Australian Government
Office of the Australian Information Commissioner

Parliamentary Joint Committee on Law Enforcement – Inquiry into the capability of law enforcement to respond to cybercrime

Submission by the Office of the Australian Information Commissioner

Angelene Falk
Australian Information Commissioner and Privacy Commissioner
22 December 2023

OAIC

December 2023

Contents

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Law Enforcement's Inquiry into the capability of law enforcement to respond to cybercrime.

2. The OAIC is Australia's independent Commonwealth privacy regulator.[1] We play an important role in the ring of defence that surrounds Australia's cyber security practices, including promoting cyber resilience. The OAIC regulates entities subject to the *Privacy Act 1988* (Privacy Act) and other laws[2] to safeguard Australians' personal information. This includes the obligation on entities to take reasonable steps to ensure that personal information is appropriately protected from misuse, interference and loss, unauthorised access, modification or disclosure under Australian Privacy Principle (APP 11) and complying with obligations under the Notifiable Data Breach (NDB) scheme.[3] The security of personal information is a key regulatory priority for the OAIC.[4]

3. This inquiry comes at a pivotal time when Australians are acutely aware of the very real risks of cybercrime and are seeking more control over the collection and use of their personal information.[5] Recent high profile data breaches in Australia have resulted in a strong community expectation that entities' personal information handling practices are robust and secure. As reflected in the OAIC's Australian Community Attitudes to Privacy Survey (ACAPS), 74-percent of Australians feel data breaches are one of the biggest privacy risks they face today.[6]

4. Privacy regulation is a critical law which underpins Australia's cyber security framework in a number of important ways. It supports both the prevention of cybercrime and harm minimisation following an incident. While the OAIC and government play an important role in providing support, information and resources to assist entities to uplift cyber resilience and security practices, the primary responsibility for preventing breaches, including cybercrime, and protecting data in accordance with the Privacy Act, rests with the entities themselves.

5. The volume and granularity of personal information that is collected by entities, combined with other practices such as profiling, monitoring, tracking, and unnecessary retention of data, amplifies privacy and security risks. Therefore, it is important that Australia can respond to this threat in an appropriate manner. Implementation of the recommendations made in the Australian Government's Privacy Act Review Report will ensure Australia's privacy framework remains fit for purpose in the digital economy. Further, the Australian Government's Cyber Security Strategy provides an opportunity to uplift established security obligations for personal information handling and ensure a consistent, whole-of-government approach to preventing and responding to cybercrime.

---

[1] The OAIC is an independent Commonwealth regulator, established to bring together three functions: privacy functions (protecting the privacy of individuals under the *Privacy Act 1988* (Cth), freedom of information (FOI) functions (access to information held by the Commonwealth Government in accordance with the *Freedom of Information Act 1982* (Cth), and information management functions (as set out in the *Australian Information Commissioner Act 2010* (Cth) (AIC Act).
[2] We note that a number of other Australian laws other than the *Privacy Act 1988* also relate to privacy see: https://www.oaic.gov.au/privacy/privacy-legislation/related-legislation.
[3] See *Privacy Act 1988* (Cth) sch 1 and Part IIIC.
[4] OAIC, *Corporate plan 2023-24*, p 29.
[5] OAIC, *Australian Community Attitudes to Privacy Survey 2023*, p 18.

6. Given the threat of cybercrime, Australia's regulatory response must also be sufficiently agile, efficient and effective to keep pace. The OAIC is working collaboratively with other Australian regulators and international counterparts to understand, respond to, and share information about cyber security risks and incidents impacting privacy. We will continue to engage with relevant domestic and international regulators to support us to perform our regulatory functions through enhanced intelligence, investigation and regulatory practices.

7. In this submission, we make 4 recommendations to assist the Committee in its consideration of current responses to cybercrime, including how effective privacy regulation can promote and enhance cyber security outcomes in Australia.

Privacy regulation is critical to effective cyber security

8. Recent high profile data breaches in Australia have brought a renewed focus on cyber security among government, business and individuals. The Australian community is keenly aware of the very real risks that come with the opportunities of a digital economy and operating online.

