PRIVACY ACT REVIEW REPORT 2022

SUBMISSION

AISA

AUSTRALIAN INFORMATION SECURITY ASSOCIATION

COVERING LETTER

10.4.2023

Attorney-General's Department
4 National Circuit BARTON ACT 2600
By email: PrivacyActReview@ag.gov.au

Dear Attorney-General,

RE: AISA and ACLI's joint Submission to the Privacy Act Review Report 2022

We have attached a submission on the Privacy Act Review Report from our perspective as the peak professional bodies for information security and cyber security law in the region.

We have no objection to the publication of this submission, and no redactions are required prior to publication.

Thank you for the opportunity to contribute our views. Please do not hesitate to contact EJ Wise or me if you would like clarification of any of the comments made in this submission.

Sincerely,

Michael S. Trovato
Board Director, AISA
Mobile: +61 404 880 793
Email: Mike.Trovato@aisa.org.au

EJ Wise
Chairperson, ACLI
Mobile: +61 487 966 813

EXECUTIVE SUMMARY

AISA

The Australian Information Security Association (AISA) champions the development of a robust information security and privacy sector by building the capacity of professionals and advancing the cyber security and safety of the Australian public as well as businesses and governments in Australia. We welcome the Attorney General's request for submissions in response to the October 2021 Discussion Paper that canvases options and poses key questions for modernising Australia's *Privacy Act 1988.*

Established in 1999 as a nationally recognised and independent not-for-profit organisation and charity, AISA has become the recognised authority and industry body for information security, cyber security and security-related privacy matters in Australia. AISA caters to all domains of the information security industry with a particular focus on sharing expertise from the field at meetings, focus groups and networking opportunities around Australia.

AISA's vision is a world where all people, businesses and governments are educated about the risks and dangers of invasion of privacy, cyber-attack, and data theft and to enable them to take all reasonable precautions to protect themselves. AISA was created to provide leadership for the development, promotion, and improvement of our profession, and AISA's strategic plan calls for continued work in the areas of advocacy, diversity, education, and organisational excellence.

AISA submissions represent our 10,000+ strong member association, most are professionals in cyber security, information technology, and privacy, and allied professionals in legal, regulatory, financial, and prudential sector, as well as cyber and IT enthusiasts and students around Australia. AISA members are tasked with protecting and securing public and private sector organisations including national, state and local governments, ASX listed companies, large enterprises, NGO's as well as SME/SMBs across all industries, verticals and sectors.

AISA proactively works to achieve its mission along with its strategic partners. These include: the Australian Women in Security Network (AWSN); Australian Institute of Company Directors (AICD); Australian Security Industry Association Limited (ASIAL); grok academy; the Oceania Cyber Security Centre (OCSC); Risk Management Institute of Australia (RMIA); untapped; as well as international partner associations such as (ISC)^2, ISACA and the Association of Information Security Professionals (AISP). AISA also works closely with both federal and state / territory governments to ensure a robust and safe sector.

ACLI

The Australasian Cyber Law Institute (ACLI) is a community of legal and cyber professionals, educators and students within the region with a shared interest in cyber law. As a professional association of specialists who are passionate about the effective governance of cyberspace, we welcome the opportunity to make a submission in response to the Privacy Act Review – Report 2022.

Joint Submission

ACLI and AISA have reviewed and referenced the submissions and commentary of IIS Partners, Privcore, and Sallinger Privacy. As such, we hope that our views will be considered alongside those of our esteemed colleagues, as collectively we are working to ensure enhancements to Australian privacy law aimed at improving organisational privacy practice, empowering consumers, and protecting their data.

In this submission we have covered matters of particular interest to this stage of the privacy reform agenda, noting that our 2021 Issues Paper submission canvased at length many of the themes mapped into the present Discussion Paper, and the submission to the Privacy Act Review – Discussion Paper (October 2021), submitted October 2022.

PRIVACY ACT REVIEW REPORT OVERVIEW

The Report is the culmination of two years of extensive consultation and review of the Privacy Act 1988 (Cth) (Review of the Act). The Review examines the Act and its enforcement mechanisms in the context of a world where Australians now spend much of their lives online and their information is collected and widely used in the digital economy.

We commend the AG and Home Affairs for their ongoing effort toward the Review. The resulting Report contains hundreds of references to cyber, cyber security, or security and contains several hundred pages of summary, proposals, information related to consultations, and terms of reference. Overall, we support the amendment of the Act and sees this as a vital step toward Australia's digital future.

Following the recent major data breaches, cyber security and privacy are now viewed as inextricably interlinked. Those events highlighted the timely imperative to make changes to the Act and associated legislation and support further funding of regulators.

In this submission, we provide further comments in relation to some key security areas of interest which include: Definition of Personal Information; Exemptions; Security of Personal Information; Notifiable Data Breach scheme, and Funding.

CONCLUSION

We thank the Attorney-General for the opportunity to contribute to this phase of privacy law reform in Australia and would be pleased to discuss any aspect of our submission.

If you have any questions or need additional information, please do not hesitate to contact us.

TABLE OF CONTENTS

Submission

As noted in the Executive Summary the Report, it is the culmination of two years of extensive consultation and review of the Privacy Act 1988 (Cth) (Review of the Act).

The Review was instigated following the Australian Competition and Consumer Commission's (ACCC) 2019 Digital Platforms Inquiry final report (DPI Report) which made several privacy recommendations. The Review commenced in October 2020 with the release of an Issues Paper, followed by a Discussion Paper in 2021 which put forward proposals for reforming the Act for consultation. The Review has considered whether the Act and its enforcement mechanisms are fit for purpose in an environment where Australians now live much of their lives online and their information is collected and used for a myriad of purposes in the digital economy.

We commend AG and previously Home Affairs for the efforts put into the Review. The resulting Report contains hundreds of references to cyber, cyber security, or security and contains over 311 pages of summary, proposals, information related to consultations (that AISA has previously participated in), and terms of refences. Overall, AISA and ACLI support the amendment and modernisation of the Act in line with our recommendations within this document.

