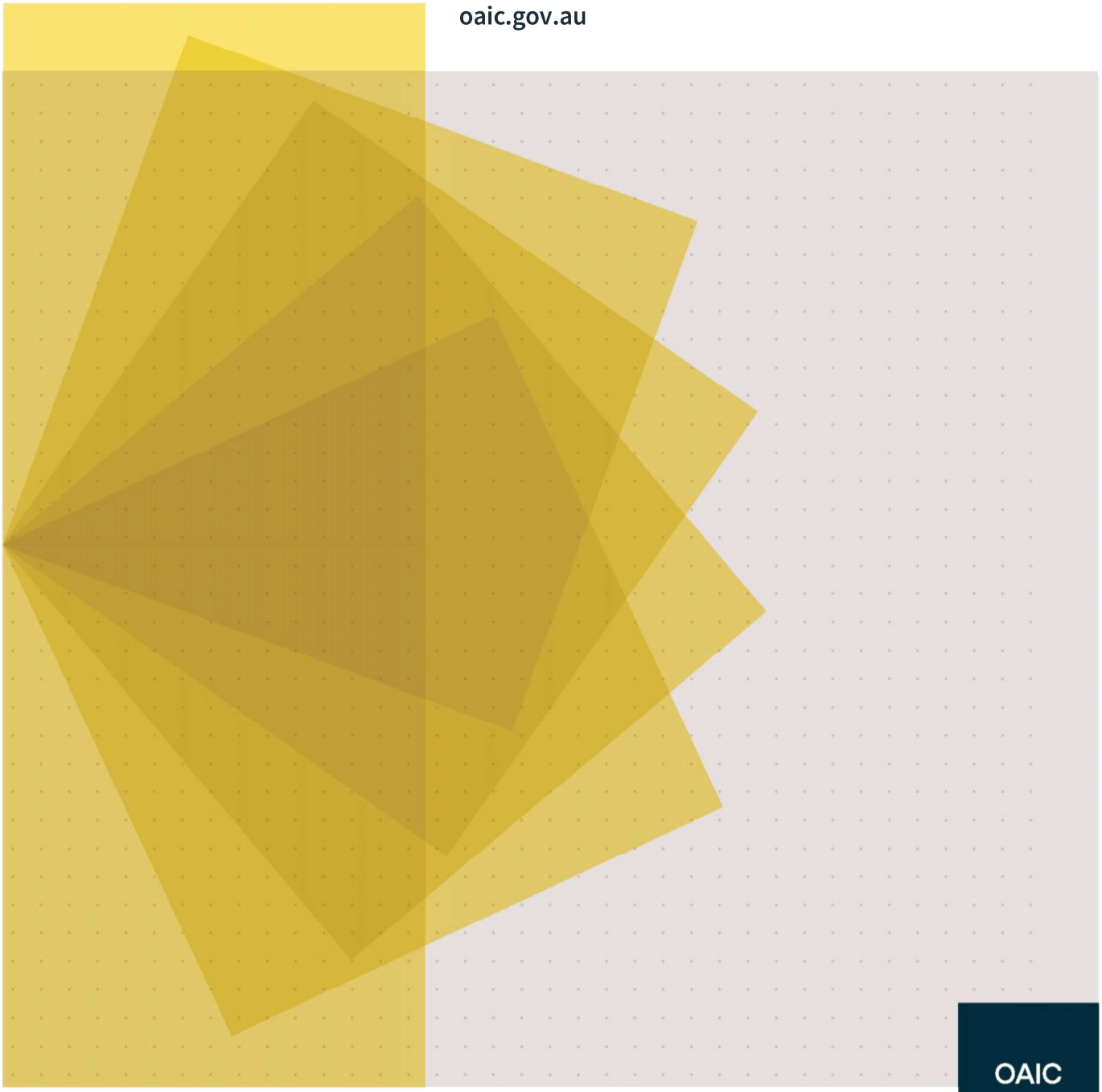
Australian Government

Office of the Australian Information Commissioner

Australia's 2020 Cyber Security Strategy: A call for views

Submission of the Office of the Australian Information Commissioner

oaic.gov.au



OAIC

Contents

Executive Summary

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to make this submission to the Department of Home Affairs regarding *Australia's 2020 Cyber Security Strategy – A Call for Views* (the Discussion Paper).
2. As the regulator of the *Privacy Act 1988* (Cth) (Privacy Act), the OAIC supports promoting the development of robust cyber security protections for Australia. Strong cyber security settings are a critical mechanism for protecting personal information and therefore individuals' privacy.[1]
3. The relationship between information security (including cyber security) and privacy is codified in the Privacy Act, particularly through Australian Privacy Principle (APP) 11, which requires all entities covered by the Privacy Act to take reasonable steps to protect personal information that they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.
4. The responses to cyber security risks cannot be static due to an evolving landscape driven by emerging technologies and malicious actors who have become more sophisticated in the tactics they employ and practices they use.[2] In this changing context, there is a substantial and necessarily agile role for Government to play in protecting Australians and Australian organisations from cyber risks. It is critical that discussions effectively leverage existing mechanisms to counter the often-linked cyber security and privacy threats and support coordinated government response and prevention.

Link between privacy protection and effective cyber security

5. There is a fundamental link between strong cyber protection and the protection of personal information under the Privacy Act.
6. Entities covered by the Privacy Act[3] are required by APP 11 to take reasonable steps to protect the personal information that they hold from misuse, interference and loss, as well as unauthorised access, modification or disclosure.[4] Entities must also take reasonable steps to destroy or de-identify the personal information they hold once it is no longer needed for any purpose for which it may be used or disclosed under the APPs.[5]
7. Importantly, cyber security is recognised as a necessary privacy protection and key consideration for entities taking 'reasonable steps' under APP 11.[6] There is an expectation that

---

[1] See Chapter 11: APP 11 – Security of Personal Information of Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines*, OAIC, Sydney

[2] See Cyber Security Policy Division 2019, *Australia's 2020 Cyber Security Strategy – A Call for Views*, Department of Home Affairs, Canberra, p 14, and also Office of the Australian Information Commissioner, *Building a secure digital future: educating cybersecurity professionals,* OAIC, Sydney available at < https://oaic.gov.au/updates/speeches/building-a-secure-digital-future-educating-cybersecurity-professionals/>

[3] This includes organisations with an annual turnover of more than $3 million, private sector health providers, businesses that sell or purchase personal information and Australian Government agencies.

[4] APP 11.1, Schedule 1 of the *Privacy Act 1988* (Cth).

[5] APP 11.2, Schedule 1 of the *Privacy Act 1988* (Cth).

