Governance Institute of Australia

T +61 2 23 5744 **F** +61 2 9232 7174

E info@governanceinstitute.com.au

Level 11, 10 Carrington Street,

Sydney NSW 2000

GPO Box 1594, Sydney NSW 2001

W governanceinstitute.com.au

31 March 2023

Attorney General's Department
Robert Garran Offices
3-5 National Circuit
BARTON ACT 2600

Dear Sirs,

Privacy Act Review Report 2022 (Report)

Governance Institute of Australia

Who we are

Governance Institute of Australia (Governance Institute) is a national professional association, advocating for our network of 43,000 governance and risk management professionals from the listed, unlisted, public, not-for-profit and charity sectors.

As the only Australian provider of chartered governance accreditation, we offer a range of short courses, certificates and postgraduate study. Our mission is to drive better governance in all organisations, which will in turn create a stronger, better society.

Our members have primary responsibility for developing and implementing governance frameworks in public listed, unlisted and private companies, as well as not-for-profit organisations and the public sector. They have a thorough working knowledge of the operations of the markets and the needs of investors. We regularly contribute to the formation of public policy through our interactions with Treasury, the Attorney General's Department, ASIC, APRA, ACCC, ASX, ACNC and the ATO.

Our activities in this area

Governance Institute members have a strong interest in digital technology policy and take the governance and risk management of privacy, data protection and cyber security in all sectors very seriously. As a membership organisation, we have advocated for some time for digital transformation and modernisation in many areas of corporate regulation, including supporting virtual and hybrid AGMs, digital document execution, digital shareholder communications, and the introduction of Director ID numbers. Many of our members work as governance and risk professionals in a range of organisations that are part of or connect with the digital economy, from the largest listed companies responsible for critical infrastructure to small

businesses and not-for-profits. They are experienced in considering the industry and economy-wide implications of data and technology governance, cyber security, and digital transformation.

Governance Institute is a founding member of the ASX Corporate Governance Council, which produces the leading Australian statement on corporate governance, the Corporate Governance Principles and Recommendations. Recommendation 7.2 of the 4th edition explicitly acknowledges the importance of an organisation's risk management framework dealing adequately with privacy and data breaches, cyber security risks, and digital disruption.[1] We strongly supported this inclusion. While the Corporate Governance Principles and Recommendations are directed at listed entities, they influence the governance practices of Australian organisations of all types and in all sectors.

We also produce a range of thought leadership and industry guidance in relevant areas. In recent years our Risk and Technology Policy Committee has published Good Governance Guides on the topics of cloud services, digital transformation, digital trust, technology strategy, technology governance, cyber security, data as an asset, and ethical use of artificial intelligence. Our 2020 Report on the future of the risk management professional identified cyber security, artificial intelligence and digital disruption as key trends likely to impact on risk management professionals by 2025.[2] In 2021, our Report on the future of the board, found that data privacy and cyber security as two of the biggest challenges associated with technological disruption facing boards of directors into the future.[3] We regularly contribute to a range of consultations on digital themes including Australia's 2020 Cyber Security Strategy and the Digital Australia Strategy 2030. Governance Institute also contributes to the international debate on digital technology and data governance issues in its capacity as a division of The Chartered Governance Institute (CGI), an international body with over 30,000 members worldwide.

Executive summary

- Governance Institute members welcome the opportunity to make this submission on the critical issue of privacy protection. We support the aims of the Government in working towards an enhanced privacy scheme that continues to protect consumers, keeps pace with rapid technological change, and promotes good governance and risk management in organisations.
- We acknowledge many of the proposals for reform outlined in the Report rely on the development of guidance by the OAIC and other agencies. We recommend that the Government commit to sufficient resourcing to allow this important task to be undertaken in a timely manner.
- We recommend that the Government consult further on any proposal to remove or lower the $3 million annual turnover exemption, including with the not-for-profit sector.
- We encourage all levels of government to coordinate to ensure better harmonisation between privacy, data breach, cyber security data sovereignty and critical infrastructure regulation.
- We recommend that the Government consider the potential unintended impacts of the introduction of direct action and tort of privacy.
- We strongly encourage the Government to collaborate and consult widely on the reforms that are proposed before they are introduced. If the changes are made at the same time this will be a major burden for business and the provision of appropriate guidance and transitional provisions will be significant in ensuring compliance.

