Australian Government

Office of the Australian Information Commissioner

Strengthening Australia's cyber security regulations and incentives

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

27 August 2021

OAIC

Contents

Introduction

1.1 The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to make a submission to the Department of Home Affairs (Home Affairs) on the discussion paper, 'Strengthening Australia's cyber security regulations and incentives' (the Discussion Paper).

1.2 The Discussion Paper is seeking views about how the Australian Government can incentivise businesses to invest in cyber security, including through adjusting policy and regulatory settings. This work forms part of Australia's Cyber Security Strategy 2020[1] and complements the Government's critical infrastructure reforms[2] and the Review of the *Privacy Act 1988* (Cth) (Privacy Act).[3]

1.3 The Discussion Paper identifies the link between protecting personal information and addressing cyber security risks. The OAIC, as the federal privacy regulator, has a clear role to play in the cyber security landscape and supports the important policy objectives in the Discussion Paper, including to set clear cyber security expectations for government, businesses, and the community.

1.4 The OAIC has engaged with the Australian Government over several years on matters related to privacy and cyber security. It will continue to support policy objectives to increase the cyber security posture of Australian businesses and the awareness of individuals through the regulation of strong privacy protections. The OAIC has a unique role, as a regulator, in bridging the shared responsibility of Government, business and the community in addressing cyber security risks.[4] The protection of information (including personal information) is a core aspect of cyber security resilience.

1.5 The OAIC and the protection of personal information are an essential part of the ring of defence to protect Australia's cyber security. In particular, the Privacy Act includes well-established security requirements, particularly through Australian Privacy Principles (APPs) 1 and 11 and the Notifiable Data Breaches (NDB) scheme. The Privacy Act also contains effective mechanisms that allow the APPs to be supplemented by more specific rules through the APP code-making provisions in Part IIIB. Furthermore, the OAIC has identified the security of personal information as a central regulatory focus.[5]

1.6 The Discussion Paper explores opportunities within Australia's current legal framework to achieve Government's goal to be a leading digital economy by 2030.[6] The OAIC supports leveraging existing mechanisms to address the shared risks to privacy and cyber security. This submission outlines the existing mechanisms that the Australian Government and the OAIC can use to realise the economic and societal benefits of strong cyber security. This submission also

[1] Department of Home Affairs, *Australia's Cyber Security Strategy 2020*.
[2] Department of Home Affairs, *Protecting Critical Infrastructure and Systems of National Significance*.
[3] Attorney General's Department, https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988.
[4] Most recently, the OAIC has participated as a member of the Cyber Security Best Practice Regulation Taskforce. The OAIC has also made a submission to Home Affairs on the Cyber Security Strategy and to the Parliamentary Joint Committee on Intelligence and Security on the Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020.
[5] Office of the Australian Information Commissioner, *Privacy Regulatory Priorities 2020-2021* .
[6] Department of Home Affairs, *'Strengthening Australia's cyber security regulations and incentives' Discussion Paper*, page 16.

provides suggestions to further strengthen current frameworks to address the clarity, coverage and enforcement limitations identified in the Discussion Paper.

The current framework: interconnected nature of privacy and cyber security

1.7 Privacy regulation plays an important role in uplifting Australia's cybersecurity posture. Whilst the Privacy Act applies specifically to the handling of personal information, in practice strong privacy compliance is likely to uplift the cyber security posture of entities generally. Most entities collect and hold some personal information and many are likely to have information handling processes or systems for both personal information and other types of information.

1.8 The Privacy Act includes well-established security obligations. Most relevantly, cyber security is recognised as a necessary privacy protection and key consideration for entities taking 'reasonable steps' to satisfy their obligations under APP 1 and 11.[7] The NDB scheme is another important part of the cyber security landscape: the mandatory reporting of breaches to the regulator and affected individuals provides visibility of compliance with relevant security standards and allows affected individuals to mitigate personal risk.

APP 1 requirements

1.9 Under APP 1, entities must 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. This 'privacy by design' approach under APP 1 supports strong cyber security practices by establishing measures which prevent the misuse, interference, loss or unauthorised accessing, modification or disclosure of personal information. This approach also ensures entities detect privacy breaches promptly and are ready to respond to potential privacy breaches (including cyber incidents) in a timely and appropriate manner.

