Privacy108
We Protect Privacy

PO Box 3295
Yeronga QLD 4104
Level 12, 259 Queen St
Brisbane QLD 4000

2 October 2024
Committee Secretary
Senate Standing Committee on Legal and Constitutional Affairs
By email: legcon.sen@aph.gov.au

Submission in response to the Inquiry into the Privacy and Other Legislation Amendment Bill 2024

We appreciate the opportunity to submit our response to the Privacy and Other Legislation Amendment Bill 2024 (the **Bill**).

Please find our submission attached. We have no objection to the publication of this submission.

Please let us know if we can provide any clarification about our response.

Thank you for your consideration.

Yours Sincerely,

Dr Jodie Siganto CISSP, CISM, CIPM, CIPP/E, CIPT

CEO

Proposed reform	Response
Part 1 – Objects of the Act	
1. **Items 1 and 2**: Amend the objects of the Act to clarify that the Act is about the protection of personal information and to recognize the public interest in protecting privacy.	Agree
Part 2- APP Codes	
2. **Items 3 to 6**: Promote the right to privacy by providing greater flexibility and efficiency to the APP code-making process by empowering the Information Commissioner to develop and register an APP code or Temporary APP code on the written direction of the Minister if the Minister is satisfied that it is in the public interest to develop the code, and for the Information Commissioner to develop the code.	Agree
Part 3 – Emergency Declarations	
3. **Items 7 to 29**: Amend the Privacy Act's emergency declaration provisions to enable emergency declarations to be more targeted by requiring that the declarations specify the kinds of personal information that may be handled, the entities which may handle the personal information, the entities to which the personal information may be disclosed, and the permitted purpose of the collection, use or disclosure of the personal information.	Agree
Part 4 – Children's privacy	

Proposed reform	Response
4. **Sections 30 to 33:** require the development of a COP Code to enhance privacy protection for children where a '*child*' means an individual who has not reached 18 years.	Agree in principle. We agree in principle with the proposed amendment to define a child as an individual under 18 years of age in the Privacy Act. However, we note the ongoing debate around restricting children's access to social media and other digital platforms until they reach a certain age, likely between 14 and 16 years. This raises a question about the need for consistency between the Privacy Act's definition of a child and any future legislation that may impose age-based restrictions on social media usage. Aligning the definition of a 'child' in the Privacy Act with such potential legislation could help reduce confusion and create a more cohesive regulatory framework. Regardless of the exact age chosen, this approach would acknowledge that individuals at that age are likely to possess the necessary maturity to navigate the internet more safely, understand privacy policies, and where applicable, provide informed consent to the collection and use of their personal information.
Part 5 – Security, retention and destruction	
5. **Items 34 to 35**: APP 11.1 to state that 'reasonable steps' includes 'technical and organisational measures'.	Agree. We recommend also updating the OAIC guidance on APP 11 to clarify what constitutes 'reasonable steps' for securing personal information. Additionally, the guidance should more explicitly outline the steps that can be taken to destroy or de-identify personal information. For matters related to cybersecurity, the guidance could benefit from incorporating technical advice from the Australian Cyber Security Centre.
Part 6 – Overseas data flows	
6. **Items 36 to 39:** Introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs.	Agree.
Part 7 – Eligible data breaches	
7. **Items 40 to 44**: Amend the Privacy Act's emergency declaration provisions to enable emergency declarations to be more targeted by requiring that the declarations specify the kinds of personal information that may be handled, the	Agree.

Proposed reform	Response
entities which may handle personal information, the entities to which the personal information may be disclosed, and the permitted purpose of the collection, use or disclosure of the personal information.	
Part 8 – Penalties for interference with privacy	
8. **Items 45 to 58:** Introduction of tiers of civil penalty provisions to allow for better targeted regulatory responses: (a) Introduction of a new mid-tier civil penalty provision to cover interferences with privacy without a 'serious' element, excluding the new low-level civil penalty provision. (b) Introduction of a new low-level civil penalty provision for specific administrative breaches of the Act and APPs with attached infringement notice powers for the Information Commissioner with set penalties.	Agree.
9. **Items 51**: Section 13G of the Act to be amended to clarify that the court may have regard to any of the following matters in determining a 'serious' interference with privacy: (a) the particular kind or kinds of information involved in the interference with privacy; (b) the sensitivity of the personal information of the individual; (c) the consequences, or potential consequences, of the interference with privacy for the individual; (d) the number of individuals affected by the interference with privacy;	Agree. We also suggest that consideration be given to linking serious interferences to: • breaches of any cyber-security regulations; • failure to comply with any accepted Code of Practice; • failure to carry out a PIA for high risk processing; • failure to implement remediations identified in a PIA.

Proposed reform	Response
(e) whether the individual affected by the interference with privacy is a child or person experiencing vulnerability; (f) whether the act was done, or the practice engaged in, repeatedly or continuously; (g) whether the contravening entity failed to take steps to implement practices, procedures and systems to comply with their obligations in relation to privacy in a way that contributed to the interference with privacy; (h) any other related matter.	
10. **Items 56**: Section 13K be inserted to introduce a civil penalty provision where infringement notices can be issued by the Information Commissioner for the following contraventions – a breach of: (a) APP 1.3 (requirement to have an APP privacy policy); (b) APP 1.4 (contents of an APP privacy policy); (c) APP 2.1 (individuals may choose not to identify themselves in dealing with entities); (d) APP 6.5 (written notice of certain uses or disclosures); (e) APP 7.2(c) or 7.3(c) (simple means for individuals to opt-out of direct marketing communication); (f) APP 7.3(d) (requirement to draw attention to ability to opt out of direct marketing communications); (g) APP 7.7(a) (giving effect to request in reasonable period); (h) APP 7.7(b) (notification of source of information); (i) APP 13.5 (dealing with requests);	Agree. However, we note the resources of the OAIC will ultimately dictate what action is taken and how effective any new penalty provisions may be.

