Australian Government

Office of the Australian Information Commissioner

5-year Productivity Inquiry: Australia's data and digital dividend Interim report

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

24 October 2022

OAIC

Contents

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to make a submission to the 5-year Productivity Inquiry: Australia's data and digital dividend Interim Report (the Report) released by the Productivity Commission (the Commission) on 23 August 2022. The Report examines the role that data and digital tools and applications can play in Australia's productivity growth.

2. 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) (Privacy Act), freedom of information (FOI) functions (access to information held by the Commonwealth Government in accordance with the *Freedom of Information Act 1982* (Cth) (FOI Act)), and information management functions (as set out in the *Information Commissioner Act 2010* (Cth)).

3. Promoting and upholding privacy and information access rights and supporting the proactive release of government-held information are key strategic priorities for the OAIC.[1] This recognises that data held by the Australian Government is a valuable national resource that can yield significant benefits for the Australian public when handled appropriately and in the public interest.

4. The OAIC's regulatory role and responsibilities also involve and intersect with a range of other laws and whole-of-government initiatives that seek to support digital, data and cyber security activity in the Australian economy, including the *Data Availability and Transparency Act 2022*, the Australian Cyber Security Strategy,[2] the National Data Security Action Plan, and the Digital Identity scheme. The OAIC co-regulates the Consumer Data Right (CDR) scheme together with the Australian Competition and Consumer Commission (ACCC). As part of this, the OAIC enforces the privacy safeguards and related Rules, provides advice to government agencies, and undertakes strategic enforcement in relation to the protection of privacy and confidentiality, to ensure that the CDR provides a secure mechanism in which consumers can share information across the digital economy to realise financial benefits.

5. The acceleration of the digital world has opened the door to increased innovation and economic opportunity but has also resulted in exponential growth in the collection of personal information. Increased collection of personal information combined with other practices such as data sharing, tracking and monitoring have the potential to amplify privacy risks and create new privacy harms. A growing digital economy may also present data security risks such as increased cyber security threats.

6. Realising the economic and social opportunities of the modern digital economy requires public trust and confidence in the data handling activities of government and business, and in the appropriateness of regulatory settings. The public is more likely to support innovative data initiatives when they have confidence in how their data is being handled.

7. The Privacy Act provides a well-established framework for minimising the privacy risks associated with personal information handling activities and facilitating community trust and confidence in

[1] OAIC, *Corporate Plan 2021/2022*, OAIC website, August 2021, accessed 13 October 2022.

[2] The Australian Cyber Security Strategy 2020 was formulated under the previous government, and is currently subject to review.

the use of digital tools, technologies and new data initiatives. It contains 13 Australian Privacy Principles (APPs), which are technology neutral and applicable to changing and emerging technologies.

8. The OAIC shares the interest of the Commission in the potential benefits of digital technology and data to facilitate innovation, reduce costs, assist with the delivery of goods and services and improve government policy making. This submission outlines how good privacy practices are critical to the realisation of these benefits. The submission focuses on those matters considered in the Report that intersect with privacy issues including the ethical use of technology and data, new data sharing and integration opportunities and cyber security and growth. It sets out how privacy provides the foundation for business and government to harness emerging digital technologies, which supports the Commission's core objectives of enabling productivity growth by fostering confidence and digital participation by the Australian community. It also sets out our views on measures that can further support the Commission's objectives through the ongoing Privacy Act Review.[3]

Supporting ethical use of technology and data

9. The continued development and use of emerging technologies such as artificial intelligence (AI) has the potential to create significant productivity enhancements as well as other benefits and opportunities for Australian society. However, the use of these technologies can also amplify privacy impacts, particularly where there is a lack of accountability, transparency and human oversight in how AI uses personal information to make decisions.

10. The Report acknowledges that community trust in new applications of technology is critical and the central driver for future uptake. As the Report states, businesses are still developing their AI ethics maturity and governments need to maintain their social licence to deliver digital and data-enabled services.

11. The Report recognises that ethical issues arising from the use of emerging technologies can reduce trust in the use of technology and data, and that a proactive approach is required to maintain trust without hampering technological progress and innovation. We would also note that privacy issues that are not properly addressed can impact the community's trust and undermine the success of new technological and data initiatives by business and government.

