9 October 2024

BSA COMMENTS ON THE PRIVACY AND OTHER LEGISLATION AMENDMENT BILL 2024

Submitted Electronically to the Senate Legal and Constitutional Affairs Legislation Committee

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to submit comments to the Senate Legal and Constitutional Affairs Legislation Committee (**Committee**) Inquiry on the Privacy and Other Legislation Amendment Bill 2024 (**Privacy Bill**)[2] and the accompanying Explanatory Memorandum (**Memo**).[3]

BSA is the leading advocate for the global software industry. BSA members create technology solutions that power other businesses, including cloud storage services, customer relationship management software, human resources management programs, identity management services, network infrastructure services, cybersecurity solutions, and collaboration systems. Our members have made significant investments in Australia, and we are proud that many Australian companies and organisations continue to rely on our members' products and services to do business and support Australia's economy. BSA members recognise that companies must earn their consumers' trust and act responsibly with their personal information.

BSA has participated in multiple consultations on the review of the Australian Privacy Act 1988 (**Privacy Act**)[4] and expressed support for many of legislative proposals that were agreed to by the Government in its Response to the Privacy Act Review Report (**Response**),[5] particularly the proposal to implement a clear distinction between controllers and processors in the Privacy Act. It is therefore disappointing that this proposal, alongside many others which the Government agreed to in its Response, are not reflected in the Privacy Bill. This represents a missed opportunity for Australia to modernise its Privacy Act and ensure it is fit-for-purpose in the digital age.

---

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Cohere, Dassault, Databricks, DocuSign, Dropbox, Elastic, ESTECO SpA, EY, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Nikon, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

[2] Privacy and Other Legislation Amendment Bill 2024, September 2024, https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r7249_first-reps/toc_pdf/24115b01.pdf;fileType=application%2Fpdf.

[3] Privacy and Other Legislation Amendment Bill 2024 Explanatory Memorandum, September 2024, https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r7249_ems_a01fc1bd-4aa3-4fc2-87d7-ed8aa84ab564/upload_pdf/JC014082.pdf;fileType=application%2Fpdf.

[4] See: BSA Comments on Australia Online Privacy Bill, December 2021, https://www.bsa.org/policy-filings/australia-bsa-comments-on-australian-online-privacy-bill; BSA Comments on Review of Australia Privacy Act, January 2022, https://www.bsa.org/policy-filings/australia-bsa-comments-on-review-of-australia-privacy-act-1988; BSA Comments on Privacy Legislation Amendment Bill, October 2022, https://www.bsa.org/policy-filings/australia-bsa-comments-on-privacy-legislation-amendment-bill; BSA Comments on Australia Privacy Act Review Report 2022, April 2023, https://www.bsa.org/policy-filings/australia-bsa-comments-on-australia-privacy-act-review-report-2022.

[5] Government Response to the Privacy Act Review Report, September 2023, https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report.

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

Summary of BSA's Recommendations

1. **Include Controller-Processor Distinction:** The Privacy Bill should be amended to include the controller-processor distinction. The distinction is a fundamental feature of privacy laws worldwide, and its inclusion will not only align Australia's privacy law with other international laws and frameworks, but also, provide much-needed clarity for businesses and consumers alike.

2. **Support International Data Transfers:** BSA supports the introduction of a mechanism to prescribe countries and binding schemes that provide substantially similar privacy protections to the Australian Privacy Principles (**APPs**). However, we recommend that the Privacy Bill specify what constitutes "substantially similar" privacy protections and conduct further consultations on the process and factors determining whether a country or binding scheme offers the appropriate level of protection. We also encourage Australia to explore ways to more fully account for international cross-border data policy frameworks, such as the Global Cross-Border Privacy Rules Forum and the OECD Declaration on Government Access to Personal Data Held by the Private Sector. These frameworks are specifically designed to bring together governments with a substantially similar view of the importance of personal data protection in a cross-border data policy context. We encourage Australia to consider presumptively deeming the signatories of these mechanisms to meet the "substantially similar" standard under the APPs.