[6] As compliance with APP 11 is context dependent, the OAIC has published the *Guide to securing personal information*, which provides guidance on the reasonable steps that entities are required to take under the Privacy Act to protect the personal information they hold. The Guide is intended for use by entities covered by the Privacy Act, but may also be

in complying with APP 11, businesses will actively monitor their cyber risk environment for emerging threats and take reasonable steps to protect personal information by mitigating those risks. This responsibility is not static and scales proportionately to the volume and type of personal information held by an entity. Where the volume or sensitivity of personal information held by an entity increases, so too will the expectations placed upon the entity to protect that information.

8. The expectations placed on entities when protecting personal information are not confined to technical security measures alone. Under APP 11, entities must also take steps beyond technical security measures in order to protect and ensure the integrity of personal information throughout the information lifecycle, including implementing strategies in relation to governance, internal practices, processes and systems, and dealing with third party providers.[7]
9. The economy-wide privacy law is supported by sector specific privacy frameworks. Sector specific frameworks add specificity and clarity in relation to certain parts of the economy. For instance, there are particular privacy security requirements relating to credit information and credit eligibility information,[8] and tax file number information.[9] There are specific personal information security requirements relating to My Health Records and retained data under the *Telecommunications (Interception and Access) Act 1979* (Cth).[10]
10. In addition, since February 2018, entities covered by the Privacy Act are required by law to notify both the OAIC and individuals at risk of serious harm in the event of a notifiable data breach (NDB). Since the inception of this mandatory reporting regime, approximately 60% of notified data breaches of personal information have been attributed to cyber intrusion.
11. The effective prevention, mitigation and responses to cyber-related threats are fundamentally linked with effective privacy protection.

The role of government, business and individuals in the prevention and response to cyber threats

12. The Discussion Paper raises questions regarding the role of government, businesses and individuals in relation to the prevention and response to cyber threats.

Government

13. The OAIC considers that government has an important role in ensuring that legislation, regulation and enforcement capabilities are comprehensive, coordinated, clear and effectively responsive to significant, sophisticated global cyber threats.
14. The OAIC is supportive of opportunities for further clarity about the prevention of information loss by harmonising existing cyber security-related laws and standards. While different entities

relevant to other organisations as a model for better personal information handling practices. See Office of the Australian Information Commissioner 2018, *Guide to Securing Personal Information*, OAIC, Sydney, available at < https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/>

[7] APP 1 also requires entities to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs.