12. The OAIC's Australian Community Attitudes to Privacy Survey 2020 (ACAPS) Report demonstrates that privacy is fundamental to building and maintaining public trust. The report shows that privacy is a major concern for most Australians (around 70%), particularly as the digital environment and data practices evolve rapidly.[4] The ACAPS Report also shows that 84% of Australians consider privacy extremely or very important when choosing a digital service – ahead of reliability, convenience and price.

[3] Attorney-General's Department (AGD), Review of the Privacy Act 1988, AGD website, accessed 17 October 2022.

[4] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, OAIC, 2020, accessed 26 September 2022.

13. The survey results indicate a general downward trend in trust since 2007. Trust in businesses in general is down by 13%, and there has been a 14% decline in trust in how the Australian Government handles personal information.

14. The survey demonstrates that awareness of privacy has increased in recent years in the community and signals the need to increase trust and confidence in privacy and data handling practices across the economy. Good privacy practices that meet community expectations through compliance with the Privacy Act and APPs will create the trust and confidence that is needed for the public to support new uses of technology and data by governments and businesses. Privacy and data protection must be central to considerations about the ethical design, development, and use of emerging technologies.

15. The Report identifies numerous frameworks and principles in Australia and internationally which promote the ethical use of technology and data and suggests that a risk-based approach is appropriate to guide governments and provide clarity to businesses in relation to emerging technology and data use.

16. This aligns with the principles-based Privacy Act and APPs, which are structured to reflect privacy obligations across the information lifecycle, as entities collect, hold, use, disclose, and destroy or de-identify personal information. These are legally binding principles, which provide entities with the flexibility to take a proportionate risk-based approach to compliance, based on their particular circumstances, including size, resources and business model, while ensuring the protection of individuals' privacy.

17. For example, under APP 3, an APP entity must only collect personal information that is reasonably necessary for, or, for agencies, directly related to, one or more of its functions or activities. In evaluating whether a collection of personal information is reasonably necessary for a particular function or activity, consideration should be given to whether any interference with privacy is proportionate to a legitimate aim sought. Several other APPs require an APP entity to take 'reasonable steps', which also requires an evaluation of the facts and circumstances to determine what steps would be required to achieve compliance.

18. Importantly, the APPs also promote accountability by requiring entities to manage personal information in an open and transparent way. Accountability can be described broadly as the different actions and controls that an entity must implement to comply, and demonstrate compliance, with the privacy regulatory framework. In a practical sense, this requires entities to implement internal privacy management processes that are commensurate with, and scalable to, the risks and threats associated with their personal information handling activities.

19. By embedding strong accountability measures, entities can build a reputation for strong and effective privacy management, which is essential to realising the benefits of the personal information they hold and meeting their corporate social responsibilities. Accountability enables entities to not only meet the expectations of regulators, but to build consumer trust and confidence in their personal information handling practices.

20. A risk-based approach which effectively identifies and appropriately manages high privacy-risk technologies combined with strong accountability measures can be an enabler of, rather than a barrier to, innovation.

Creating new data sharing and integration opportunities

21. Section 3.2 of the Report considers the need to improve public sector data sharing and integration to generate greater value and productivity growth from the use of data by building upon existing government initiatives. The Report highlights that more access to and better use of data enables productivity growth by increasing competition, innovation and allocative efficiency.

22. The Report points to the potential for data held by government agencies through current initiatives such as the CDR and My Health Record, to be used to provide a range of benefits, and suggests that collaboration between government and the private sector can lead to new opportunities for data sharing. As the Report acknowledges, the benefits of data sharing must be balanced against safety and privacy concerns.[5]

23. The OAIC acknowledges that data sharing can lead to an increase in productivity growth, however, measures to increase data sharing of, and access to, personal information necessarily have privacy impacts. The Privacy Act recognises that the right to privacy is not absolute, and privacy rights may give way where there is a compelling public interest reason to do so. Whether it is appropriate will depend on whether any privacy impacts are reasonable, necessary and proportionate to achieving a legitimate objective.

24. In striking the right balance, it is important to consider the privacy risks attaching to the particular types of data involved in any data sharing or integration activity. In addition, consideration of what safeguards can be put in place to mitigate privacy risks is necessary. For example, health information is considered by the community to be highly sensitive, with the potential to give rise to discrimination against individuals.[6] In recognition of this sensitivity, the Privacy Act treats health information as 'sensitive information' and provides extra protections around its handling, such as generally requiring consent before an individual's health information is collected.[7]

25. Proposals to require healthcare providers to provide health information as a condition to receiving government funding, or to expand access to health datasets, should be approached cautiously to ensure that privacy impacts are properly considered.