9. Privacy and cyber security are inextricably interwoven and when an entity's cyber security fails, individual's privacy can be compromised. This can have significant impacts on the community. As personal information becomes increasingly available to malicious actors through data breaches, the likelihood of other attacks, such as targeted social engineering, impersonation fraud and scams, increases. The OAIC's ACAPS indicates that 76-percent of people whose data was involved in a breach said they experienced harm as a result.[7]

10. It is important that Australia's ring of defence for cyber security includes the appropriate tools to ensure prevention as well as minimisation where cybercrime occurs. As the Australian Signal's Directorate's Cyber Threat Report 2022-23 notes, protecting data, particularly sensitive personal information, is vital for the safety of the community, the prosperity of business, and the nation's security.[8]

11. However, it is essential that responsibility for cyber security is appropriately aligned within our digital ecosystem with those that are best positioned to reduce risk. Many Australian entities do not have the capability or expertise to assess the security standard of software products or services. Entities rely on digital products which may have inherent vulnerabilities in their design that can be exploited. The OAIC welcomes the Australian Government's initiative to adopt international security standards for digital products, ensuring entities can trust that their digital products and services are safe, secure and fit for purpose.[9] The OAIC considers that it is better to manage privacy risks proactively by embedding good privacy and security practices into the design specifications and architecture of new systems and processes, rather than to retrospectively alter digital products to address privacy and security risks that come to light. As the trusted national independent privacy regulator, the OAIC plays an essential role in providing advice, assurance, and where appropriate, taking enforcement action, to ensure entities are adhering to best practices.

12. Privacy regulation is key to uplifting Australia's cyber security posture, contributing to the prevention and investigation of cybercrime and the protection of Australians' personal

[7] OAIC, *Australian Community Attitudes to Privacy Survey 2023*, p 10.
[8] ASD, *ASD Cyber Threat Report 2022-2023*, p 45.
[9] Department of Home Affairs, *2023-2030 Australian Cyber Security Strategy Action Plan*, p 29.

information. The OAIC plays an important role in providing entities with guidance to equip them with resources to comply with their privacy obligations. The OAIC works with entities to facilitate legal compliance and best privacy practices to increase awareness of privacy risks, including the threat of cybercrime, and prevent the risk of data being compromised, or misused. The OAIC also publishes twice-yearly reports on statistical information about notifications received under the NDB scheme to help entities understand privacy risks, including the causes of data breaches.[10].

13. One of the OAIC's powers is to conduct a privacy assessment of most Australian Government agencies and some private sector organisations (APP entities) covered by the Privacy Act, including law enforcement.[11] The OAIC uses assessments to facilitate legal and best practice compliance by identifying and making recommendations to address privacy risks to the effective handling of personal information by an entity, and areas of non-compliance with relevant legislation.[12]

14. A key focus of the OAIC's privacy assessments is to ensure that personal information held by APP entities is being maintained and handled in accordance with the APPs.[13] This includes building the capacity of APP entities to comply with APP 11, which requires APP entities to take reasonable steps to protect the personal information they hold, including monitoring the effectiveness of ICT security measures to ensure that they remain responsive to changing cyber threats and cybercrime.

15. The OAIC decides whether or not to take regulatory action in accordance with its Privacy regulatory action policy,[14] including whether investigation and enforcement action will act as a future general deterrent to entities, as well as encourage the implementation of privacy best practice and compliance with legislative requirements.

16. Following a significant investigation, on 3 November 2023, the Information Commissioner commenced civil penalty proceedings in the Federal Court against Australian Clinical Labs Limited (ACL), in connection with a data breach which occurred in February 2022. In these proceedings, the Commissioner alleges that ACL seriously interfered with the privacy of millions of Australians by failing to take reasonable steps to protect their personal information from unauthorised access or disclosure in breach of the Privacy Act. The Commissioner further alleges that these failures left ACL vulnerable to a cyberattack.[15]

17. This investigation highlights the importance of appropriate resources for regulators to conduct timely and effective investigations where significant cybercrime occurs.