After the recent major data breaches, cyber security and privacy are truly "married". This makes changes to the Act and associated legislation, supporting codes, interrelated legislation, and funding of regulators and urgent and important initiative by government.

In this submission, we provide additional amplification of additional comments that are confined to some key areas of interest which include: Definition of Personal Information; Exemptions; Security of Personal Information; Notifiable Data Breach scheme, and Funding. Detailed recommendations per specific sections can be found in the "Detailed Proposal Submission" section of this document.

Definition of personal information

Overall, we agree that the definition of personal information in the Privacy Act sets the Act's regulatory parameters, since the Act is, in large part, constrained to regulating the collection and handling of personal information. As such, the scope of the definition has enormous implications for the Privacy Act and its effectiveness. Narrowing the definition in any way would risk excluding activities that seriously affect individual privacy.

The series 4 proposals outline several reforms to the definition of personal information. Largely, these proposals are 'clarifying amendments' in the sense that they add further certainty to the framing of the definition but do not substantially change the operation of the Act. We support the series 4 proposals, particularly proposals 4.1 and 4.6.

Exemptions

We broadly support removal of the Small Business, Employee Records, Political Acts and Practices and Journalism exemptions from the Privacy Act.

Small business exemption

We strongly recommended the removal of the small business exemption. We therefore support proposals 6.1 and 6.2. We agree, in line with proposal 6.1, that small businesses will need support to adjust their privacy practices and comply with the Privacy Act, hence why it is critical that the Office of the Australian Information Commissioner (OAIC) be appropriately resourced to offer that support.

We further believe that the efforts of the Australian Cyber Security Centre (ACSC) should be supported with adequate budget to support Small to Medium businesses (SMEs). https://www.cyber.gov.au/acsc/small-and-medium-businesses. It cannot be understated that messaging and communications with the SME sector needs to resonate with the time poor nature of that sector and delivery partners such as AISA, AICD and CPA Australia should be engaged to assist. It is also important to recognise that a one size fits all strategy of communication does not work across SMEs and messaging should be tuned to several business personas (e.g., sole traders, micro businesses etc.)

Employee records exemption

We recommend the exemption should be removed rather than subject to conditions and exceptions. Currently Australian Privacy Principles (APP) entities that are agencies must comply with the APPs in relation to their employee records. It is not clear why extending this coverage to the private sector would raise different or problematic considerations.

Political exemption

We support removal of the political exemption and therefore support the series 8 proposals. Political organisations should follow the same practices and principles that are required in the wider community. Imposing some of the requirements of the Privacy Act would not stop political parties collecting and using personal information but would apply appropriate guardrails to information handling.

Fair and Reasonable Test

The Review suggests the introduction of the fair and reasonable test to the Privacy Act as an objective standard which will apply irrespective of whether consent has been obtained (Proposal 12.1, 12.2 and 12.3).

We are not opposed to the implementation of these measures. Though we note that the list of proposed matters to be taken into account can be considered vague and may pose a potentially onerous test which introduces additional regulatory considerations requiring regulated entities to speculate regarding what might be expected by customers and a range of other matters. This is especially the case given Proposal 12.3, which significant expands the scope of its application in practice. As such, we stress the importance of providing detailed guidance coupled with consistent enforcement action to ensure a clear bar is set.

Additional Protections

The Review suggests the additional protections for certain high privacy risk activities, defined as activity that is 'likely to have a significant impact on the privacy of individuals'.

This includes the requirement to conduct a Privacy Impact Assessment (Proposal 13.1) with consideration given to how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted (Proposal 13.2). It further suggests the development of practice-specific guidance for new technologies and emerging privacy risks (Proposal 13.3) and introduction of a reasonable steps requirement in relation to third party data collections (Proposal 13.4).

We support these proposals with reference to the following clarifications.

OAIC need to be clear in defining the threshold for 'high privacy risk activities'. Given it is likely to be principles based, such a definition may impose an unnecessary burden on organisations who choose to default on the side of undertaking a privacy impact assessment on matters which may be safely handled within the existing framework. An indicative list of activities not captured in additional to the list of activities captured could be a useful guidance tool in mitigating this issue.

Security of personal information

Information security – whether in relation to boots on the ground or data in the cloud – is within the direct purview of AISA and its stakeholders.

Public discourse after the recent, large-scale data breaches in Australia have surfaced two common post-breach questions: *"Why was all this data retained and not removed?"* and *"Why was the data not better protected?"* The Australian Privacy Principle 11 aims to address both questions, as it deals with the protection and destruction of personal information under the title "Security of personal information". Although APP 11 requires that APP entities take such steps as are reasonable in the circumstances, our experience is that government and organisations alike struggle to understand what the Privacy Act intends as 'reasonable.'

Businesses have legitimate reasons to retain personal information. Firstly, personal information may be required to provide services to customers with an ongoing relationship. Secondly, an APP entity may be required to retain personal information as part of a document required by statute. Thirdly, personal information may form part of a record which is necessary for management of risk. For example, where service is being provided and there is a risk of the service recipient claiming negligence. Lastly, information may be retained because an organisation is on notice of a dispute. From a privacy point of view, the primary obligation an organisation must observe is to destroy or de-identify information which is not needed for any one of these four reasons. Further, the requirement to think about and declare personal information retention policies is likely to be a useful forcing function for organisations.

Essentially, APP 11 requires organisation to implement "reasonable" steps to protect, destroy or de-identify personal information (subject to any retention requirements). It comes with no surprise then, that the proposed amendments from the Privacy Act review aim to clarify and provide guidance on what 'reasonable' might mean. The Report section 'Security, Destruction and Retention of Personal Information' discusses the benefits and drawbacks of either amending the Act or updating the accompanying OIAC guidance and throughout the report weaves in the challenges of articulating 'reasonable' to be not prescriptive, technology neutral but still clear and useful. The section contains eight proposals.

The review suggests working out a **set of baseline privacy outcomes** (Proposal 21.2), clarifying that 'reasonable steps' **include organisational measures** in addition to just technical measures (Proposal 21.1) and specifying that even **de-identified data needs to be protected** (Proposal 21.4). We support these proposals.