[1] ASX 2019, Corporate Governance Principles and Recommendations 4th Edition, p. 27.
[2] Governance Institute, 2020, *Future of the Risk Management Professional*, p. 19.
[3] Governance Institute, 2021, *Future of the board*, p. 10.

- Governance Institute's members would welcome the provision of clear frameworks setting compliance with various obligations to reduce the burden on training, skills uplift and technology uplift confusion as this is something that can easily be centralised in Government.

General comments

Support and consultation

1. Governance Institute supports the key themes of the Report including, in particular the enhanced transparency for individuals in relation to the handling of their personal information as increased transparency builds societal trust and trust in organisations. Governance Institute considers that the removal of exemptions from the Act, and particularly the small business exemption is a proposal which needs significant government led work to ensure any change is not overly burdensome for small businesses. This would include broad consultation with various stakeholders and peak bodies representing various affected sectors, collaboration and the provision of comprehensive guidance, particularly for small businesses.

General economic factors

2. Governance Institute considers that any implementation of the proposals in the Report should consider and provide transitional provisions which take account the current and likely ongoing general economic factors. There has been for some time, is currently, and is likely to continue to be a shortage of skilled workers in Australia. The staff required to implement the privacy uplift under the proposals are unlikely to be available in any short-term timeframe. Any staff that are available will likely need significant training. Governance Institute recognises that this is a burden for businesses particularly if there are significant penalties for non-compliance. In this regard, the staging and implementation of any changes should take into account the likelihood that businesses may be constrained in obtaining and training the relevant staff to undertake the work required.

Complexity and interplay with other legislation

3. As governance professionals, our members are required to comply with often competing regulations. Information which may constitute information regulated by the Privacy Act may be required to be retained for particular periods under other Acts which may be in conflict with one another. Governance Institute recommends that prior to implementing any new law regarding data retention periods that the Government undertake and publish at a minimum a document which sets out the prescribed retention periods for personal information collected under various Commonwealth Laws. This would act as a guide for regulators and a guide for business and if it was made available before law was passed then it may be that there would be an opportunity to align some of the retention periods so as to remove conflicting obligations on business. Governance Institute appreciates that the advent of technology may mean that in the future less personal information is required to be collected as various identity verification methods may emerge, but currently those technologies do not exist and guidance around competing requirements is requested.

4. In addition to overlapping regulation in terms of retention periods, our members are also concerned with overlapping regulation and complementary issues being dealt with in a holistic way. One element of data security is cyber security and to the extent that this aligns with the obligation to keep personal information secure our members consider that at least for the purpose of removing the small business exemption, guidance and resources should be provided to small businesses to assist them to achieve compliance with the requirements of the privacy regime.

5. While it goes without saying that creating a single source of guidance is a far more cost-effective approach than each individual business having to take its own compliance journey, this is exacerbated

by competing retention requirements and, in the case of small businesses and in the current environment of scarce resources, the need for government to take the lead in providing retention period guidance is even more important.

Staged approach to consultation

6. At a number of points in the Report there is a commitment to consultation on various measures for a minimum of 40 days. Governance Institute's members consider that this period is insufficient and there should be multiple points at which consultation occurs. They would suggest that engaging with industry by way of roundtables and other forums will enable a range of potential issues to be uncovered before such time as legislation is drafted. This would be to the benefit of government, regulators, industry and individuals. It is suggested that a program of roundtables occur after an exposure draft of the actual legislation is released. This would give further scope to refine and improve the final law.