APP 11 requirements

1.10 In complying with APP 11, businesses are required to take reasonable steps to protect the personal information they hold, which includes actively monitoring their cyber risk environment for emerging threats and implementing appropriate mitigation strategies. This is a dynamic responsibility which scales proportionately to the volume and sensitivity of personal information held by an entity, the nature and size of the entity and the threat environment in which it operates.

NDB scheme

1.11 The NDB scheme requires entities covered by the Privacy Act to carry out an assessment whenever they suspect that there may have been a loss of, unauthorised access to, or unauthorised disclosure of personal information that they hold. If serious harm is likely to result to an individual, entities must notify the OAIC and also affected individuals so they can take actions to address the possible consequences. Malicious or criminal attacks remain the

[7] Office of the Australian Information Commissioner 2018, Guide to Securing Personal Information, OAIC, Sydney.

leading source of data breaches (65%) notified to the OAIC, with 66% of these involving a cyber incident.[8]

1.12 The NDB scheme incentivises entities to improve security standards in relation to the protection of personal information, including cyber resilience.

Getting the right regulatory settings: Cyber Security Code for personal information

1.13 The Discussion Paper identifies the following limitations within Australia's current legal landscape in addressing cyber security:

a. Clarity of expectations for regulated entities

b. Limited coverage of appropriate entities and

c. Limited enforcement in a cyber security context.[9]

1.14 The OAIC supports the proposed development of an APP Cyber Security Code (Cyber Security Code) to provide clarity to the regulated community about the cyber security requirements of APP 11. The code-making provisions of the Privacy Act are an existing and effective tool to further particularise APP obligations where there is a need to do so.[10]

Clarity of expectations

1.15 The principles-based APPs enable entities to take a risk-based approach to compliance, based on their particular circumstances, including size, resources and business models, while ensuring the protection of individuals' privacy. However, the OAIC acknowledges that there may be areas that require further certainty or specificity. As noted above, the Privacy Act provides the legislative flexibility through the code-making provisions to adapt and particularise the law where appropriate, while maintaining the broader principles-based approach of the APPs.

1.16 Accordingly, the OAIC supports the development of an APP Cyber Security Code with associated resources, as it will assist entities by providing clear expectations on how to meet their existing cyber security obligations under APP 11.

1.17 An APP code sets out how one or more of the APPs are to be applied or complied with, and the particular entities that are bound by the code.[11] In the case of APP 11, an APP code can set out the steps an entity must take to satisfy its cyber security obligations related to personal information under APP 11.

---

[8] Office of the Australian Information Commissioner (August 2021), Notifiable Data Breaches Report January-June 2021.

[9] Department of Home Affairs, *'Strengthening Australia's cyber security regulations and incentives' Discussion Paper*, page 15-16.

[10] Office of the Australian Information Commissioner (2013), Guidelines for developing codes.

[11] Office of the Australian Information Commissioner (2013), Guidelines for developing codes.

1.18 An APP Code can be flexible and scalable to take into account an entities' size, and the sensitivity and amount of personal information it handles.[12] As such, it is possible that an APP Code can achieve the appropriate balance between providing clear steps entities should take, whilst maintaining a principles-based approach that reflects the different technologies and practices of entities. This ensures that entities maintain a risk-based approach to cyber security. Importantly, the Code development process is industry-led, providing opportunities for the regulated community to ensure that the Code is adaptable, technologically-agnostic, proportionate to risk and aligned with existing standards.

1.19 The proposed Cyber Security Code contributes to a number of the objectives set out in the Discussion Paper including by providing greater transparency about information handling practices and promoting cultural change to security postures.

Coverage of appropriate entities

1.20 The Discussion Paper notes that a Cyber Security Code would be limited to entities that are within the jurisdiction of the Privacy Act (generally organisations with an annual turnover of more than $3 million).[13] However, we note that there are existing mechanisms to bring entities into the jurisdiction of the Privacy Act, through either regulatory prescription[14] or voluntarily opt-in.[15] Regulations can also be made to prescribe that certain acts or practices of small business operators will be subject to the Act.[16]

