children.

People experiencing vulnerability

116. ACCI supports proposals 17.1, 17.2, and 17.3, which would improve privacy protections for children.

Rights of the Individual

117. ACCI has concerns about the proposed rights for individuals under privacy law. The Commonwealth should remain cautious about the potential regulatory impact of these new individual rights before implementing them. An impact analysis of the proposals would be prudent.

118. ACCI considers the exceptions to the rights of individuals in proposal 18.6 to be appropriate. Further exceptions may be necessary, which could include where complying with the request would impose significant financial cost and provide limited benefit to the individual. This would be different to the exception for competing public interests because it would compare the competing private interests of the APP entity and the individual, taking into account the propensity for the exercise of some rights to be significantly costly, particularly in light of the Report's proposal to remove the small business exemption.

119. More broadly, ACCI contends that the introduction of new individual rights should not be the focus of privacy law reform. Instead, as indicated by proposal 3.1, the focus of privacy law should be about the *protection* of personal information, rather than the rights of individuals. If, on a particular issue, the creation of an individual right is considered to be the most effective means of protecting personal information while minimising the adverse regulatory impact, then the individual right may then be appropriate.

Automated decision making

120. ACCI does not intend to make any submissions with respect to automated decision making.

Direct marketing, targeting and trading

121. ACCI does not intend to make any submissions with respect to direct marketing.

Security, retention and destruction

122. It is necessary for both Commonwealth and state/territory governments to evaluate their data collection mandates on businesses. For instance, Group Training Providers are obligated to securely store the personal information of individuals who have completed their qualifications, so as to be able to match their identity if requested years or even decades later. This requirement imposes an undue responsibility on businesses to maintain the personal information of former students for extended periods, solely at the government's discretion. It would be more appropriate to establish a uniform identity verification standard, with the onus on the requester, thus relieving businesses of the obligation to retain such data.

Controllers and processors of personal information

123. ACCI does not intend to make any submissions with respect to APP entity controllers and APP entity processors because the small business exemption should not be removed.

Overseas data flows

124. ACCI does not intend to make any submissions with respect to overseas data flows.

CBPR and domestic certification

125. The Report made no proposals with respect to CBPR and domestic certification.

Enforcement

126. ACCI does not intend to make any submissions with respect to the enforcement proposals.

Notifiable data breaches scheme

127. Proposal 28.2 recommends introducing a 72 hour threshold for notification if there has been an eligible data breach. ACCI notes that a 72 hour time limit is very onerous for businesses to comply with, especially around public holidays. Small or medium businesses in particular would struggle to meet this time limit and we would reinforce that numerous reports point to businesses taking over 200 days for initial detection of an incident. Given this, we don't believe a strict 72 hour window for notification once aware would add a lot of value.

128. The detrimental impacts would likely outweigh any positives, such as potential significant impacts on insurance premiums and further strain on an already under-resourced cyber security capability in Australia to support this initiative.

129. It should be sufficient to require notification "as soon as practicable after the entity becomes so aware".

Interactions with other schemes

130. ACCI does not intend to make any submissions with respect to the specific proposals in this section.

131. We would raise however that there is concern about the interaction of proposal 4.10 with existing state and federal legislation. For example: NSW has the *Workplace Surveillance Act 2005* which sets out a regime surrounding consent for the installation and operation of workplace surveillance, which covers geolocation tracking. To have two systems of consent for the same technology will provide confusion for business as to which system to follow and if implemented lead to additional processes and costs associated with the introduction of this technology. Careful consideration and additional consultation is needed to ensure any interaction issues are clearly resolved for businesses seeking to comply.

132. In the context of any changes to the current Privacy Act provisions, we have concerns about Australia's alignment with other international standards, regulatory frameworks or commitments.

133. Whilst the review proposes consideration be given to the alignment of Australian domestic law with the requirements under the European Union's General Data Protection Regulation, serious consideration must be given to the potential implications for Australia's alignment with other standards or commitments. Research undertaken by APEC demonstrates the substantial number of cross-cutting initiatives internationally in relation to cross-border data flows, including the APEC Cross-Border Privacy Rules.[22] Australia is a participating economy in the CBPR system, alongside USA, Mexico, Japan, Canada, Singapore, the Republic of Korea, Chinese Taipei and the Philippines. Any consideration of alignment with EU General Data Protection Regulation must be mindful to avoid negative impacts on Australia's alignment with other international standards, including ISO standards, or contributing to regulatory fragmentation.

Further review

134. ACCI supports a statutory review of any amendments to the Act which implement the proposals in this Report within three years of the date of their commencement. The review should particularly take into account the impact on Australian businesses and the regulatory burden imposed on them.

[22] APEC Policy Support Unit, *Fostering an Enabling Policy and Regulatory Environment in APEC for Data Utilizing Businesses* (July 2019), https://www.apec.org/publications/2019/07/fostering-an-enabling-policy-and-regulatory-environment-in-apec-for-data-utilizing-businesses.

About ACCI

The Australian Chamber of Commerce and Industry represents hundreds of thousands of businesses in every state and territory and across all industries. Ranging from small and medium enterprises to the largest companies, our network employs millions of people.

ACCI strives to make Australia the best place in the world to do business – so that Australians have the jobs, living standards and opportunities to which they aspire.

We seek to create an environment in which businesspeople, employees and independent contractors can achieve their potential as part of a dynamic private sector. We encourage entrepreneurship and innovation to achieve prosperity, economic growth and jobs.

We focus on issues that impact on business, including economics, trade, workplace relations, work health and safety, and employment, education and training.

We advocate for Australian business in public debate and to policy decision-makers, including ministers, shadow ministers, other members of parliament, ministerial policy advisors, public servants, regulators and other national agencies. We represent Australian business in international forums.

We represent the broad interests of the private sector rather than individual clients or a narrow sectional interest.

ACCI Members

State and Territory Chambers

Industry Associations

Australian
Chamber of Commerce
and Industry