18. The investigation into ACL also highlights how important it is that entities take reasonable steps to protect personal information they hold, and that they consider the volume and size of their information holdings. Equally important is whether they are required under legislation to destroy

---

[10] See OAIC, *Notifiable Data Breaches Report: January to June 2023*.

[11] Australian Government agencies (and the Norfolk Island administration) and organisations with an annual turnover more than $3 million have responsibilities under the Privacy Act, subject to some exceptions; *Privacy Act 1988* (Cth) s 33C.

[12] This may include, for example, the APPs, *Privacy (Credit Reporting) Code 2014*, Consumer Data Right privacy safeguards or requirements for the handling of Tax File Numbers.

[13] *Privacy Act 1988* (Cth) s 33C(1)(a)(i).

[14] OAIC, *Privacy regulatory action policy*, p 5.

[15] OAIC, *OAIC commences Federal Court proceedings against Australian Clinical Labs Limited*.

or de-identify information once it is no longer needed for any purpose under the APPs.[16] This is especially important where the information is highly sensitive.

Balancing effective regulation with access to trusted support

19. As noted earlier in this submission, while government plays an important role in providing support, information and resources to assist entities to uplift cyber resilience and security practices, the primary responsibility for preventing breaches and protecting data in accordance with the Privacy Act, rests with the entities themselves.

20. As part of a range of measures in the Australian Cyber Security Strategy 2023-2030, the Australian Government supports the development of a 'limited use' obligation.[17] This obligation seeks to encourage industry to share information with the Australian Signals Directorate (ASD) or the National Cyber Coordinator following a cyber incident, by providing comfort to industry that the information will not be used for compliance or punitive purposes.

21. The OAIC's view is that any such obligation needs to be developed carefully and subject to clear boundaries so that regulatory activity in the public interest is not impeded. In particular, it is important that any confidentiality obligations do not impede the current reporting obligations under the OAIC's NDB scheme nor subvert the OAIC's regulatory role. Ultimately, entities must comply with their legal obligations under the Privacy Act, including their NDB reporting obligation and the obligation to take reasonable steps to protect their data under APP 11.

22. While the OAIC appreciates the importance of immediate collaboration and information sharing between affected entities, and the ASD and the National Cyber Coordinator to facilitate an effective immediate response to cyber incidents, there is a need to balance the facilitation of industry cooperation during an incident with the ability of regulatory agencies to enforce laws and deter non-compliance at an appropriate time.

Recommendation 1 – That the limited use mechanism is carefully designed in consultation with regulators so that it does not preclude regulatory action in the public interest or impact any legislative reporting requirements, including for the OAIC.

Making Australian entities more resilient to cyber security threats

23. A key goal of the OAIC is to make Australian entities more resilient to cyber security threats by providing advice and guidance to individuals and entities about steps to secure personal information; increasing awareness about the causes of data breaches and prevention strategies; advising entities that experience a breach to contain and remediate; and taking regulatory action.

[16] *Privacy Act 1988* (Cth) APP 11.2.
[17] Department of Home Affairs, *2023-2030 Australian Cyber Security Strategy Action Plan*, p 9.

24. The Privacy Act includes well-established security requirements, including obligations under the APPs, in particular APP 1 and APP 11, and the NDB scheme.[18] These requirements could be said to provide a 'baseline' level of security protections across the whole economy for personal information. In conjunction with the deterrent value of strategic regulatory action, the baseline protections of the NDB scheme uplift cyber security practices across regulated entities, reducing opportunities for cybercriminals.

25. Under the NDB scheme, regulated entities must notify affected individuals and the Australian Information Commissioner when a data breach is likely to result in serious harm to an individual whose personal information is involved. The NDB scheme is now a mature model and the OAIC expects that entities will have strong personal information security practices and systems in place to ensure a timely response to data breaches and compliance with the requirements.

26. The OAIC ensures compliance with the NDB scheme, including by handling complaints, conducting inquiries and investigations into data breaches and taking other regulatory action. The NDB scheme is a critical element of Australia's current framework supporting the prevention of cybercrime and harm minimisation following an incident and must be considered in any future response model.