3. **Harmonise Approach to Automated Decisions and Privacy Policies:** BSA supports establishing strong consumer rights with respect to personal data. However, key terms, notably what would constitute a decision that significantly "affect the rights or interests of an individual", and what is "a thing substantially and directly related to making a decision", are left undefined. These terms should be clearly defined. In addition, given the lack of specificity and the overlap between this requirement and ongoing work on introducing mandatory guardrails for high-risk uses of AI, BSA recommends ensuring any requirements related to automated decision-making are harmonised with — and not duplicative of, or conflicting with — any future mandatory guardrails on high-risk uses of AI.

4. **Identify Future Amendments to the Privacy Act:** The Attorney General's Department (**AGD**) should provide a clear and detailed roadmap for future amendments to the Privacy Act, outlining the specific recommendations that will be implemented in subsequent tranches and the expected timeframe for their introduction, with priority accorded to the controller-processor distinction. BSA also recommends that the AGD release exposure drafts of future bills for public consultation before introducing them to the Parliament.

Controller-Processor Distinction

Distinguishing between controllers and processors is a core feature of leading global privacy laws. The Government recognised as much in its Response, which stated that a key focus area of the Privacy Act review was to "increase clarity and simplicity for entities and individuals".[6] To that end, the Government agreed in-principle that "a distinction between controllers and processors of personal information should be introduced into the Privacy Act (*proposal 22.1*)", recognising that "different entities have differing degrees of control over the handling of personal information".[7] The Response also highlights that introducing the distinction will "bring Australia into line with other jurisdictions, reflect the operational reality of modern business relationships, and reduce the compliance burden for entities acting as processors".[8]

[6] Response (2023), p. 15.

[7] Response (2023), p. 15.

[8] Response (2023), p. 15.

BSA strongly agrees with the Government's observations. We therefore have significant concerns that a feature as fundamental as the controller-processor distinction is absent from this Privacy Bill. In our view, the introduction of a controller-processor distinction is the most important proposal to emerge from the Privacy Act review. This distinction has existed for more than 40 years and is foundational to privacy laws worldwide.[9] By reflecting the different roles of controllers (which decide how and why to process personal data) and processors (which handle personal data on behalf of other companies and pursuant to their instructions), a privacy law can better craft obligations that fit both types of organisations. There are significant benefits to distinguishing between controllers and processors under the Act:

- Adopting a distinction between controllers and processors will align the Act with privacy laws globally, including, but not limited to the European Union's General Data Protection Regulation (**GDPR**),[10] California's Consumer Privacy Act (**CCPA**),[11] Japan's Act on the Protection of Personal Information (**APPI**),[12] and Singapore's Personal Data Protection Act (**PDPA**).[13] This alignment will help Australian entities understand how their obligations under the Privacy Act map to their obligations under data protection laws in other major markets. It will also help entities streamline data protection and transfer practices across markets.
- Clearly distinguishing between the roles of controllers and processors also improves consumer protection and enhances regulatory certainty for businesses. As noted in the AGD's Privacy Act Review Report 2022 (**AGD Report**),[14] distinguishing between controllers and processors will "clarify consent obligations and assist with clarifying obligations in relation to any new individual rights (such as a right to erasure) that may be introduced following this review", and "help entities more effectively respond to data breaches."[15]

In the absence of a controller-processor distinction, both consumers and businesses face increased uncertainty. Consumers may struggle to understand which entities are responsible for safeguarding their data and how they can exercise their rights, while businesses lack clear guidance on their respective obligations, leading to potential gaps in accountability and compliance. Australia's Privacy Act will also remain an outlier among major jurisdictions. This means that both Australian businesses expanding into new markets and businesses looking to invest in Australia will need to navigate inconsistent privacy frameworks across multiple regions, which increases compliance costs and complexity in any way.

As noted in BSA's recent opinion piece on the need for privacy reform to reflect different roles in data handling,[16] the current efforts to reform the Privacy Act present the best opportunity to introduce the controller-processor distinction into Australian law. We strongly recommend that the Privacy Bill be amended to include the controller-processor distinction.