7. It is also recognised that it is likely that a number of separate but related issues will be subject to consultation concurrently or overlapping at or about the same time and this will increase the burden on business in making timely submissions. There should be a 'whole of review', timetabled approach to consultation.

8. Many parts of the Report make reference to the OAIC providing guidance to business. It is Governance Institute's view that this guidance would need to be publicly available well in advance of any law becoming operational to allow businesses to determine how they would best comply in understanding the legislation. We recommend the Government commit to allocating sufficient additional resources to the OAIC to undertake this work.

Technology and legacy systems

9. In order to comply with any enhanced privacy scheme it is likely that all businesses will need to invest in new systems and uplift existing systems. There is a cost attached to this which will need to be budgeted for by businesses and there is also the timeframe required to actually implement the uplift. Governance Institute recommends that any changes which potentially require an uplift to systems be given a minimum of two financial years to allow businesses to find the funds to invest in system changes and test and implement them. The time and cost of systems changes has been factored into legislative amendment programmes in other sectors. For example, the banking sector needed several years to uplift systems to comply with and be able to offer positive credit reporting, legislation that the banks themselves had proposed. Similarly, the Consumer Data Right has required uplifts with applications for accreditation being subject to the time and cost required to uplift systems.

10. Other sectors that are subject to heavy regulation may also require time to review and enhance system capabilities, such as insurance, utilities and organisations handling health information. This is a situation where the availability of skilled resources raised above needs also to be taken into consideration. The need for time to upgrade systems is a further reason why a 'whole of review', timetabled approach to consultation and implementation is required.

Clear frameworks

11. Increasingly organisations are being provided with clear frameworks that set out how compliance with various obligations is satisfied. Governance Institute believes that the government has an opportunity in this instance to provide clear frameworks to support changes and that such frameworks should be made available at the earliest possible stage to allow businesses to clarify and understand their obligations in this space.

Comments on specific proposals

3 Objects of the Act

Proposal 3.2 Amend the objects of the Act to recognise the public interest in protecting privacy.

Governance Institute supports this proposal but notes that, in the digital age, many business models legitimately rely on the collection and processing of personal information. Accordingly, the public interest in protecting privacy must always be balanced against the inevitable cost to business of complying with additional privacy regulations, particularly where such regulations may overlap or interact with other legislative regimes. The Act currently recognises the balancing of rights in section 2A(b). Our members consider that maintenance of a clear statement of balance in the objects of the Act is critical.

4 Personal Information

Proposal 4.6 Extend the following protections of the Privacy Act to de-identified information:

(a) APP 11.1 – require APP entities to take such steps as are reasonable in the circumstances to protect de-identified information:

(a) from misuse, interference and loss; and

(b) from unauthorised re-identification, access, modification or disclosure.

(b) APP 8 – require APP entities when disclosing de-identified information overseas to take steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to de-identified information, including ensuring that the receiving entity does not re-identify the information or further disclose the information in such a way as to undermine the effectiveness of the de-identification.

(c) Targeting proposals – the proposed regulation of content tailored to individuals should apply to de-identified information to the extent that it is used in that act or practice.

Our members recognise the potential risk that de-identified information could be re-identified when combined with data from other sources.

However, given that de-identified information is not personal information, our members consider that care needs to be taken when extending the APPs to de-identified information to ensure that organisations have certainty around when the information they handle will fall within this expanded scope.

Confusion can arise if the concept is defined in a nebulous or ambiguous way.

5 Flexibility of the APPs

Proposal 5.1 Amend the Act to give power to the Information Commissioner to make an APP code where the Attorney General has directed or approved that a code should be made:

(a) where it is in the public interest for a code to be developed, and

(b) where there is unlikely to be an appropriate industry representative to develop the code.

Our members support this proposal. Our members work in a wide range of sectors. In some sectors, particularly the time and resource poor charitable and not-for-profit sectors there may not be an appropriate industry representative that is capable of drafting an APP code.