Proposed reform	Response
(j) Any other APPs prescribed by the regulations.	
Part 9 – Federal court orders	
11. **Items 59, 60**: Enable the FCA or the FCFCOA to issue any order it sees fit, if the Court is satisfied there has been contravention of a civil penalty provision.	Agree
Part 10 – Commissioner to conduct public inquiries	
12. **Items 61 to 64**: Enable the Information Commissioner to conduct public inquiries into specified matters as directed by or subject to Ministerial approval.	Agree
Part 11 – Determinations following investigations	
13. **Items 65 to 67:** Allow the information Commissioner to issue a determination requiring a respondent to a privacy matter to perform any reasonable act or course of conduct to prevent or reduce reasonably foreseeable future loss or damage.	Agree
Part 12 – Annual reports	
14. **Items 68 to 71**: The annual report prepared by the Information Commissioner should also include: (a) details about the number of complaints made under s 36 of the Act during the year; (b) and details about the number of complaints made under s 36 of the Act in relation to which the Commissioner has decided during the year under section 41 of tat Act not to investigate, or not to investigate further, and the relevant grounds for that decision.	Agree
Part 13 – External dispute resolution	

Proposed reform	Response
15. **Items 72, 73:** Enable the Information Commissioner to decide not to investigate a complaint that has been dealt with by a recognised external dispute resolution scheme.	Agree
Part 14 – Monitoring and investigation	
16. **Items 74 to 86**: Amend the Privacy Act to apply the standard monitoring and investigation powers contained in the Regulatory Powers Act. In addition, make necessary consequential amendments to other Acts that enliven the Information Commissioner's investigation powers within those Acts by applying provisions of the regulatory regime in the Privacy Act.	No comment
Part 15 – Automated decision making	
17. **Items 87 to 89:** Introduce requirements that entities must 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 an individual.	We agree in principle, but more needs to be done. Relying on additional information in a privacy policy has limited value. While transparency is important, it does not mitigate the potential harm or address the power imbalance between entities and individuals, especially when AI is involved. We are also concerned about effectively this will tackle algorithmic explainability or how Australian entities will ensure compliance when using AI products from jurisdictions with weaker privacy protections. We strongly encourage greater involvement from the OAIC in this area. Specifically, we recommend the OAIC provide comprehensive guidance and recommendations to Australian entities on developing and using AI/ML in a manner that is privacy-conscious, ethically sound, and non-discriminatory. Moreover, the Privacy Act should include clear indicators of decisions that have a significant affect on the rights or interests of individuals. These should be further supported by detailed OAIC guidance. Additionally, individuals must have stronger rights beyond transparency when AI is used. At a minimum, these should include:

Proposed reform	Response
	• The right to human intervention in AI-driven decision-making processes; • The right to refer AI uses to a specialist regulator for review based on fairness and the protection of broader human rights, particularly regarding their impact on individuals.
Schedule 2 – Serious invasions of privacy	
18. Introduction of a new cause of action for serious invasions of privacy. Cause of action in tort arises if: (a) the defendant invaded the plaintiff's privacy by doing one or more or both of the following: (i) intruding upon the plaintiff's seclusion; (ii) misusing information that relates to the plaintiff; and (b) a person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances; and (c) the invasion of privacy was intentional or reckless; and (d) the invasion of privacy was serious. The sum of any damages awarded for non-economic loss and any exemplary or punitive damages, must not exceed the greater of $478,550 and the maximum amount of damages for non-economic loss that may be awarded in defamation proceedings under an Australian law. A plaintiff must commence proceedings: (a) if the plaintiff was under 18 years of age when the invasion of privacy occurred – before the plaintiff's 21st birthday; or (b) otherwise – before the earlier of: (i) the day that is 1 year after the day on which the plaintiff became aware of the invasion of privacy; and (ii) the day that is 3 years after the invasion of privacy occurred.	Agree

Proposed reform	Response
Schedule 3 – Doxxing offences	
19. Introduction into the Commonwealth Criminal Code of two new offences for 'doxxing' activities. Including introduction of a definition of "personal data" for the purpose of 'doxxing' which shall means "information about the individual that enables the individual to be identified, contacted or located, and includes the following: (a) the name of the individual; (b) a photograph or other image of the individual; (c) a telephone number of the individual; (d) an email address of the individual; (e) an online account of the individual; (f) a residential address of the individual; (g) a work or business address of the individual; (h) a place of education of the individual; (i) a place of worship of the individual.	Agree in principle. However, we note that the introduction of the term '*personal data'* into the Criminal Code creates an unnecessary distinction from the established term '*personal information*' under the Privacy Act. While it is arguable that 'personal data' in the context of doxing might aim to encompass a broader or more specific range of information that can be used to cause harm, the Privacy Act is designed to safeguard individual privacy rights, not just regulate the use of information. Despite the differing objectives of these two pieces of legislation, we believe there should be consistency in terminology. Rather than introducing a new term, both the Criminal Code and the Privacy Act should refer to 'personal information', and the definition of this term should be updated to reflect moder digital realities. Specifically, the definition needs to be broadened to include metadata, geolocation data, and digital identifiers such as IP addresses, usernames, and other indirect identifiers, which are currently not comprehensively covered under the Privacy Act. In both contexts, using 'personal information' as the unified term would ensure clarity and consistency across Australian law. The definition should be expanded to cover data shared in digital environments, such as social media and online forums, and must be flexible enough to address emerging forms of digital information. This alignment would effectively support the legislative goals of both privacy protection and the criminalisation of malicious online behaviours, including doxxing.