[8] Part IIIA of the *Privacy Act 1988* (Cth).

[9] Rule 11 of the Privacy (Tax File Number) Rule 2015, issued under section 17 of the *Privacy Act 1988* (Cth).

[10] Rule 44 of the My Health Records Rules 2016, issued under section 109 of the *My Health Records Act 2012* (Cth), and Section 187LA of the *Telecommunications (Interception and Access) Act 1979* (Cth).

and industries may require different approaches to cyber security, this must be balanced with the need to provide consistent, comprehensive and unfragmented regulatory frameworks which help regulated entities and individuals to clearly understand their rights and obligations.

15. There are a number of Commonwealth entities with mandates that intersect with and respond to cyber-related risks. For example, in addition to the Privacy Act, entities may also have to comply with non-privacy related cyber security regulations or standards such as the Australian Prudential Regulation Authority's (APRA) *Prudential Standard CPS 234 – Information Security*, which applies to all APRA-regulated industries. Separately, Australian Government agencies must act consistently with the policies of the Australian Government,[11] such as the Attorney-General's Department's 'Protective Security Policy Framework'[12] and the Australian Signals Directorate's 'Australian Government Information Security Manual'.[13]

16. Mapping and clarity around the Commonwealth entities' actual and potential engagement in combating cyber risks may identify enhanced opportunities to leverage existing powers and capabilities to build a comprehensive cyber security framework.

17. For example, consideration could be given to utilising the Australian Information Commissioner's code-making powers to further enhance requirements that prevent information loss attributable to cyber intrusion.[14] Under the Privacy Act, the Commissioner has the power to approve and register an enforceable 'APP Code', which could impose additional and particular requirements in relation to cyber security related information handling practices under the APPs.

18. Additionally, mandating the requirement to conduct a Privacy Impact Assessment (PIA) in specified circumstances may assist to ensure that any impacts on privacy are reasonable, necessary and proportionate in the circumstances. A PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. For Australian Government Agencies covered by the *Privacy (Australian Government Agencies – Governance) APP Code 2017*, a PIA is a mandatory requirement for high privacy risk projects.[15]

19. Further co-operation and information sharing on cyber security incidents, vulnerabilities, threats and trends, would help agencies to provide more comprehensive advice to regulated entities and the public, and to more efficiently and effectively act to mitigate the harms caused by cyber security events. In some instances, co-operation through referral powers or information sharing arrangements may need to be facilitated by legislative reform.

20. For example, while the OAIC is notified of cyber intrusions through the NDB scheme, the ability of the OAIC to share that information with the Australian Cyber Security Centre (ACSC) is currently limited. This means that the ACSC's risk assessments may not be fully informed by information held by the OAIC. This can also create challenges for the OAIC and ACSC to work collaboratively to mitigate those risks.

---

[11] See the *Public Governance, Performance and Accountability Act 2013* (Cth)

[12] Available at: <https://www.protectivesecurity.gov.au/>

[13] Available at: <https://www.cyber.gov.au/ism>

[14] The Australian Information Commissioner may make 'APP Codes' (as defined by section 26C of the Privacy Act), under Part IIIB of the Privacy Act.

[15] A high privacy risk project is one the 'agency reasonably considers …involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals' (cl. 12.1 of the *Privacy (Australian Government Agencies – Governance) APP Code 2017*).

21. In addition to information sharing, the OAIC agrees that sharing of technical cyber security expertise across Government could assist Commonwealth agencies to manage their own cyber risks and enable agencies to better support regulated entities to manage cyber risk.

22. For example, drawing on technical cyber security expertise from across Government assists the OAIC to effectively carry out guidance, assessment and enforcement functions. Putting in place frameworks to formalise opportunities to share expertise would assist the OAIC and other regulators and agencies to carry out cyber security related functions in a harmonised way. Technical expertise sharing could potentially be achieved by ensuring that all cyber security agencies are equipped with advisory functions in enabling legislation.

Business

23. Identifying, implementing and maintaining appropriate protection against cyber threats is complex, requiring individuals to navigate complicated legal and technical frameworks and understand specialist ICT concepts. In this environment, as recognised in the Discussion Paper, informational asymmetries and the current onus on individuals to self-manage or take a dominant role in their cybersecurity can create a high level of risk for people operating in an online environment. The OAIC supports a greater role for providers of software services, infrastructure and internet platforms in supporting the cyber security of their customers.