1.21 These mechanisms provide small businesses with the opportunity to benefit from increases in consumer confidence and trust derived from compliance with the Privacy Act, and, by extension, an APP Code. Under the Digital Economy Strategy, the Australian Government has committed to lifting the digital capability of Small-to-Medium Enterprises, with a view to having all future businesses being 'born digital'. The OAIC considers that the protection of personal information is a vital part of doing business in today's digital economy. Appropriate privacy protections create the consumer trust and confidence needed to support economic and social engagement with the product or service, regardless of an entity's size. Ensuring businesses are being established with strong privacy foundations from the outset will also mean that they do not face significant regulatory hurdles in re-building their systems for compliance as they grow. The OAIC has recommended that small businesses should be brought into the jurisdiction of the Privacy Act which includes for the purposes of the proposed APP Code.[17] Ahead of any reform arising from the Privacy Review government could utilise the current mechanisms in the Privacy Act to bring certain small businesses into the coverage of the Act.[18]

---

[12] Office of the Australian Information Commissioner (2017), Australian Government Agencies Privacy Code.

[13] Most notably sections ss 6D(4)(b)-(f), 6E(1A)-(1D), 6D(9) of the Privacy Act stipulate organisations that are subject to the Privacy Act regardless of their annual turnover, including businesses that are a health service provider, trade in personal information, provide services under a Commonwealth contract, credit reporting bodies, operators of a residential tenancy database, accredited under the Consumer Data Right system, amongst others.

[14] *Privacy Regulation 2013* (Cth) s 7.

[15] Privacy Act s 6EA.

[16] Privacy Act ss 6E(1) and 6E(2).

[17] Office of the Australian Information Commissioner (December 2020), Submission to Australian Government's Privacy Act Review Issues Paper.

[18] Privacy Act ss6E(1) and 6E(2).

1.22 Notwithstanding the current jurisdictional limitations set out above, an APP Cyber Security Code could have a flow on effects to small businesses, if it applied to regulated APP entities who supply particular services to small businesses. By ensuring that the services being provided to small businesses met a minimum standard, an APP Cyber Security Code could effectively strengthen the cyber resilience of the supply chain.

Enforcement powers

1.23 The Discussion Paper notes that the regulatory powers conferred on the Commissioner through the Privacy Act are based on an escalation model which focusses OAIC resources on the resolution and conciliation of individual complaints. The OAIC has previously indicated the importance of ensuring that the Privacy Act provides the appropriate regulatory framework and tools to address significant and systemic risks in Australia's growing threat environment.[19]

1.24 To achieve the goal of being a leading digital economy by 2030, the OAIC recommends that the Commissioner be provided with greater discretion to focus the OAIC's resources on significant emerging risks. While complaints provide redress for individuals and serve as a valuable source of intelligence for the OAIC, increased flexibility and discretion in relation to the Commissioner's complaint handling functions will ensure that the OAIC can effectively prioritise matters and direct its resources to resolving issues that have systemic importance or where more serious misconduct or harms have occurred. This will be particularly important for the enforcement of the proposed APP Code.

1.25 While the Privacy Act contains a range of regulatory tools and powers, the OAIC considers that legislative reform is required to ensure that its regulatory and enforcement framework is flexible and responsive to emerging privacy issues in the coming years. The Review of the Privacy Act is considering these issues, and the OAIC's recommendations to that Review are relevant to the Discussion Paper.[20]

Conclusion

1.26 The OAIC considers that strong data protection and privacy rights are an essential link in the ring of defence that is being built to protect Australians in the online environment. Accordingly, cyber security controls and the protection of personal information have complementary roles to play in achieving the Government's agenda to uplift the cyber security of digitally-enabled businesses and to keep Australians safe online.

1.27 The OAIC supports opportunities to enhance the current privacy framework by utilising the existing mechanisms under the Privacy Act to introduce specific measures in relation to cyber security. An uplift in the cyber security protection of personal information through a Cyber Security Code is likely to result in a general elevation of the cyber security resilience of regulated entities. Providing a consistent, comprehensive and unfragmented regulatory

[19] Office of the Australian Information Commissioner (December 2020), Submission to Australian Government's Privacy Act Review Issues Paper.

[20] Office of the Australian Information Commissioner (December 2020), Submission to Australian Government's Privacy Act Review Issues Paper.

framework that addresses this intersection will improve the cyber security of Australian businesses, particularly those operating in Australia's growing digital economy.

1.28 We look forward to advising government on these important initiatives.