In addition, the **OAIC guidelines** are to be further improved to what 'reasonable steps' might mean to **protect** (Proposal 21.3) and **destroy** (Proposal 21.5) personal information. AISA supports these proposals on the basis that careful consideration is given to exclude information: required for ordinary business purposes, that must be retained under statute, and for risk management and/or dispute resolution purposes from destruction and de-identification in relation to Proposal 21.5.

On the topic of retention, the review proposes that organisations establish their own **maximum and minimum retention periods for personal information** (Proposal 21.7) and **publish these in their privacy policy** (Proposal 21.8). In addition, the Commonwealth should review all legal provisions for retention requirements to ensure they appropriately balance their policy objectives with the privacy and cyber security risks (Proposal 21.6).

Broadly we **support these proposals.**

Security of Critical Infrastructure (SOCI) Act as a guide

The Critical Infrastructure Risk Management Program (CIRMP) has been recently put in force by Home Affairs and takes all hazards approach to material risks impacting the critical assets. Organisations with existing Critical Infrastructure assets will need to have a written CIRMP by 17 August 2023, including cyber and information security hazards. "A responsible entity must establish and maintain a process or system in the CIRMP to—as far as it is reasonably practicable to do so:

(a) minimise or eliminate any material risk of a cyber and information security hazard occurring; and
(b) mitigate the relevant impact of a cyber and information security hazard on the CI asset.

Although this guidance may not be appropriate for all organisations, such as SMBs, it is a starting and harmonisation point for a new guidance for all organisations.

Many have called for use of voluntary standards and the appeal is both that this is politically palatable, business friendly, and allows for greatest flexibility. Essentially this is what we have now, which many AISA and ACLI members would tend to agree has not worked that well – if it did, we would not be having the scale of service outages and data breaches we have today.

We offer the attached (Appendix) overview of standards for consideration. Ultimately the guidance should suggest a risk-based approach, aligned to the risk of data breach and serious harm. For larger organisations these kinds of frameworks must be considered.

For SMBs a tailored version of the ACSC Essential Eight, may be useful. AISA is drafting in consultation with business and director associations, the AISA Essential Eight Small Business and NFP Edition which will be released this year (2023).

Better guidance on what may be considered 'reasonable' for data protection, destruction and de-identification is recommended, but ultimately, enforcement action of OAIC will set the real bar.

The shared risks landscape

We are witnessing how data breaches have a direct impact to individuals. Interconnectivity and dependencies on service providers and individuals will only increase. Although the Report did not contain a discussion of Shared Risk, AG should look at increasing risk management requirements and obligations to help managed Shared Risks.

AISA and ACLI recommend AG to consult the Commonwealth Risks Management Policy [1] and consider the definition of 'shared risk' and consider the benefit of its inclusion and potential OAIC powers as an element of the Act.

According to the Department of Finance, shared risks are those risks extending beyond a single entity which emerges from a single source and impacts interrelated objectives of entities. A collaborative approach to managing shared risk is required to: identify accountability, nominate transparent roles and responsibilities, define risk appetite boundaries, and seek agreement between all parties. This may require extended application guidance for APP 11, in particular. Additional delays managing the risks of fourth parties may be encountered due to contractual uplift requirements with service providers.

[1] https://www.finance.gov.au/government/comcover/commonwealth-risk-managment-policy

The cyber security skilled gap and lack of standardised accreditation

AISA champions the development of a robust information security sector by building the capacity of professionals in Australia and advancing the cyber security and safety of Australian public as well as businesses and government in Australia. As part of the Australian Cyber Conference 2022, also known as CyberCon, in her opening speech, The Hon Clare O'Neil MP said:

"*The new Government in Australia has made the decision to have a cyber security minister because we want to elevate this issue to the level of importance that it so clearly is for Australia business, for Australia citizens and very much for our nation. Cyber is everything and it is everywhere. A resilient cyber ecosystem is going to be fundamental to our country's future. Cyber security underpins economic growth both here in Australia and across our region more broadly. It provides confidence in the services and infrastructure that enable business activity. It supports our economy, and it enables our way of life."*

AISA applauds the announcement but is also raises the following statistics of concern that APRA entities will have to confront:

The mismatch of job-ready cyber security and technology focused risk professionals will remain a key challenge. It is estimated that Australia may need around 30,000 additional cyber security workers for technical as well as non-technical positions by 2026. While there are challenges to solve at both the supply (education) and demand (hiring / employer) sides it is evident that remediation will take many years while the cost of obtaining and retaining cyber security, cloud and technology risk staff will continue to increase. While some proponents in the sector may say there is a skills shortage, AISA notes it is contacted daily by students who have completed their studies in tertiary education in cyber security and are unable to find meaningful work as the lack hands on work experience.

Support for industry accreditation is mixed and not sufficiently supported by industry leaders. Recent AISA Research into Cyber Security Accreditation in Australia [2] indicates that: (i) support for industry accreditation is mixed. Only 53.1 % of respondents support accreditation of the sector to ensure a base level of qualification and standard; and (ii) Industry leaders see accreditation of the cyber sector as unnecessary and complex to be inclusive. In addition, hiring managers consider a candidate's aptitude, attitude and work experience to be the most important when making hiring decisions. Industry certifications and educational background are deemed much less important when recruiting cyber security staff. A recent study conducted by AISA for the 2023-2030 cyber security strategy found that a majority of respondents in the sector support licensing / accreditation of cyber security providers (e.g. MSP / integrators and consulting businesses) as opposed to individuals.

Controllers and Processors

The Review is suggesting introducing the concepts of APP entity controllers and processors into the Privacy Act (Proposal 22.1).

We support the introduction of a controllers and processors distinction. As currently drafted the Privacy Act is difficult to apply to an entity that is receiving and managing information for a third party (a processor). Strictly speaking the processor organisation is required to be aware of the information that it is receiving and processing so that it can describe how it is managed in its privacy policy, to give collection notices to relevant data subjects enter permit access and inspection. In many cases these requirements are highly impracticable for a processing entity and in some cases work against restrictions on access and security that are intended to protect the relevant information.