26. Consideration should be given to the types of data being requested or shared and whether there are less privacy-intrusive options to achieve the same purpose. It should be noted that even in the case of anonymised or de-identified data, appropriate de-identification may be complex, especially in relation to detailed datasets that may be disclosed widely and combined with other datasets. In this context, de-identification will generally require more than removing personal identifiers such as names and addresses. Additional techniques and controls are likely to be required to remove, obscure, aggregate, alter and/or protect data in some way so that it is no longer about an identifiable (or reasonably identifiable) individual. The OAIC together with the

[5] Productivity Commission, *5 Year Productivity Inquiry: Australia's data and digital dividend – Interim Report 2*, 23 August 2022, p. 52.

[6] See Australian Law Reform Commission(ALRC) (2008), For Your Information: Australian Privacy Law and Practice (ALRC Report 108), p. 319.

[7] *Privacy Act 1988* (Cth), section 6 (definition of 'sensitive information').

CSIRO's Data61 has produced guidance on de-identification to assist entities to de-identify their data effectively.[8]

27. Careful consideration is required as to whether controls and safeguards can appropriately limit the associated privacy risks. Examples of additional protections include limits on what types of personal information the recipient of the data is permitted to combine with the data provided and purpose limitations or prohibitions to ensure that the data is being used in a fair and reasonable way.

28. A 'privacy by design' approach, by which privacy compliance is designed into data sharing initiatives from the start, and then throughout the information lifecycle, rather than being bolted on afterwards, will encourage government agencies and businesses to consider ways to achieve their objectives that are less privacy intrusive. Shifting the focus of an organisation to fostering a strong privacy culture which values the personal information of its customers, rather than simply achieving minimum compliance with privacy laws, provides a more effective and efficient way of managing privacy risks, as well as building public trust, confidence and loyalty.

29. We note that as part of its Digital Platform Services Inquiry, the ACCC is also considering whether measures aimed at increasing data access, such as promoting data portability and interoperability, may be effective in addressing competition concerns in the supply of digital platform services.[9] In our submission to the ACCC's February 2022 Discussion Paper for Interim Report No. 5, the OAIC has made recommendations to address the potential privacy risks associated with such measures.[10]

30. The Productivity Commission's Report notes the rapidly increasing amount of data that is produced and analysed by the private sector and identifies the CDR scheme as an important example of enabling data portability for consumer benefit. The Report suggests that the value that could be created from CDR data portability is yet to be realised, and that expanding the scheme's sectoral coverage and incorporating additional functionality may increase uptake and create new uses of, and value from, CDR data.[11]

31. The OAIC co-regulates the CDR scheme together with the ACCC. The OAIC enforces the privacy safeguards (and related Rules) and advises Treasury, the ACCC and Data Standards Body on the privacy implications of the CDR legislation, rules and data standards. The OAIC is also responsible for undertaking strategic enforcement in relation to the protection of privacy and confidentiality, as well as investigating individual and small business consumer complaints regarding the handling of their CDR data.

32. The OAIC recognises the CDR is an example of a data portability scheme with robust privacy controls and safeguards. The CDR scheme seeks to address privacy risks through obligations around consent, transparency, accreditation and data minimisation.

---

[8] OAIC, *De-identification and the Privacy Act*, OAIC, 21 March 2018, accessed October 2022.

[9] DPSI September 2022 Report - Discussion Paper (accc.gov.au) pp. 88 to 94.

[10] DBP - DPSI - September 2022 report - Submission - Office of the Australian Information Commission - Public (1).pdf (accc.gov.au)

[11] Productivity Commission, *5 Year Productivity Inquiry: Australia's data and digital dividend – Interim Report 2*, 23 August 2022, pp. 46 to 47.

33. At the same time, as we noted in our submission to Treasury's CDR Strategic Assessment Consultation in September 2021, the expansion of the CDR into new sectors will have significant implications for the handling of consumers' personal information.[12] Increased data flows across and within these sectors, and the potential for inherently sensitive datasets to be combined and provide richer insights about individuals, may create opportunities for innovation and consumer benefit, but will also give rise to increased privacy risk.

34. We have recommended that Treasury take a cautious approach to designating datasets with significant data sensitivities that may pose privacy risks for consumers, particularly vulnerable consumers. Further, we have advised against designating sectors and datasets with inherent sensitivities (such as the health insurance sector, digital platform data or location data) unless the privacy impacts are reasonable, necessary and proportionate to achieving the policy objectives of the CDR, and appropriate safeguards are put in place to ensure privacy risks are mitigated.