Recommendation 2 – The OAIC is appropriately resourced to exercise its powers and functions under the Privacy Act, including regulating the NDB scheme, and the integrity of the NDB scheme is preserved.

Uplifting cyber security in Australia

27. The OAIC welcomes the Australian Government's response to the Attorney-General's Department's (AGD) review of the Privacy Act as a crucial step in ensuring Australia's privacy framework is strengthened for the future. Implementation of the reforms in the Privacy Act Review Report provide an important opportunity to uplift existing security obligations. In conjunction with the Australian Cyber Security Strategy 2023-2030, the reforms will enhance cyber security across the economy.

28. The Privacy Act Review Report contains 116 proposals for reform that seek to ensure the Privacy Act remains 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.[19] The proposals include changes to the Privacy Act's enforcement framework to ensure the OAIC has the appropriate regulatory toolkit to respond effectively to privacy harms and emerging threats in a strategic and proportionate way. These changes to existing enforcement powers are key to enabling the OAIC to take a more targeted approach to enforcement and use its resources to secure the greatest benefit for Australians and the regulated community.

[18] *Privacy Act 1988* (Cth) pt IIIC.
[19] AGD, *Privacy Act Review Report*, p 251.

29. In relation to the security and retention of data, the Government has agreed in principle:

    - that entities should be required to comply with baseline privacy outcomes (proposal 21.2). It is proposed that APP 11 include a list which outlines the baseline privacy *outcomes* APP entities should consider when taking reasonable steps to protect the personal information they hold. AGD has highlighted the approach under the European Union's General Data Protection Regulation (GDPR) as an example, for instance, under Article 32 it is a requirement that entities have the 'ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services which hold personal information.'
    - that organisations should be required to establish maximum and minimum retention periods for personal information, and specify these in their privacy policies (proposals 21.7 and 21.8).
    - to review all legal provisions requiring retention of personal information to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information (proposal 21.6).
    - that the small business exemption under the Privacy Act should be removed in light of the privacy risks applicable in the digital environment, (proposal 6.1).

30. The OAIC supports taking forward these proposals as measures to uplift the security practices of organisations, in particular the OAIC supports the removal of the small business exemption, noting that a significant proportion of businesses in Australia are not subject to the Privacy Act.[20]

31. In relation to enforcement, the Government has agreed:

    - to the creation of tiers of civil penalty provisions to allow for better targeted regulatory responses, in particular the introduction of a new mid-tier civil penalty provision to cover interferences with privacy which do not meet the threshold of being 'serious', and a new low-level civil penalty provision for specific administrative breaches of the Privacy Act and APPs with attached infringement notice powers for the Information Commissioner with set penalties (proposal 25.1).

32. The OAIC considers that the proposals in relation to tiered civil penalties and infringement notices will ensure that the OAIC is able to undertake faster and more effective deterrent action.

33. In relation to the NDB scheme, the Government has agreed in principle:

    - to changes to reporting timeframes namely that entities must:
        - notify the OAIC as soon as practicable, and not later than 72 hours, after becoming aware of an eligible data breach, and
        - notify individuals as soon as practicable, including providing information to individuals in phases if it is not practicable to provide the information at the same time.

[20] As at June 2021, it was estimated that less than 5 per cent of businesses actively trading in the Australian economy had an annual turnover of more than $3 million and consequently obligations under the Privacy Act. This estimate was prepared for the OAIC using ABS counts of Australian Businesses, including entries and exits. Note this estimate does not include exceptions to the small business exemption.

- that entities should be required to take reasonable steps to implement practices, procedures and systems to respond to a data breach (proposal 28.2).

34. The Government has also signalled that further consultation should be undertaken on whether entities should be required to take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a data breach.

35. The OAIC considers that this is an important measure warranting further consideration as there is currently no express requirement in the Privacy Act for an entity to take any steps to reduce the harm that is likely to result to individuals, and provide support, as a result of the data breach. We have observed that best practice entities take responsibility for the costs and impacts of data breaches when they occur, and support individuals to mitigate the impact of a data breach.