24. As principles-based law, the APPs are technology neutral, flexible, and can adapt to changing and emerging technologies. However, as acknowledged by the Australian Law Reform Commission in its report 'For Your Information: Australian Privacy Law and Practice', this principles-based approach 'does not foreclose the possibility of technology specific regulation or legislative instruments in certain circumstances'.[16]

25. The OAIC supports opportunities to enhance the current privacy framework through the introduction of additional and specific measures in relation to information security, including the implementation of an accreditation or certification framework.

26. Accreditation or certification schemes may help to rebalance the information asymmetry and risk between individuals and providers of ICT products and services – particularly as effective cyber protection is complex and evolving. A cyber security accreditation or certification scheme could assist individuals to differentiate the cyber security expertise and credentials of software services, infrastructure and internet platform providers.

27. The Australian Competition and Consumer Commission's (ACCC) Final Report for the Digital Platforms Inquiry considered that a third-party privacy audit or certification scheme could help increase the transparency of organisations' data practices and reduce information asymmetries between individuals and digital platforms.[17]

28. An accreditation scheme has been created under the Consumer Data Right (CDR) model, which provides a safe mechanism for individuals and businesses to direct data holders to share their data with accredited third parties.

29. The Cross Border Privacy Rules (CBPR) is an international privacy certification scheme that allows entities to be certified as having data privacy policies and practices that are compliant

[16] Chapter 10 of Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC Report 108, Canberra, available at < https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/>

[17] Australian Competition and Consumer Commission, *Digital Platforms Inquiry, Final Report*, ACCC, Canberra (26 July 2019), available at <https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry>

with the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[18] This global scheme enables companies to have their privacy practices assessed by an accredited Accountability Agent, and assists consumers to make informed privacy decisions. Australia has also been endorsed as a participating economy in the APEC CBPR.[19] The OAIC will be responsible for regulating the CBPR in Australia, once implemented.

30. The OAIC considers that an accreditation or certification scheme may assist entities to meet their obligations under the Privacy Act while providing consumers with evidence-based information about the cyber credentials of entities with which they may engage.[20] This could give individuals greater confidence in the information handling and cyber security practices of entities handling their personal information. Any such scheme would necessarily entail a consideration of cyber security practices as part of compliance with APP 11.

Individuals

31. Australia's 2020 Cyber Security Strategy has a strong focus on awareness-raising, to empower individuals, businesses and government agencies to take steps to identify and manage cyber risks.

32. The OAIC supports strategies to increase the awareness and understanding of Australian consumers in relation to cyber security. We note that a human element is a common trend in the OAIC's NDB data (in approximately 35% of notified breaches) and is also a dominant cause in data breaches that resulted from a malicious or criminal attack (approximately 60%). This may have involved an employee clicking on a link that resulted in the compromise of user credentials, or an individual sending personal information to the wrong person. Consistent with the OAIC's observations, the Discussion Paper recognises that human behaviour is one of the most significant vulnerabilities exploited by actors committing cybercrimes.

33. Raising awareness about these cyber risks can empower entities and individuals with capabilities to identify and manage these risks and take steps to protect their own personal information or the information that they hold.

34. The Australian Government currently runs several awareness campaigns designed to raise awareness of rights, obligations and responsibilities around information protection and cyber security. For example, the Australian Cyber Security Centre's (ACSC) annual Stay Smart Online campaign,[21] and the OAIC's annual Privacy Awareness Week campaign, which is undertaken in conjunction the Asia Pacific Privacy Authorities Forum and includes Australian State and Territory and international privacy regulators.[22] Guidance and standards on cyber security also exist, including the OAIC's *Guide to securing personal information* and the Australian Security and Investments Commission's *Cyber resilience good practices*.[23] There are also widely used

[18] Currently the eight participating economies are USA, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, and Chinese Taipei. Only the USA, Japan and Singapore have fully implemented the CBPR.

[19] Australia is currently in the process of implementing the CBPR domestically.

[20] See the OAIC's, *Submission to the ACCC Digital Platforms Inquiry preliminary report* <https://www.oaic.gov.au/engage-with-us/submissions/digital-platforms-inquiry-preliminary-report-submission-to-the-australian-competition-and-consumer-commission> for where the OAIC has previously recommended independent third party certification as a proactive method to increase organisational accountability.