[2] https://www.aisa.org.au/common/Uploaded%20files/PDF/Surveys/2022/AISA%20Accreditation%20Survey%20Report.pdf

AISA and ACLI support the introduction of the concept of a processor on condition that the controller include contractual provisions like those imposed on processors by the General Data protection Regulation (GDPR) in order to protect personal information.

Notifiable Data Breaches Scheme

As noted in our 2021 and 2022 responses on this topic, we believe compliance with the NDB Scheme is a complex and complicated business problem for government and organisations and requires skill and subject matter expertise to provide guidance. Organisations often ask us which requirements they should follow. As such anything that provides clarity (such as additional OAIC guidance) is desired and will be beneficial, both for improving organisational competence and reducing costs of compliance over time.

We strongly support proposal 28.1, to undertake further work to better facilitate the reporting processes for NBDs to assist both the OAIC and entities with multiple reporting obligations.

AISA and ACLI strongly support proposal 28.2 to:

- Amend paragraph 26WK(2)(b) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity, the entity must give a copy of the statement to the Commissioner as soon as practicable and not later than 72 hours after the entity becomes so aware, with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours. We note that the proposed 72-hour deadline is consistent with the notification requirements under the security of critical infrastructure framework.

- Amend subsection 26WL(3) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity, the entity must notify the individuals to whom the information relates as soon as practicable and where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases as soon as practicable.

- Require entities to take reasonable steps to implement practices, procedures, and systems to enable it to respond to a data breach.

We also support OAIC funding for more case studies and online learning modules based on the types of NDBs that have been reported so people can use them to learn what not to do or what to improve. Ideally this will bring to life the statistics on the OAIC website to highlight possible cyber security hygiene issues, issues with misconfiguration of systems, control failures, human errors, and the like.

Funding for regulators

AISA and ACLI believe that appropriate funding for the OAIC cannot wait.

It is imperative that the Government acts immediately on the discrepancy between the size of the challenge facing the OAIC and the resources at its disposal to meet that challenge.

Conclusion

We thank the Attorney-General for the opportunity to contribute to this phase of privacy law reform in Australia and would be pleased to discuss any aspect of our submission.

If you have any questions or need additional information, please do not hesitate to contact us.

Detailed Proposal Submissions

Clause	Proposal (in brief)	Position	Comments
3.2	Recognise the public interest in protecting privacy	Support	Implement this proposal as is.
4.1 (pt 1)	Change 'about' to 'relates to'	Support and note comments	It is critical for the design and operation of secure information systems that information be clearly identified and the responsibilities associated with different classes of information properly assigned. The proposal to change the word "about" to "relates to" fails to consider relevant privacy attributes of the different classes of information that might be captured. It is clear that when information is "about" an individual the individual may be concerned about that information and, therefore, it is reasonable to create a legal framework regarding its collection use and disclosure. However, there are many classes of information that "relate to" an individual which have no privacy implications. For example, general information about human physiology could be said to relate to a individual: the average body temperature, the average height, the range of shoe sizes that fit a person of a particular age. This general information can be said to "relate to an individual" but the collection of use of the information has no privacy implications. In an electronic system, whether or not communication is taking place over Wi-Fi, Bluetooth or 5G could in some cases be said to "relate to an individual" because the information is associated with device owned or used by the individual. However, it tells us nothing about the relevant person and has no privacy implications. In our submission the definition of personal information should retain the word "about". If a change is to be made it should include a definition and or examples that clearly establish that the information must describe the individual's behaviour, positions, attributes or history in order to be personal information.
4.1 (pt 2)	Include guidance about the meaning of 'relates to'	Amend	Remove from the relevant considerations: 'the extent to which the APP entity or a third party seeks to collect and use or is likely to use information to learn about or to evaluate an individual, or to treat them in a certain way, or seek to influence their behaviour or decisions'.

Clause	Proposal (in brief)	Position	Comments
4.2	List of examples	Amend	This list of examples should instead be described, in statute, as what ***would*** make an individual 'reasonably identifiable'. The list should also include data with a weakly-obfuscated individual identifier, data with a unique or near unique collection of demographics, and data with enough detail about the individual to identify them.
4.3	Definition of 'collect' to include inferred information	Support	Implement this proposal as is.
4.4	Entities to make own assessment about the 'reasonably identifiable' test	Amend	Amend the definition of personal information in the statute, to add: "An individual is 'reasonably identifiable' if they are capable of being distinguished from all others, even if their identity is not known." There has been some confusion in the Privacy community over which of these meanings applies with many advisers adopting the logical approach that intended meaning is "distinguished from a group" and others regarding systems that target or are customised to specific individuals as not regulated because the customised data cannot be linked to a name and address. In our view, the Act should be amended so that identified means distinguished from a group. Targeted web advertising which addresses an individual identified only by a cookie is considered regulated personal information under the GDPR because the targeted individual is distinguished from a group. This interpretation (with the limitation that the relevant individual needs to be about the individual) would provide a straightforward, privacy relevant, test which would encompass data linked to a particular individual through a persistent identifier without raising complex issues regarding when association of personal attribute information might describe Personal Identity.
4.5	Amend definition of 'deidentified'	Support and note comments	We agree in general terms with proposal 4.5. However, it is important that any clarification of the meaning of de-identification also consider our comments above in relation to the meaning of identify. For example, if a spreadsheet includes data relating to a set of individuals each of which is identified by a number but there is no way to link that number to a particular person or to recognise a person previously associated with that number if they come back in contact, provided the data itself is not personal identity information, the information may be said to be de-identified. The critical test is that any link between a natural person and listed information is broken in such a way that the data cannot be re-associated with the listed person.