They consider that this proposal would support those businesses to achieve compliance with the Act and is consistent with their other comments regarding the broad availability of guidance to businesses from government or the OAIC.

Proposal 5.5 Amend the Act to permit organisations to disclose personal information to state and territory authorities under an Emergency Declaration, provided the state or territory has enacted comparable privacy laws to the Commonwealth.

Governance Institute supports this proposal. The COVID pandemic and the natural disasters that have occurred in recent years (for example, the 2019 bushfires and 2022 floods) created a great deal of uncertainty for businesses and, in some cases, businesses were unnecessarily restricted from sharing information with government authorities.

Our members support this proposal on the basis that it would reduce friction for businesses during natural disasters and other similar emergencies. Although our members note that the General Data Protection Regulation (GDPR) has a clause discussing emergencies. Article 23 of the GDPR allows member states to restrict certain individual rights under specific conditions in order to safeguard important objectives of general public interest, including the protection of public security and national security. Article 23(1)(e) of the GDPR allows member states to restrict certain individual rights, such as the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, and the right to data portability, if such restrictions are necessary and proportionate to protect public security in the event of a natural or man-made disaster or an emergency situation.

It is important to note that any such restrictions must be necessary, proportionate and subject to appropriate safeguards in order to protect the fundamental rights and freedoms of individuals. Additionally, the GDPR requires member states to put in place adequate and effective measures to ensure that any personal data processing that takes place during an emergency situation is lawful and compliant with the regulation. Our members consider these would be important safeguards.

6 Small business exemption

Proposal 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.

Proposal 6.2 In the short term:

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

(b) remove the exemption from the Act for small businesses that obtain consent to trade in personal information.

Privacy law is a highly specialised area that is challenging for smaller businesses and not-for-profits to navigate and comply with.

As at 30 June 2021 there were 2,288,441 Australian businesses with revenue under $3 million and hence generally outside the Act's scope and application.[4] However, as also set out in the Report, there are many categories of small businesses to which the Act applies by virtue of the nature of personal information held, for example, health service providers, or the nature of the business, for example, operators of a residential tenancy database. This exemption also applies to many not-for-profits, which are often even less capable than their commercial counterparts to comply with onerous levels of regulation.

We note that one of the objects of the Australian charities regulator, the Australian Charities and Not-for-profits Commission's (ACNC), statutory objects is promoting the reduction of unnecessary regulatory burden on the sector. The ACNC actively promotes activities directed at achieving this object. Governance Institute is a founding member of the #FixFundraising advocacy campaign that is urging a reduction in regulatory complexity in the area of charitable fundraising law.

Our members are pleased to note that the Commonwealth Government is working with the states and territories on reform in this area. At the same time as regulations are improved in one area, we would not want to see smaller charities and not-for-profits subjected to unnecessarily onerous levels of regulation in another area.

We agree that the small business and not-for-profit sectors need to play a part in economy-wide efforts to promote Australia's cyber security posture and prevent privacy breaches. We have noted elsewhere in this submission that reducing complexity of regulation of privacy including the number of laws that cover common subject matter and the number of regulators that cover common subject matter is an approach that should be considered. It is our view that removing the small business exemption for small businesses and not-for-profits would bring them and their treatment of personal information into line with community expectations, and other businesses, thus reducing complexity for both businesses and for individuals in understanding how their information is protected.

In addition, we note that in a number of places in the Report it is proposed the OAIC provide support and guidance for business. It is our view that this support and guidance could be made available to the small business and not-for-profit sector to allow them to comply with the Privacy Act. As has been pointed out by the OAIC in its submission, in 2021 56 per cent of cyber security incidents involved small businesses with less than 1,000 employees. Given the prevalence of cyber security incidents in small businesses, compliance with best practice personal information handling would be recommended. This is further necessitated by the move towards a digital economy. In addition, it would also be useful to consider the need for a consistent definition of what constitutes a 'small business'. As noted above under General Comments conflicting and overlapping definitions in many areas are a source of confusion. A consistent definition of what constitutes a 'small business' would assist this sector understand their obligations.