[21] See <https://www.staysmartonline.gov.au/>

[22] See <https://www.oaic.gov.au/engage-with-us/privacy-awareness-week/>

[23] Available at: <https://asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/cyber-resilience-good-practices>

non-government standards published by organisations like the International Organisation for Standardisation.

35. The OAIC recommends building on the success of these campaigns with national, whole-of-government education campaigns, to raise awareness in the Australian community about cyber risks and ways to mitigate online harms. In particular, there is still work to be done to address the human factor in relation to data breaches and cyber incidents.[24]

36. A national campaign could leverage the expertise of relevant Australian Government agencies and other stakeholders, such as not-for-profit organisations and State and Territory Government agencies. The OAIC would welcome involvement in such a campaign from a privacy and information security perspective. This could include collaborating with relevant agencies such as the ACSC and Department of Home Affairs on a joint communications strategy.

Responses to cyber intrusion

37. The OAIC agrees that a central component of Australia's 2020 Cyber Security Strategy should be robust regulatory and enforcement regimes, including in relation to Australia's privacy framework, which is essential to protecting personal information against cyber threats.

38. Under the Privacy Act, there are a range of remedies available where the Australian Information Commissioner finds that there has been an interference with privacy by an entity, including as a result of a cyber intrusion. Entities may be required to take steps to address the matter, apologise, make changes to their practices or procedures, introduce mandatory staff training, pay compensation to the complainant for financial or non-financial loss or provide other non-financial compensation. The Australian Information Commissioner may make a determination or accept an enforceable undertaking from entities to mandate these steps.

39. The Australian Information Commissioner may also seek civil penalties for serious or repeated practices that constitute an interference with privacy.[25] Currently, the civil penalty that may be awarded is 2000 penalty units, or $2.1M.

40. In order to be an effective deterrent, it is important that the penalty is commensurate with the nature and consequence of the breach and the entity involved. The OAIC considers that the penalties for breaches of the Privacy Act should at least mirror whichever is the highest of the increased penalties for breaches of the Australian Consumer Law, or the penalties under the European Union's General Data Protection Regulation (GDPR). The Government announced its intention to increase penalties under the Privacy Act in March 2019,[26] which the OAIC supported in its response to the Digital Platforms Inquiry final report.

41. Strong penalties are required to disincentivise non-compliance and effect behavioural change across all entities. For penalties to act as effective deterrence for large multinational corporations, it is important that maximum penalties cannot easily be absorbed as a minor cost

[24] The OAIC's Notifiable data breaches statistics show that since the commencement of the scheme in February 2018, at least a third of data breaches have been caused by human error <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/>

[25] S 13G of the Privacy Act

[26] See <https://www.minister.communications.gov.au/minister/mitch-fifield/news/tougher-penalties-keep-australians-safe-online>

of doing business in Australia. This recommendation is consistent with an international trend of increasing penalties for breaches of data protection laws.[27]

42. However, there are some limitations to the OAIC's regulatory responses. In the event the OAIC becomes aware of a cyber-related data breach under the NDB scheme, the Australian Information Commissioner has no formal powers to direct an entity to take immediate, short-term steps to mitigate serious harm to affected individuals. Rather, the power to make such an order arises following the completion of an investigation and a determination made by the Australian Information Commissioner. Similarly, the Australian Information Commissioner can only apply to the Federal Court for an injunction when an entity has engaged, is engaging or is proposing to engage in an act or practice that contravenes of one or more of the APPs.

43. The power to make a short-term order to compel an entity to take specified, reasonable steps to mitigate serious harm following an NDB may provide additional protection to individuals affected by the data-breach by reducing serious harm to individuals who are victims of cybercrime. Such powers could be considered as part of a broader review of the Privacy Act as suggested by the Digital Platforms Inquiry final report and supported by the OAIC.

44. For enforcement to be effective, regulatory frameworks must be supported by adequate resourcing. While the OAIC welcomes recent Government commitments to increase the OAIC's resources,[28] any review of Australia's cyber security arrangements should ensure that the OAIC is adequately resourced to provide effective oversight of entities and drive best practice in personal information security.