Recommendation: The Privacy Bill should be amended to include the controller-processor distinction. The distinction is a fundamental feature of privacy laws worldwide, and will not only align

[9] For more information about the importance of the controller-processor distinction, *see* BSA, Controllers and Processors: A Longstanding Distinction in Privacy, October 2023, https://www.bsa.org/files/policy-filings/10122022controllerprodistinction.pdf.

[10] European Union General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

[11] California Consumer Privacy Act of 2018, http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

[12] Amended Act on the Protection of Personal Information (English), https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf.

[13] Personal Data Protection Act 2012, https://sso.agc.gov.sg/Act/PDPA2012.

[14] Privacy Act Review Report 2022, February 2023, https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf.

[15] AGD Report (2023), p. 231.

[16] "Privacy reform must reflect different roles in data handling", September 2024, https://www.innovationaus.com/privacy-reform-must-reflect-different-roles-in-data-handling/.

Australia's privacy law with other international laws and frameworks, but also provide much-needed clarity for businesses and consumers alike.

Overseas Data Transfers

The Privacy Bill will introduce a mechanism to prescribe countries and binding schemes that provide substantially similar privacy protections to the APPs.[17]

As explained in the Memo, companies can already transfer data to overseas recipients through a variety of methods consistent with the Privacy Act.[18] These include disclosing data pursuant to APP 8.1, which adopts the accountability model and requires companies to meet certain obligations before transferring data to an overseas recipient, most notably the requirement to "take reasonable steps" to ensure the overseas recipient does not breach the APPs in relation to the information.[19] Separately, companies can also transfer data under APP 8.2 to an overseas recipient that is subject to a "substantially similar" privacy law or binding scheme, without adopting the obligations imposed in APP 8.1.[20]

The proposed mechanism under the Privacy Act would prescribe the countries and certification schemes that provide "substantially similar protection" under APP 8.2(a). The new mechanism would therefore make it easier for companies to transfer data under APP 8.2(a) by identifying countries that have "substantially similar protections," rather than requiring companies to assess for themselves which countries have such protections. Crucially, BSA notes that the new scheme would not limit companies from transferring data under the accountability model reflected in APP 8.1 or pursuant to any of the other grounds for transfers recognised in APP 8.2(b)-(f). In the circumstances, BSA supports the introduction of this proposed mechanism, as it will provide businesses with greater legal certainty and substantially reduce compliance burdens.

However, BSA also observed that neither the Privacy Bill nor the Memo explained what would constitute a "substantially similar" level of protection. If the mechanism establishes an unnecessarily strict interpretation of "substantially similar", it would be counterproductive to the policy objective of increasing certainty for companies transferring data internationally. For example, to the extent a new mechanism applies the term "substantially similar" to mean a standard akin to the European Union's "essentially equivalent" standard, it may unnecessarily restrict transfers conducted under APP 8.2(a).[21] Requiring foreign privacy laws deemed "substantially similar" to mirror, point-by-point, the APPs, would defeat the purpose of the mechanism. We recommend conducting further consultations on the process for, and factors involved in, determining whether a country or certification scheme offers the appropriate level of protection.

Relatedly, BSA recalls the AGD Report suggested that Australia could prescribe the Cross Border Privacy Rules (**CBPR**) system under APP 8.2(a) as a binding scheme that provides a "substantially similar" level of protection to the APPs.[22] In this regard, we reiterate our support for recognising internationally recognised certifications and standards such as the Global CBPR system. Similarly, the Act could also recognise compliance with ISO 27701 as creating "substantially similar" protections; that standard was published in 2019 and is the first privacy management standard published by the International Standards Organization.

---

[17] Explanatory Memo (2024), p. 11. See also: The Australian Privacy Principles, January 2014, https://www.oaic.gov.au/__data/assets/pdf_file/0006/2004/the-australian-privacy-principles.pdf.

[18] Explanatory Memo (2024), p. 44.

[19] The Australian Privacy Principles (2014), APP 8.1.

[20] The Australian Privacy Principles (2014), APP 8.2.

[21] We note that the GDPR's adequacy determinations are based on the standard of "essential equivalence." See: Questions & Answers on the adoption of the adequacy decision ensuring safe data flows between the EU and the Republic of Korea, December 2021, https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_6916.