Section 6.5 of the Report sets out a range of support that could be provided to small businesses and not-for-profits to support the transition and provides examples of overseas initiatives which could be replicated here as well as suggestions made by a number of submissions to the review.

Our members consider that such resources should be prepared and made available to small businesses to support them and that an appropriate transition phase be implemented for these small businesses.

In conjunction with this phased transition our members consider that consultation prior to implementation of the legislation removing the exemption could be held with industry and stakeholders such as representative bodies to ensure that the guidance and materials were appropriate.

[4] As cited at p 67 of the report based on Estimate prepared for the OAIC using ABS counts of Australian Businesses, including entries and exits.

A number of submitters to the Report identified that small businesses were the 'weakest link' in supply chains and given the complexity of supply chains in the modern economy - this is another reason to move small businesses into the Privacy Act regime for protecting personal information.

There is an opportunity for the Australian Cyber Security Centre, which already has some resources, to do more in this area for small businesses. We acknowledge, as noted in the Report, that Australia's exemption for small organisations is not replicated in other comparable jurisdictions and that some have argued keeping the exemption in place may be a barrier to a GDPR adequacy decision.

These are valid concerns that warrant further investigation.

Our members note with approval that, as part of the development of the Australian Cyber Security Strategy, the Department of Home Affairs is currently consulting on opportunities to assist small businesses to manage their cyber security risks.

In any event, Governance Institute agrees that, in light of the general economic factors and the burden on small businesses, any restriction of the small business exemption should only be implemented on a staged basis and subject to the provision of appropriate guidance.

10 Privacy policies and collection notices

Proposal 10.3 Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP codes that may apply to particular sectors or personal information-handling practices.

Governance Institute supports this proposal on the basis that it would reduce the cost to business of developing a privacy policy and would be a meaningful method of supporting small businesses to comply with the APPs and the Act more generally.

11 Consent and privacy default settings

Proposal 11.2 The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context. Consideration could be given to further progressing standardised consents as part of any future APP codes.

Governance Institute has previously argued that informed consent is 'vital to upholding contractual rights and mitigating risks to potential breaches of privacy, misuse of personal data and other dangers unique to the digital economy' and advocated for the need for terms and conditions to be more accessible.[5]

Governance Institute's members note the ACCC's earlier comments on the 'privacy paradox', defined as the 'perceived discrepancy between the strong privacy concerns voiced by consumers who, paradoxically, do not appear to make choices that prioritise privacy'.

Our members consider that Australians do generally care strongly about their privacy but are often incapable of giving effect to these concerns, generally due to the complexity of terms and conditions used under the current consent model, which often lack clarity and precision. It is often impractical for consumers to opt out of using popular digital platforms and services despite any real and present concerns they may have over the use of their sensitive personal data.

[5] See Governance Institute of Australia 2021, Submission on Digital Australia Strategy 2030, pp. 7-8.

We believe there is a role for government, under an enhanced privacy scheme, to better enable informed consent through clearer and more accessible terms and conditions, but there is also an opportunity to further protect consumers by acknowledging the limits of informed consent in this context.

For these reasons, we agree there should not be an overreliance on notice and consent mechanisms.

Proposal 11.3 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.

Governance Institute supports this proposal in principle, but refers to its concerns outlined in relation to Proposal 18.3 below.

In particular, we believe that there must be exemptions to the ability to withdraw consent, including to allow for data to be retained for legitimate commercial and public interest purposes and to allow for compliance with other legislative regimes that require retention of information in certain circumstances that are set out in these regimes.

The introduction of a right to withdraw consent would require a phased approach, as the software used by Australian organisations may not immediately allow for deletion capability.

12 Fair and reasonable personal information handling

Proposal 12.1 Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person.