45. Finally, the OAIC also suggests that consideration be given to the introduction of a statutory cause of action for serious cyber deficiencies in the goods and services provided to Australian consumers by digital service providers, as an additional regulatory response to cyber intrusion and the risks that cyber intrusions pose to individuals. The ACCC's Final Report for the Digital Platforms Inquiry recommended the introduction of a statutory cause of action for serious invasions of privacy. The OAIC recommends that such a statutory cause of action be supplemented by legislative powers for the OAIC to be notified of, to exercise a right to intervene in proceedings, and to seek the leave of the court to act in the role of amicus curiae in the proceedings, where the proceedings involve a misuse of personal information. This will be important where proceedings have the potential to impact the evolution of the Privacy Act and privacy jurisprudence and policy.

Global coordination and interoperability

46. To maximise the effectiveness of Australian privacy regulatory framework in protecting personal information, including through cyber security, it is important to ensure alignment where appropriate between Australian laws and international frameworks to promote interoperability and support enforcement cooperation.

47. In relation to privacy, interoperability allows co-operation between the OAIC and other international regulators on cross-border issues and enforcement. However, the benefits of

[27] For example, in the EU there can be administrative fines of up to €20 million or 4% of annual worldwide turnover (whichever is higher): EU GDPR Art 83(6)). In Singapore there can be financial penalties of up to $1million: *Personal Data Protection Act 2012* (Singapore) s 29)).

[28] Available at: <https://www.minister.communications.gov.au/minister/mitch-fifield/news/tougher-penalties-keep-australians-safe-online>

interoperability are not limited to privacy and are likely to apply to other facets of cyber security.

48. As a member of the Executive Council for the International Conference of Data Protection and Privacy Commissioners (ICDPPC),[29] and co-chair of the Digital Citizen and Consumer working group, the Australian Information Commissioner plays a leadership role in improving the interoperability of global privacy frameworks. The Commissioner recently proposed a global resolution, endorsed by the Conference, aimed at addressing the role of human error in data breaches. This resolution called upon ICDPPC members to:

    a. collect, analyse and publish statistics on data breaches notified to them under voluntary or mandatory data breach notification schemes

    b. promote appropriate security safeguards to prevent human errors that can result in data breaches, including establishing effective data protection and privacy practices, procedures and systems, and building workplace cultures where data protection and privacy are organisational priorities

    c. liaise with relevant international and regional networks to promote the resolution.[30]

49. The resolution also called on organisations (including government and business) to understand and recognise that data breaches often involve human error and act to implement appropriate security safeguards.

50. The ICDPPC has also placed a significant focus on global enforcement cooperation through its Working Group on International Enforcement Cooperation. The Working Group recently released its final report into international enforcement cooperation and has established a repository to share non-confidential, publicly available information about enforcement activities with members.

51. Steps to develop globally aligned privacy regulation and ensure effective trans-national coordination provide enhanced privacy protections to Australians. The corollary is that the enhanced privacy protections – particularly through strong security – contribute to an increased cyber resilience.

52. The OAIC contends that the agile, global nature of serious cyber threat actors supports the view that global alignment, and opportunities for trans-national cooperation in relation to combating cybercrime, similarly offer the strongest protections for Australians.

Assistance to victims

53. There is a clear role for the private and not-for-profit sectors to play in minimising serious harm to individuals caused by cybercrime. The OAIC acknowledges the ongoing work of Australia and New Zealand's national identity and cyber support service, IDCARE, in helping individuals and organisations reduce the harm they experience from cybercrime.

[29] We note that at the 41st ICDPPC Conference in Albania, the conference members moved to adopt a new name; the 'Global Privacy Assembly'. It is anticipated that this name change will be made official in mid-November.

[30] International Conference of Data Protection and Privacy Commissioners 2019, *Resolution to address the role of human error in personal data breaches*, 41th International Conference of Data Protection and Privacy Commissioners, October 2019, Tirana.

54. Further development of integrated and coordinated response frameworks for private sector organisations to respond to cybercrimes will assist victims to minimise harm and recover from incidents.

55. In acknowledging the role that the private sector can play in remediation and restoration frameworks, the Government may nonetheless have some stewardship, coordination or facilitative role to play to ensure a base level of protection exists economy-wide. The OAIC's NDB scheme 12-month insights report recognised that entities should build further community trust by supporting individuals to rectify the negative impacts of breaches when they occur.[31] To that end, further work could be undertaken by Government to ensure that appropriate remediation and support frameworks around cybercrime, identity theft and fraud are put in place.

56. The OAIC is available to engage with the Department of Home Affairs further regarding issues raised as Australia's 2020 Cyber Security Strategy progresses. If you would like to discuss these comments further, please contact Sarah Croxall, Director, Regulation & Strategy, on [redacted] or [redacted].

[31] Available at: <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/>