Clause	Proposal (in brief)	Position	Comments
			Another issue that should be closely considered when coming up with a definition of de-identification is that some personal information describes attributes that are shared by a large group of individuals. For example, an entity might hold an individual identifier associated with the attribute: age group 20 to 35. There may be 10,000 people in the category of age group 20 to 35. Nevertheless, the information that my individual is in the age group 20 to 35 is still personal information and is not de-identified until or unless I remove the identifier, or I change my arrangements such that the description "age group 20 to 35" cannot be associated with the individual if they come back in contact.
4.6	Apply some APPs to deidentified data	Amend	This proposal will not be necessary if the 'reasonably identifiable' test is defined as we recommend above. Alternatively, fix this proposal to extend to disclosures under APP 6 as well. In our view it is going too far to create rules that apply to information which has no privacy impact by definition
4.7	Criminalise re-identification	Does not support	We do not support this proposal. We are not aware of any instances of malicious re-identification of deidentified information which would meet the test suggested. If information is de-identified it becomes personal information and subject to the existing privacy regime including collection notification obligations. An individual that re-identifies information would be subject to ordinary regulation under the Privacy Act and could be the subject of prosecution for breach of the Act if acting in breach of its requirements.
4.8	Prohibit re-identification by recipients	Amend	This proposal will not be necessary if the 'reasonably identifiable' test is defined as we recommend above. Alternatively, fix this proposal to avoid unintended consequences. The re identification of information will constitute a collection of personal information under the Privacy Act and will be subject to existing rules regarding collection, use, storage and disclosure. A general prohibition on re-identification could inhibit secure storage of information re-identified form which is capable of being re-identified when it is needed or becomes useful.
4.9	Sensitive information	Amend	Add to this proposal an additional protection, by removing 'that is to be used for the purpose of automated biometric verification or biometric identification' from the definition of 'biometric information'.
4.10	Geolocation tracking data	Amend	Include geolocation tracking data in the definition of sensitive information. Reconsider the definition of 'geolocation tracking data'.

Clause	Proposal (in brief)	Position	Comments
6.1	Small business exemption	Amend	Immediately abolish the small business exemption, apply a 12-month period for small businesses to prepare before any penalties apply. We support the removal of the small business exemption. If the protection of personal information is justified on public policy grounds it does not make logical sense for a large part of the Australian economy to be exempt from regulation. In addition, considering that small business does not have the resource is of larger businesses in the economy, the inclusion of small business within the regulatory framework may encourage the clarification and simplification of requirements to make them more practical and privacy impactful then is currently the case.
6.2	In the short term	Support	Consistent with our support for the removal of the small business exemption we support these proposals.
7.1	Employee records exemption	Amend	Abolish the employee records exemption but introduce limited exceptions to APPs 12 and 13.
8.1 – 8.5	Political parties exemption	Amend	Remove the political parties exemption but give tailored public interest exceptions to APPs 3, 6, 12 and 13.
8.6	OAIC guidance for political parties	Support	Implement this proposal as is.
9.1 – 9.5	Journalism exemption	Amend	Abolish the journalism exemption and replace it with a limited exemption to the collection, use and disclosure principles (APPs 3, 5 and 6) for activities necessary to the conduct of investigative and public interest journalism.
10.1	Clear, up-to-date, concise and understandable collection notices	Support and note comment	We note that APP5 does not literally require delivery of a collection notice. APP5 requires that the regulated entity take reasonable steps to ensure that an individual is aware of certain matters. We do not support any amendment which specifies the means by which communication of the matters in APP5 must take place. Also, it seems somewhat Inconsistent to insert a requirement that the matters to be communicated under APP5 must be "concise" when they are already largely irrelevant for most consumers, and it is proposed to increase the number of issues which must be addressed in a collection notification.
10.2	Matters to include in a notice	Support and note comments	We support the observation made in the discussion paper that consumers have notification fatigue. In our view, there is a benefit to advising consumers that a collection is being made or has been made of their personal information and letting them know the purpose of the collection. However, each of the other matters listed in APP 5.2 are of marginal interest to most consumers, create a regulatory burden on operating businesses and serve no useful purpose. We suggest that APP5 be replaced with an obligation to notify consumers that their information has been or is being

Clause	Proposal (in brief)	Position	Comments
			collected. the purpose of the collection and refers them to the organisation's privacy policy regarding other issues that may be of interest.
10.3	Standardised templates and layouts	Support and note comments	We support the prescription of standardised templates and layouts including standard terminology and icons where they are consistent with international frameworks and standards. To the maximum extent possible Australian privacy rules should be consistent with similar international frameworks and not adopt specific and unique requirements that are unnecessary and burdensome. In our submission, the Privacy Act should describe a framework which protects individual privacy rather than transforming into an extensive list of procedural and form prescriptions that create a unique and unnecessary compliance burden.
11.1	Definition of consent	Amend	Revert to Discussion Paper proposal 9.1: 'consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action'. Ensure consent cannot be tied to the provision of goods and services. Recognise a very narrow contractual necessity exemption to the requirement for consent to collect sensitive information.
11.2	Consent request design	Support and note comments	See our comments in relation to proposal 10.3.
11.3	Withdrawal of consent	Support	Implement this proposal as is.
11.4	Accessible privacy settings	Amend	Introduce a pro-privacy by default requirement.
12.1	Fair and reasonable test	Support and note comments	While it sounds worthy, the obligation to publish personal information handling practises in a privacy policy ensures that individual businesses are prepared to stand behind their information handling practises. It is not clear that any practise or procedure might change in light of this requirement and why it would be a necessary addition to the existing framework.
12.2	Fair and reasonable test matters	Amend	Include all matters in the Act itself, rather than the EM. Include vulnerability in the matters to consider. Clarify that these matters will also apply to the means of collection. As stated above in relation to proposal 12.1, the adoption of a fair and reasonable handling requirement needs to be clarified. The list of matters which is proposed to be considered demonstrates a view that this vague but potentially onerous test would introduce additional unnecessary regulatory considerations requiring regulated entities to speculate regarding what might be expected by customers and a range of other matters.