Proposal 12.3 The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should apply irrespective of whether consent has been obtained. The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should not apply to exceptions in APPs 3.4 and 6.2. The reference to a 'fair means' of collection in APP 3.5 should be repealed.

Governance Institute supports this proposal, subject to ensuring sufficient guidance is available regarding what is fair and reasonable.

The extension of the principles-based regulatory approach ensures that businesses are able to assess what is fair and reasonable in the circumstances of their own business model and data practices.

13 Additional protections

Proposal 13.1 APP entities must conduct a Privacy Impact Assessment for activities with high privacy risks.

(a) A Privacy Impact Assessment should be undertaken prior to the commencement of the high-risk activity.

(b) An entity should be required to produce a Privacy Impact Assessment to the OAIC on request.

The Act should provide that a high privacy risk activity is one that is 'likely to have a significant impact on the privacy of individuals'. OAIC guidance should be developed which articulates factors that that may indicate a high privacy risk, and provides examples of activities that will generally require a Privacy Impact Assessment to be completed. Specific high risk practices could also be set out in the Act.

Governance Institute recognises the need for businesses to ensure that projects are privacy-protective. This must be balanced against the regulatory burden and cost of compliance that is imposed on businesses.

If this requirement is implemented, we urge the Government to take particular care in drafting the legislation to ensure that the situations in which a Privacy Impact Assessment (PIA) is required are clear and unambiguous and that guidance is available to the business community. For example, in the digital age where most business models depend to some extent on the use of data, any number of activities could arguably be 'likely to have a significant impact on the privacy of individuals'.

We propose that the legislation or supporting regulations should include a non-exhaustive list of the circumstances in which an activity might be likely to have a significant impact on the privacy of individuals. Governance Institute supports the OAIC developing guidance for businesses to assist in defining those high-risk activities. We urge the Government to ensure that any such guidance is released before this requirement commences.

Governance Institute also emphasises that this proposal would require businesses to make a significant investment in resources and training for personnel conducting PIAs. If this proposal were to be implemented, it is the Governance Institute's view that a phased approach must be taken to ensure that businesses have the time to train their workforce and procure any additional resources as necessary.

Proposal 13.3 The OAIC should continue to develop practice-specific guidance for new technologies and emerging privacy risks. Practice-specific guidance could outline the OAIC's expectations for compliance with the Act when engaging in specific high-risk practices, including compliance with the fair and reasonable personal information handling test.

Governance Institute supports the development of practice-specific guidance by the OAIC to assist businesses to understand the OAIC's expectations for compliance with the Act.

It is our view that this guidance would need to be available well in advance of any law becoming operational to allow businesses to determine how they would best comply in understanding the legislation.

15. Organisational Accountability

Proposal 15.2 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.

This proposal would require businesses to, as a minimum, provide additional training to senior employees assuming this responsibility or, in some cases, recruit additional specialist personnel.

If this proposal is ultimately implemented, we propose the rule apply after a transitions period to allow for training/recruitment.

18. Rights of the Individual

Objection

Proposal 18.2 Introduce a right to object to the collection, use or disclosure of personal information. An APP entity must provide a written response to an objection with reasons.

Erasure

Proposal 18.3 Introduce a right to erasure with the following features:

(a) An individual may seek to exercise the right to erasure for any of their personal information.

(b) An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort.

Governance Institute supports in principle the introduction of these additional protective mechanisms.

It is important that Australians are able to enforce their privacy rights. However, these rights, especially the right to erasure, should not be absolute.

There should be exemptions, as there are under the GDPR, to allow for data to be retained for legitimate commercial and public interest purposes and to allow for compliance with other legislative regimes that require retention of information in certain circumstances that are set out in these regimes.

Good governance of an organisation may require the retention of certain kinds of data, including to comply with other regulations, for use in litigation, and to adequately respond to, and resolve, customer complaints.