36. The steps that may be reasonable to take depending on the circumstances may include setting up support lines to provide customers centralised channels to ask questions and find out what they can do to reduce harm, paying for a subscription to a credit monitoring service which alerts affected individuals if there are changes to their credit report, assisting individuals to replace compromised credentials such as passports and drivers licences, and engaging providers such as IDCARE to provide post-incident support to individuals.

37. With increasing use of high impact technologies, it is critical that the Privacy Act Review reforms proceed as a priority alongside other key initiatives that rely on a strong privacy foundation, such as the Australian Cyber Security Strategy 2023-2030 and Digital Identity framework, which also contribute to mitigating the risk of cybercrime.

Recommendation 3 – The Government progress reforms which have been agreed in principle and agreed in the Privacy Act Review Report as a matter of priority to ensure the Privacy Act remains fit for purpose in an environment where the personal information of Australians is collected and used for a myriad of purposes in the digital economy and they are increasingly at risk of cybercrime.

Working collaboratively with other domestic and international regulators

38. As the digital world continues to evolve and malicious actors find new and emerging ways to attempt to access data, it is important that Australia look to its international counterparts to ensure consistency, and to learn from emerging technologies and trends.

39. The OAIC prioritises collaboration with domestic and international regulators to continue to address the complexities of new and emerging types of cybercrime. These issues can intersect with a number of regulatory regimes, and it is important for regulators to work together to avoid unnecessary or inadvertent overlap for consumers and industry. While there may be intersections, it is important to acknowledge that these regulatory frameworks address different economic and consumer risks. In this way, the various regimes are essential and complementary components to address the risk and harms of cybercrime faced by Australians. An effective approach requires

complementary expertise, and collaboration and coordination between regulators to ensure proportionate, efficient and cohesive regulation.

40. The OAIC considers that collaboration with other Australian regulators is key to understanding, responding to, and sharing information about cyber security risks and incidents impacting privacy. As a founding member of the Cyber Security Regulator Network (CSRN), we are collaborating with other Australian regulators to meet the challenges posed by the current environment. The CSRN comprises the Australian Prudential Regulation Authority (APRA), OAIC, the Australian Securities and Investments Commission (ASIC), the Australian Communications and Media Authority (ACMA), and the Australian Competition and Consumer Commission (ACCC). The Cyber and Infrastructure Security Centre (CISC), Reserve Bank of Australia (RBA) and Treasury are standing attendees. Through this collaboration, the CSRN is uniquely positioned to consider and advise on opportunities to reduce duplication or gaps in regulatory responses and improve the effectiveness and efficiency of regulatory activity. Its current focus is on cyber incidents and information sharing between regulators to identify appropriate responses to future incidents and to ensure collaboration can occur quickly and effectively.

41. The OAIC considers that greater collaboration between regulators, supported through legislative amendment where appropriate and necessary, will uplift Australia's cyber resilience and security and promote a 'whole-of-government' regulatory approach to addressing cyber risks, including cybercrime. In this regard, the OAIC notes that the *Privacy Amendment (Enforcement and Other Measures) Act 2022* (Cth) which commenced in December 2022 enhanced the Commissioner's information-sharing powers and ability to work collaboratively with other regulators.

42. Increasingly, challenges extend beyond national borders. In light of this, a coordinated international approach can also be effective to responding to challenges that impact upon privacy and data protection, including cybercrime. It is essential to ensure that Australia's frameworks are fit for purpose and align with best practice.

43. The OAIC will continue to lead and engage with both domestic and international regulators to shape the global regulatory environment, and to advance higher standards of privacy and data protection around the world to address privacy challenges, including the threat that cybercrime poses.

Recommendation 4 – Collaboration and information sharing mechanisms, supported through legislative amendment where necessary, should be encouraged to reduce the regulatory burden on entities and ensure a consistent, whole-of-government regulatory approach to uplifting Australia's cyber security and resilience.