Clause	Proposal (in brief)	Position	Comments
			If there are particular activities or practises that would not pass the proposed criteria and have been observed by the OAIC as not being already prohibited by the existing privacy framework. Our submission is that they should be identified and specifically prohibited by amendment to the Act rather than imposing a broad and vague obligation of doubtful value on every regulated entity.
12.3 (pt.1)	Fair and reasonable test to apply even where consent was obtained	Support and note comments	See 12.1 and 12.2 above.
12.3 (pt.2)	Fair and reasonable test application to APPs 3.4 and 6.2	Amend	The fair and reasonable test should also apply to conduct authorised under APPs 3.4 and 6.2.
13.1	PIAs for high-risk activities	Amend	Ensure small businesses are captured within the requirements of this proposal. We support the requirement to undertake a privacy impact assessment in relation to changes that are likely to have "a significant impact on the privacy of individuals". Unfortunately, the test as to whether a change is likely to have a significant impact on the privacy of individuals is not defined in the discussion paper and when clarified is likely to be vague and principles based, giving rise to a tendency for organisations to misinterpret when a privacy impact assessment. When personal information is collected by a business for its functions or activities and handled securely and in accordance with its privacy policy the practical impact is very unlikely to have a significant impact on individual privacy. Changes to information handling practises should be also handled by notification of changes to an organisation privacy policy and, where relevant, a collection notification.
13.2	Enhanced risk assessments for FRT	Support	We support a cautious approach to the adoption and use of facial recognition technology and other biometrics. Noting that these technologies can be privacy enhancing to the extent that they can be task specific and potentially eliminate the need for personal information to be recorded and shared outside a discrete system. Also, the statistics on the error on biometric data tools mean that absolute reliance upon them is risky (i.e. many systems are not updated, their data set aged and not checked).
13.3	Practice-specific guidance for new technologies and emerging privacy risks	Support	We support the production of practise specific guidance by the OAIC.
13.4	Third party collection requirements	Support	We support this additional requirement.

Clause	Proposal (in brief)	Position	Comments
14.1	Broad consent for research	Amend	Any reforms in this area should be enabled as a clear and additional alternative to consent, as a ground on which a research activity can lawfully occur. This alternative legal pathway should only be enabled once an HREC has approved that use of the lower standard is appropriate and necessary in the circumstances (e.g., creation of biobanks, longitudinal or multi-use data assets).
14.2	Research permitted without consent	Support	We support this proposal.
14.3	Single exception for research without consent	Support	We support this proposal.
15.1	Organisational accountability	Amend	Organisations are required to anticipate the purposes for which they will collect use and disclose personal information when they prepare their Privacy Policies. Under existing law there is also a requirement to make a relevant notification under APP 5.2. An additional requirement that purposes be determined and recorded at or before the time of collection will either introduce a formality leading to the creation of documentation with wide scope and vague objectives of little practical use, or if strictly observed may become a burdensome and costly limitation on the ability of a business to change and adapt the way it users information collected for one purpose but now applied more broadly. We propose additional guidance be offered to allow for reasonableness test vs strict compliance.
15.2	Senior employee responsible for privacy	Support	We support the designation of a person responsible for privacy organisation on the basis that the individual is not personally liable or responsible for the organisation's implementation or compliance with the requirements of the Privacy Act. As you would appreciate decisions regarding the operation of an organisation are taken at board and senior executive level and cannot be made the responsibility of a single individual.
16.1	Define a child in the Act	Support	Implement this proposal as is.
16.2	Children's consent	Support	Implement this proposal as is.
16.3	Clear and understandable collection notices / privacy policies	Support	Implement this proposal as is.
16.4	Best interest of the child	Support	Implement this proposal as is.
16.5	Online privacy code	Oppose	Reject this proposal.
17.1	OAIC guidance on vulnerability	Support	Implement this proposal as is.

Clause	Proposal (in brief)	Position	Comments
17.2	Supported decision-making	Support	Implement this proposal as is.
17.3	Consult on acting on financial abuse	Support	Implement this proposal as is.
18.1	Access and explanation	Amend	Rephrase to state that unless an entity has incurred actual expenses over and above the reasonable processes that APP 1.2 would require them to implement to comply with this obligation, no fee should be charged.
18.2	Objection	Support	Implement this proposal as is.
18.3	Erasure	Support	Implement this proposal as is.
18.4	Correction	Support	Implement this proposal as is.
18.5	De-indexing	Support	Implement this proposal as is.
18.6	Exceptions	Amend	Explicitly state that 'rights should always continue to operate to the extent the balancing does not weigh against it'. Clarify 18.6(c) to ensure entities don't use poor process or system design to excuse not responding to individual requests.
18.7	Notification to individuals	Support and note comment	See our comment in relation to proposal 10.2. This information would be set out in a Privacy Policy and referenced in a collection notice.
18.8	Reasonable assistance	Support	Implement this proposal as is.
18.9	Reasonable steps to respond	Do not support	Compliance should not be based on a 'reasonable steps' test.
18.10	Acknowledgement of receipt	Support	Implement this proposal as is.
19.1	ADM in privacy policies	Support	Implement this proposal as is.
19.2	Indicators of decisions with a legal or similarly significant effect	Support	Implement this proposal as is.
19.3	Right to obtain meaningful information	Amend	Include a right to obtain a human review of a decision made by automated means.
20.1	Definitions of direct marketing, targeting, trading	Amend	Amend the proposed definitions.
20.2	Direct marketing opt-out	Amend	Clarify that the right extends to uses of personal information underpinning direct marketing. Add fair and reasonable test considerations.