The introduction of a right to erasure is likely to require a phased approach, as the current technology used by Australian organisations may not immediately allow for deletion capability. We refer to our previous comments (see page 4 above) regarding system uplift requirements. It should also be noted that erasure is likely to be highly challenging for particular sectors to implement.

19 Automated decision making

Proposal 19.1 Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights.

Governance Institute is mindful that the area of automated decision-making falls within a number of overlapping spheres of regulation, including artificial intelligence. Given the concurrent consultation on the regulation of artificial intelligence that is being undertaken by the Department of Industry, Science and Resources, Governance Institute urges any Privacy Act regulation and oversight to be consistent with other regimes to avoid any duplication or conflicting obligations on businesses.

21 Security, retention and destruction

Proposal 21.1 Amend APP 11.1 to state that 'reasonable steps' include technical and organisational measures.

Proposal 21.2 Include a set of baseline privacy outcomes under APP 11 and consult further with industry and government to determine these outcomes, informed by the development of the Government's 2023-2030 Australian Cyber Security Strategy.

Proposal 21.3 Enhance the OAIC guidance in relation to APP 11 on what reasonable steps are to secure personal information. The guidance that relates to cyber security could draw on technical advice from the Australian Cyber Security Centre.

The APPs currently recognise the importance of governance, risk management and culture to the protection of privacy.

APP 11.1 and 11.8 currently require organisations to take active measures, including adopting governance, culture and training strategies, where relevant, to ensure the security of personal information they hold.

This is appropriate, as Governance Institute is firmly of the view that cyber security and privacy protection go hand-in-hand as part of effective governance and risk management. However, it is also important that Australia's cyber security regulatory frameworks are cohesive, regulatory overlap is avoided, and that enforcement activities are overseen by agencies with appropriate expertise and resourcing.

Governance Institute supports in principle the addition of further clarity to APP 11. This is on the basis that it signals to organisations the critical importance of this principle and encourages organisations to continually improve their governance and risk management frameworks and cyber security posture.

However, we would discourage Government from taking a prescriptive approach via an enforceable code that requires organisations to put in place particular governance, risk management or cyber security systems and controls, given the pace of technological change and adaptation of organisations. The principles-based regulatory approach should be retained.

Our members also suggest that Government consider and consult further on whether the Australian Privacy Principles is the most appropriate place to mandate minimum cyber security standards. In Governance Institute's submission to the Department of Home Affairs on this issue, we recommended that any cyber security governance standards be voluntary not mandatory, to reduce regulatory compliance burden.

We also advocate that Government consider the potential for regulatory confusion if the OAIC, ASIC, APRA, the Department of Home Affairs, the Australian Signals Directorate and the Australian Cyber Security Centre were to operate simultaneously in the area of cyber security regulation, standards setting and awareness raising.

We consider there is a need for consolidation, not expansion, in this critical policy area.

23 Overseas data flows

Proposal 23.2 Introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a).

Governance Institute welcomes the Government's consideration of overseas data flows.

Many organisations now use cloud services that result in the transfer and/or storage of data to overseas jurisdictions. It is not always possible for organisations to specify data storage locations or contractually bind suppliers to comply with the APPs. Consequently, it can be challenging for organisations to comply with APP 8.

Adopting a more straightforward process that allows for the transfer of personal information and storage across borders would be more in line with how data actually flows in a digitally based, global economy.

To further facilitate the free flow of information across borders, Governance Institute supports in principle the introduction of a mechanism to prescribe countries and certification schemes that are substantially similar to the APPs. This would provide much needed clarity in respect of the overseas privacy and data protection laws that would satisfy APP 8.2(a) requirements.

It can be challenging for organisations to make such an assessment without obtaining specialist legal advice. There is an opportunity for the Australian Cyber Security Centre to do more in this area for small businesses; given it already has some resources.

Consideration could also be given to the introduction of a 'safe harbour' or similar concept to facilitate the transfer of personal information across borders to overseas jurisdictions with broadly equivalent privacy and data protection laws to Australian privacy laws.