[22] AGD Report (2023), p. 247-248.

Finally, we also observe that Australia – and many of its closest trading partners – have reflected their commitment to the protection of personal data from governmental overreach in the context of the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities.[23] The Global CBPR Forum and the OECD Declaration on Government Access to Personal Data Held By Private Sector Entities are specifically designed to bring together governments with a substantially similar view of the importance of personal data protection in a cross-border data policy context. We encourage Australia to consider presumptively deeming the signatories of these mechanisms to meet the "substantially similar" standard under the APPs.

Recommendation: BSA supports the introduction of a mechanism to prescribe countries and binding schemes that provide substantially similar privacy protections to the APPs. However, we recommend that the Privacy Bill specify what constitutes "substantially similar" privacy protections and conduct further consultations on the process for, and factors involved in, determining whether a country or certification scheme offers the appropriate level of protection. We also encourage Australia to take account of the longstanding efforts of Australia and its allies to improve cross-border data privacy interoperability by presumptively deeming the signatories of the Global CBPR Forum and OECD Declaration on Government Access to Personal Data Held By Private Sector Entities to meet the "substantially similar" standard under the APPs.

Automated Decisions and Privacy Policies

The Privacy Bill will introduce requirements for entities to "include information in privacy policies about the kinds of personal information used in, and types of decisions made by, computer programs that use personal information to make decisions that could reasonably be expected to significantly affect the rights or interests of the individual".[24]

BSA supports comprehensive consumer privacy laws that establish strong consumer rights regarding their personal data. This is particularly relevant in the context of automated decision making, as the data-intensive nature of AI underscores the importance of meaningful consumer privacy protections. Consumers deserve to know how their personal data is used and protected, and consumer expectations should be backstopped by strong legal obligations on companies that collect or process personal information.

However, BSA notes that while the Privacy Bill provided examples of automated decisions that may "affect the rights or interests of an individual",[25] it did not clearly specify what would constitute such a decision. The Privacy Bill should provide a comprehensive definition to increase certainty for both individuals and companies about when related rights are available.[26]

---

[23] OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, December 2022, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.

[24] Explanatory Memo (2024), p. 15.

[25] Privacy Bill, p. 58. These examples include: (i) a decision made under a provision of an Act or a legislative instrument to grant, or to refuse to grant, a benefit to the individual; (ii) a decision that affects the individual's rights under a contract, agreement or arrangement; and (iii) a decision that affects the individual's access to a significant service or support.

[26] For example, it could define these terms in a manner similar to state privacy laws in the United States, where Virginia, Colorado, and Connecticut all create rights to opt out of certain types of profiling that create legal or similarly significant effects. *See* Colorado Privacy Act, Sec. 6-1-1303(10) ("Decisions that produce legal or similarly significant effects concerning a consumer" is defined as "a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services."); Connecticut Data Privacy Act Sec.1(22) ("Decisions that produce legal or similarly significant effects concerning the consumer" are defined as "decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services."); Virginia Consumer Data Protection Act, Sec. 59.1-575 ("Decisions that produce legal or similarly significant effects concerning a consumer" are defined as "a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.").

The Privacy Bill also provides that disclosures would be required where a computer program is used to "do a thing substantially and directly related to making a decision".[27] This appears to be the case even if there is a "human decision-maker" involved.[28] However, many key elements of this requirement remain unclear, notably when would something be "substantially and directly related to making a decision". This ambiguity creates uncertainty about when disclosures may be required.[29] This is further exacerbated by the broad definition of "computer program",[30] which does not appear to be limited to AI-related systems. This expansive definition will: a) create further ambiguity in respect of which "computer programs" are used in decision-making processes; and b) significantly increase the volume of potential disclosures.The Privacy Bill should clearly specify what is meant by "substantially and directly related to making a decision", and clarify whether the intent is to cover fully automated decisions or extend to situations where decisions are subject to human oversight.