Clause	Proposal (in brief)	Position	Comments
20.3	Targeting opt-out	Amend	In order to create proactive obligations on the APP entity (rather than reactive requirements of individuals), amend the definition of 'personal information' to include information where an individual may be singled out and acted upon, even if their identity is not known. (See also Proposal 4.4.) Operationalise this proposal by amending APP 6 to specify that targeting cannot be considered a primary purpose or related secondary purpose.
20.4	Trading	Amend	Operationalise this proposal by instead amending APP 6 to specify that trade in personal information cannot be considered a primary purpose or related secondary purpose. Specify that consent to trade in personal information cannot be tied to terms of service.
20.5	Direct marketing to children	Support	Implement this proposal as is.
20.6	Targeting to children	Amend	Specify that the child must have opted in to targeting. Prohibit targeting based on any sensitive information.
20.7	Trading in the personal information of children	Support	Implement this proposal as is.
20.8	Targeting – fair and reasonable test, prohibit targeting based on certain sensitive information	Amend	Entities should be required to comply with all APPs. Amend the definition of 'personal information' to include information where an individual may be singled out and acted upon, even if their identity is not known. (See also Proposal 4.4.). Prohibit targeting based on any sensitive information.
20.9	Information about targeting	Support	Implement this proposal as is.
21.1	'Reasonable steps' to include technical and organisational measures.	Support	We support this proposal. It is not a significant change.
21.2	Baseline privacy outcomes	Support and note comments	Cyber security aims to secure data but even the best systems can be compromised by zero-day, insider and sophisticated nation state attacks. Security officers can take reasonable steps to secure data, but they cannot guarantee outcomes.
21.3	Enhance APP 11 guidance	Support	We welcome proposal for publication of further guidance from the OAIC regarding the interpretation of APP11.
21.4	APP 11 requirements for deidentified information	Support and note comments	A primary purpose of de-identifying information is so that it becomes shareable and does not need to be secured. De-identification is used to ensure the protection of personal information. Extending obligations in the Act to cover de-identified information could expand the obligations of regulated entities in relation to data that has no relevant privacy significance.
21.5	Enhance APP 11.2 guidance	Support	We support this requirement on the basis that the OAIC take care to consider and exclude from required destruction or deidentification information is required for ordinary business

Clause	Proposal (in brief)	Position	Comments
			purposes, information that must be retained under statute, for risk management and/or dispute resolution purposes.
21.6	Review of retention provisions	Support	We support proposal 21.6. A review of data retention obligations across Commonwealth legislation with a view to establishing a consistent framework clearly identifying the information that must be retained and, subject to business and legal requirements information which can be destroyed would be of great assistance to industry. We suggest that the review should also take into account the need to retain copies of identification records in circumstances where providers might make use of Trusted Digital Identity Frameworks (TDIF) with a view to establishing procedures for customer authentication but do not require the maintenance and retention of records that may pose a high risk to personal privacy. The review should also consider whether and in what circumstances identity theft is taking place in the Australian economy and the extent to which the procedures for the creation of and access to customer accounts should be updated so that copies of personal identity documents and or personal information cannot of themselves be used to commit identity fraud. We note that NSW driver's licences did not need to be replaced even though, reportedly, many were disclosed in the Optus data breach.
21.7	Require the establishment of retention periods	Support and note comments	In our submission any requirement that APP entities established their own maximum and minimum retention periods should be expressed so that the retention periods are variable depending upon the requirements of the relevant APP entity. Some personal information must be retained because the customer relationship is ongoing, and it is necessary to service the customer. In other circumstances personal information must be retained because it forms part of a document which the AP entity is required to retain by statute. In some cases, personal information will form part of a record which is necessary for management of risk. For example where service is being provided and there is a risk of the service recipient claiming negligence. Information sometimes must be retained because an organisation is on notice of a dispute. From a privacy point of view, the primary obligation that an organisation must observe is to destroy or de-identify information which is not needed for any one of these four reasons.

Clause	Proposal (in brief)	Position	Comments
21.8	Retention periods in the privacy policy	Do not support	This proposal creates unnecessary administration, will make privacy policies even harder to read, and shifts the burden onto individuals to understand lengthy retention schedules. Please see our comment in relation to proposal 21.7 above
22.1	Controllers and processors	Do not support note comments	We support the introduction of a controllers and processors distinction; this proposal creates unnecessary administration with limited benefit to individuals. As currently drafted the Privacy Act is difficult to apply to an entity that is receiving and managing information for a third party (a processor). Strictly speaking the processor organisation is required to be aware of the information that it is receiving and processing so that it can describe how it is managed in its privacy policy, to give collection notices to relevant data subjects enter permit access and inspection. In many cases these requirements are highly impracticable for a processing entity and in some cases work against restrictions on access and security that are intended to protect the relevant information. We support the introduction of the concept of a processor perhaps on condition that the controller include contractual provisions like those imposed on processors by the European General Data Protection Regulation (GDPR) in order to protect personal information.
23.1	Overseas data flows	Support	We support the proposal to undertake a consultation on 5B(3). The recent amendment of this section removed a requirement that personal information regulated under the Privacy Act be connected with Australia. Accordingly, the Act now purports to regulate personal information collected from data subjects outside Australia where the collecting party is an APP entity. We support the Privacy Act only regulating personal information that is information connected with Australia.
23.2	Prescribed countries	Support	We support this proposal.
23.3	Standard contractual clauses	Support	We support the creation of standard contractual clauses provided they are not mandatory. In many cases personal information is regulated by generally applicable cross border agreements which may not adopt any standard language prescribed by the Privacy Act but which are within the scope of the requirements of APP8.
23.4	Strengthen the informed consent exception	Amend	Many organisations collecting personal information in Australia have operations overseas that manage customer service and fulfilment obligations. In some cases, information is stored securely in cloud systems which involve the use of servers outside Australia. These practises generally do not pose any significant risks to Australian data subjects that could be subject to the proposed

Clause	Proposal (in brief)	Position	Comments
			new rule. We would support this rule if was with regard to the data is stored in countries reasonably considered to be potential national security risks as determined by the Commonwealth. Any new requirement in the Privacy Act should focus on cases where a collecting entity is located offshore and/or proposes to disclose personal information without control or conditions to a third party in a foreign jurisdiction. In other cases the information is already protected.
23.5	Strengthen APP5	Amend	Australian data subjects are used to the fact that the Internet is global and that a lot of information moves between countries around the globe. It is not particularly relevant to inform data subjects regarding the countries where their information might be located, with some exceptions. It is only relevant to inform data subjects that the information may be disclosed offshore if the disclosure is being made without conditions or controlled which, in almost every case, is required to comply with Australian collection and notification rules. It would be more helpful for consumers to the advised that the collecting entity accepts responsibility for their information under the Privacy Act and will attend to arrangements which may include storage management and processing of the information offshore.
23.6	Introduce definition of disclosure	Support	We support the inclusion of the definition of disclosure in the Act.
25.1	Civil penalty tiers	Amend	The proposal should contemplate the size of the business in determining enforcement tiers and penalties, so as to not expose small businesses to fines of $50m. We note the proposed changes to civil penalty provisions. The Privacy Act is principle based legislation where a fine line between compliant and non-compliant behaviour is often difficult to determine. It is inappropriate for legislation of this kind to be subject to regulatory discretion as to the issue of penalties. Under the existing regime organisations are penalised for a failure to protect the privacy of an individual through the complaints in compensation mechanism maintained by the OAIC. This existing mechanism is badly underfunded, and individuals can wait for more than a year to have complaints considered and processed by the OAIC. In our view it would be better for the government to properly fund support the existing framework rather instead introducing new discretionary penalties which to not assist data subjects and