Articulating minimum standards that organisations must comply with to disclose personal information to an overseas recipient would also encourage better privacy practices generally.

Proposal 23.3 Standard contractual clauses for use when transferring personal information overseas should be made available to APP entities.

Governance Institute supports consistency and guidelines wherever possible.

26 A direct right of action

Proposal 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 this chapter.

A direct right of action will need to be carefully balanced to prevent abuses of process, an unnecessary high case load on the court system, and a deterrent to doing business in Australia.

Any direct right of action should first require an individual to follow internal dispute resolution and external dispute resolution processes, such as via complaint to the OAIC and conciliation prior to instituting action, to avoid unnecessary costs to business.

27 Statutory tort

Proposal 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.

Governance Institute defers to legal experts as to whether it is appropriate to introduce a statutory tort of privacy.

A robust direct cause of action and a well-resourced Privacy Commissioner mitigates against the need for a statutory tort.

It is also important to note that proposals 26.1 and 27.1 may have unintended impacts on reporting under the NDB scheme, especially the proposals for a direct right of action and a tort of privacy. As noted in the next section there are now a range of mandatory notification and reporting schemes in operation in relation to data and security incidents and it is not necessarily clear how they interact. The introduction of a direct right of action and/or a statutory tort may have the unintended result of leading to organisations avoiding voluntary reporting where to do so might enliven a class of potential claims. We encourage the Government to consider these potential unintended impacts.

28 Notifiable data breaches (NDB) scheme – impact and effectiveness

Proposal 28.1 Undertake further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations.

Governance Institute broadly supports the current NDB scheme.

Our members believe that timely disclosure is important to drive best practice. However, they support calls for greater clarity and more regulatory guidance on the application of the NDB scheme, including practical examples of how to apply the threshold of 'serious harm'. Governance Institute members are aware of organisations facing practical challenges when attempting to interpret these provisions and understand their compliance obligations.

We also encourage Government to consider how it may increase the practical use of mandatory reports in threat intelligence gathering and awareness raising across industry.

Governance Institute's members support proposal 28.3 requiring organisations making breach notifications to include information on steps taken by way of remediation. They anticipate this will encourage organisations to strengthen their governance and risk management in relation to data and cyber security. This should be supported by regulatory guidance on best practice in these areas. However, the Government should consider the potential for this to reduce the timeliness of breach notifications.

It is important to note that mandatory notification and reporting schemes appear to have become a preferred regulatory tool for addressing a range of policy issues. The NDB scheme, modern slavery reporting, mandatory cyber incident reporting under Part 2B of the SOCI Act, and potential ransomware reporting are some examples.

We would urge Government to consider how these schemes interact. A scenario where organisations of all sizes are required to notify and report on an ever-widening array of issues may result in boards and management being distracted and taking a 'tick-box' approach to compliance, rather than being proactive in addressing underlying issues, building capability, enhancing security awareness and seizing opportunities to innovate. Our members consider that inconsistent and overlapping reporting requirements do not assist with improving compliance and transparency, especially when there is an obligation to act promptly and as a priority on speedy remediation when dealing with potential or actual data breaches and cyber security risks. This is a further reason why clarity around the applicable obligations and harmonisation between the various regimes is essential.

29 Interaction with state and territory privacy legislation

Proposal 29.3.3 Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.

Our members experience first hand on a daily basis the burden and confusion created by inconsistent Commonwealth and State legislation. As noted in our recent Submission on the review of the Electronic Transactions Act 'one of the key barriers to achieving leadership in digital economy regulation is the current inconsistent patchwork of legislative and administrative requirements'. Our members therefore support establishment of a state and territory working group to harmonise privacy laws.

Please contact me or Catherine Maxwell, GM Policy and Research if you have any questions in connection with this submission.

Yours faithfully,

Megan Motto

CEO