BSA also notes that the Department of Industry, Science and Resources (**DISR**) is conducting consultations on introducing mandatory guardrails for high-risk uses of AI.[31] In particular, the Privacy Bill's examples of automated decisions that may "affect the rights or interests of an individual" may intersect with high-risk uses of AI. There was no indication in the Privacy Bill or Memo that these obligations would be harmonised. This leads to uncertainty over, for example, whether "low-risk" AI uses would be subject to this disclosure obligation, and whether the obligation might apply differently depending on the role of the entity in the AI supply chain. It is critical that any requirement on automated decision-making included in the Privacy Bill is consistent with any subsequent cross-sector frameworks or legislation related to AI.

Recommendation: BSA supports establishing strong consumer rights with respect to personal data. However, key terms, notably what would constitute a decision that significantly "affect the rights or interests of an individual", and what is "a thing substantially and directly related to making a decision" are left undefined. These terms should be clearly defined. In addition, given the lack of specificity and the overlap between this requirement and ongoing work on introducing mandatory guardrails for high-risk uses of AI, BSA recommends ensuring any requirements related to automated decision-making are harmonised with — and not duplicative of, or conflicting with — any future mandatory guardrails on high-risk uses of AI.

Future Amendments to the Privacy Act

In the Attorney-General's media release on the Privacy Bill, he stated that the Privacy Bill "implements a first tranche of agreed recommendations from the Privacy Act".[32] However, there was no indication as to *which* recommendations will be implemented next, and *when* they will be introduced. Without a clear roadmap or timeframe, there is significant uncertainty regarding how and when businesses will need to adjust their privacy practices to comply with the evolving landscape.

In the circumstances, we urge the Committee to encourage the AGD to provide a roadmap of future amendments to the Privacy Act. This roadmap should clearly set out which agreed recommendations the AGD will implement next, and when stakeholders can expect these agreed recommendations to be presented in a bill for public consultation. To the extent that the controller-processor distinction

---

[27] Privacy Bill, p. 57.

[28] Explanatory Memo (2024), p. 77-78.

[29] Explanatory Memo (2024), p. 77-78. The Memo's explanation that "*substantially* means where it is a key factor in facilitating the human's decision making;" and "*directly* means where the thing has a direct connection with making the decision" is too vague to be helpful. This is further exacerbated by the broadly-defined term "computer program".

[30] Explanatory Memo (2024), p. 77. The term "computer program" will "encompass a broad range of matters, including pre-programmed rule-based processes, artificial intelligence and machine learning processes to make a computer execute a task".

[31] Introducing Mandatory Guardrails for AI in High-Risk Settings: Proposals Paper, September 2024, https://storage.googleapis.com/converlens-au-industry/industry/p/prj2f6f02ebfe6a8190c7bdc/page/proposals_paper_for_introducing_mandatory_guardrails_for_ai_in_high_risk_settings.pdf.

[32] Media Release by the Hon Mark Dreyfus KC MP: "Better protection of Australians' privacy", September 2024, https://ministers.ag.gov.au/media-centre/better-protection-australians-privacy-12-09-2024.

cannot be introduced in this Privacy Bill, we strongly urge any subsequent tranches of reform to prioritise introducing this distinction due to how fundamental it is to the function and structure of a privacy law.

In addition, BSA notes that the AGD did not release an exposure draft of the Privacy Bill before introducing it into Parliament, despite multiple requests from various industry stakeholders. As a matter of good practice, releasing an exposure draft of a bill for public consultation would allow industry to engage on draft legislative text and comment on any potential concerns or ambiguities before it is submitted to Parliament. We find this practice invaluable in helping to create more widely-supported and effective legislation.

Recommendation: The AGD should provide a clear and detailed roadmap for future amendments to the Privacy Act, outlining the specific recommendations that will be implemented in subsequent tranches and the expected timeframe for their introduction, with priority given to the controller-processor distinction. BSA also recommends that the AGD release exposure drafts of future bills for public consultation before introducing them to Parliament.

Conclusion

We hope that our comments will assist the Committee. We look forward to serving as a resource in this public consultation process. Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Sincerely,

Tham Shen Hong
Senior Manager, Policy – APAC