Clause	Proposal (in brief)	Position	Comments
			are not supported by evidence of a failure in the existing regime.
25.2	Clarify 'serious' interference with privacy	Amend	For clarity, consideration (c) should include children as well as vulnerable people.
25.3	Amend the Act to apply the powers in Part 3	Amend	See our response in relation to proposal 25.1.
25.5	Requirement to identify, mitigate and redress actual or reasonably foreseeable loss	Support	We support the suggestion that an organisation should be required to identify, mitigate, and redress any actual loss. However, we submit that organisation should not be required to redress "reasonably foreseeable loss". Following a data breach there are many circumstances where an individual has not suffered a loss but on the basis of various assumptions regarding the motivation or characteristics of the party responsible and/or where there is uncertainty regarding the information lost (it is often unclear to what extent information has been exfiltrated from a system once at a weakness has been identified) it is possible to see all kinds of loss as "foreseeable". In our submission a reasonable obligation is to identify, mitigate and, to the extent possible, prevent foreseeable loss. It is not reasonable to introduce a requirement that would have APP entities providing compensation or ameliorating services to individuals only on the basis that some kind of loss can be foreseen where it is in fact uncertain and possibly highly unlikely.
25.9	Amend the annual reporting requirements in AIC Act	Amend	Amend to allow a complainant to require the Commissioner make a determination under section 52.
26.1	Direct right of action	Amend & note comments	Establish a more direct and accessible avenue to exercise this right than proceedings in the Federal Court would achieve. We note the introduction of a direct right of action for breach of the Privacy Act. It would be more constructive and better for consumers to properly fund the existing compensation scheme.
27.1	Statutory tort	Support	Implement this proposal as is.
28.1	Better facilitated reporting processes for notifiable data breaches	Support	Implement this proposal as is.
28.2	72 hour notification	Support	We support this proposal noting that the proposed 72 hour deadline is consistent with the notification requirements under the security of critical infrastructure framework.
28.3	NDB statement enhancements	Support and note comments	We support these recommendations. However, we note that it can take some time to analyse a cohort of individuals the subject of a data breach, work out how they can be adversely

Clause	Proposal (in brief)	Position	Comments
			affected and what steps might be appropriate by way of mitigation or amelioration. It is important that any new requirement of the kind be imposed only after the relevant organisation has had time to undertake proper analysis and put in place services that are meaningful and appropriate.
28.4	AG to permit data sharing during breaches	Support	Implement this proposal as is.
29.1	Privacy law design guide	Support	Implement this proposal as is.
29.2	Regulatory cooperation	Support	Implement this proposal as is.
29.3	Working group on harmonising privacy laws	Support and note comments	We support this proposal. The differences between the federal Privacy Act and the state privacy acts are significant and complex. In particular the manner in which state organisations supported by Commonwealth funding are regulated in whole or part by state law and/or federal law can be complex and confusing. It should be possible to develop a harmonised privacy regime which impose that a simple and workable framework across the entire economy.

Appendix – Security Standards Overview

Purpose and scope	ISO 27000 Series (1)	NIST CSF (3)	C2M2 (4)	AESCSF (5)
	How is cyber security managed?	**How good are we at using industry standards and best practices to manage our cyber security risks?**	**How mature are our cyber security capabilities? Can we measure them?**	**How mature are our cyber security capabilities? Can we measure them using a tool specifically developed for the Australian Energy sector?**
	The ISO 27000 Series provides a broad range of best practice recommendations on information security management. It covers monitoring, risk management, measurement, analysis, and evaluation of the Information Security Management System (ISMS). ISO 27000 Series are arguably the most well-known, international set of standards on information security. **These standards are broad and independent of industry.**	A high level, taxonomy of non-prescriptive cyber security outcomes and a methodology to assess and manage those outcomes. Focuses on cyber security, not information security (i.e., does not include physical information). A very popular framework originating from the US critical infrastructure sector. Provides Informative references and mapping to several control frameworks. **The standard is cyber security specific and (although initially designed for critical infrastructure in 2014) independent of industry.** **It can be used to measure maturity of capabilities but was not initially designed for it.**	The Cyber Security Capability Maturity Model (C2M2) contains a set of common cyber security practices that can be used to evaluate, prioritise, and improve cyber security capabilities. As a maturity model, C2M2 includes practices that range from foundational to more advanced in terms of either technical sophistication or consistency and repeatability. This enables C2M2 to be used to understand the current state of a cyber security program and track growth over time. **The standard is cyber security specific and (although initially designed for critical infrastructure) independent of industry. It was designed to measure maturity of a cyber security program.**	The framework's purpose is to enable the Australian energy sector to assess, evaluate, prioritise, and improve their cyber security capability and maturity. It leverages Electricity Subsector Cyber Security Capability Maturity Model (ES- C2M2), NIST CSF, Australian Privacy Principles and ACSC Essential Eight. **The standard is designed for the Australian energy sector and cyber security specific. It was designed to measure maturity of a cyber security program. In 2022, the framework was planned for extension to the liquid fuels sector.**

NB Item numbers above are from Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023 Section 8 Cyber and information security. Explanations were originally provided by AISA in Public Consultation on 'Draft SOCI Risk Management Program (RMP) Rules', 18 November 2022.

Lead Authors

Michael Trovato
Board Member AISA

Patrick Fair
Fellow of AISA

EJ Wise
Fellow of AISA

Contributing Authors

Nicole Stephensen
Fellow of AISA

Sascha Hess
Member of AISA

Damien Manuel
Board Member AISA

Andrew Evans
Board Member AISA

Akash Mittal
Board Member AISA

Craig Ford
Board Member AISA