35. More generally, we consider that any data portability scheme should be fully informed, voluntary, initiated and controlled by the consumer (including the ability for the consumer to revoke sharing), include appropriate privacy safeguards and be consistent with the Privacy Act and other data portability frameworks, such as the CDR.

36. Ensuring that data sharing and data portability initiatives are designed and implemented with privacy as a central consideration will help to engender public trust and build a social licence for organisations to engage in these initiatives.

Balancing cyber security and growth

37. Cyber security is an important pre-condition for the effective use of digital technology and data. Poor security practices can limit productivity and economic gains in various ways. The OAIC, as the federal privacy regulator, has a unique role in bridging the shared responsibility of government, business and the community in addressing cyber security risks. The OAIC supports 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.[13] Furthermore, the OAIC has identified the security of personal information as a central regulatory focus.[14]

38. 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.[15] 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

[12] OAIC Submission to Treasury's CDR Strategic Assessment Consultation - Home

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

[14] Office of the Australian Information Commissioner, Privacy Regulatory Priorities 2020-2021.

[15] 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.

mechanisms to counter the often-linked cyber security and privacy threats and support coordinated government response and prevention.

39. The protection of information, including personal information, is a core aspect of cyber security resilience. 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.

40. The relationship between information security (including cyber security) and privacy is codified in the Privacy Act under 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 APP 11.

41. 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 outcomes focused approach also assists entities to detect privacy breaches promptly and ensure they are ready to respond to potential privacy breaches (including cyber incidents) in a timely and appropriate manner.

42. 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.

43. The OAIC administers the NDB scheme and is responsible for receiving notifications of eligible data breaches, handling complaints and conducting investigations and providing guidance and information to regulated organisations and the community. 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 protective action and mitigate the harm from the breach.

44. Malicious or criminal attacks remain the leading source of data breaches (55%) notified to the OAIC, with 68% of these involving a cyber incident.[16] The NDB scheme incentivises entities to improve security standards in relation to the protection of personal information, including cyber resilience.

[16] Office of the Australian Information Commissioner (February 2022), Notifiable Data Breaches Report July to December 2021, accessed October 2022.

45. As the Report acknowledges, government has a necessary role to play in mitigating and managing cyber risk, though cyber security regulation should minimise unnecessary burden and establish clear expectations on regulated entities. 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. Government action in relation to cyber security must reflect the evolving nature of cyber security risks which are shaped by emerging technologies and increasingly sophisticated tactics of malicious actors.

46. The OAIC is actively engaged with the Australian Government and many different stakeholders regarding new and emerging cyber security initiatives. We engage regularly with other regulators with cyber security responsibilities such as the Australian Securities and Investments Commission and the Australian Prudential Regulation Authority (APRA), with the aim of reducing duplication or gaps in cyber security regulatory responses. The OAIC considers that this coordination and collaboration among regulators, along with engagement with policymakers, experts, researchers, academics and advocacy organisations is essential for achieving an effective outcomes focused approach to cyber risks.

47. To support compliance and better practice the OAIC provides guidance on a range of issues relating to cyber security, including data breach preparation and response,[17] data breach action plans for health service providers,[18] and securing personal information.[19]

Streamlining regulation

48. As the Report recognises, 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 APRA's 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,[20] such as the Attorney-General's Department's 'Protective Security Policy Framework'[21] and the Australian Signals Directorate's 'Australian Government Information Security Manual'.[22]

49. Mapping and clarity around these entities' actual and potential roles in combating cyber risks may identify enhanced opportunities to leverage existing powers and capabilities to build a comprehensive cyber security framework.

50. The OAIC supports measures to reduce duplication and harmonise existing cyber security-related laws and standards. While different entities and industries may require different approaches to

[17] Office of the Australian Information Commissioner (July 2019), Data breach preparation and response, accessed October 2022.

[18] Office of the Australian Information Commissioner (February 2020), Data breach action plan for health service providers, accessed October 2022.

[19] Office of the Australian Information Commissioner (June 2018), Guide to securing personal information, accessed October 2022.

[20] See the Public Governance, Performance and Accountability Act 2013 (Cth).

[21] Available at Protective Security Policy Framework.

[22] Available at Australian Government Information Security Manual.

cyber security, this must be balanced with the need to provide consistent, comprehensive and unfragmented regulatory frameworks which help businesses, governments and individuals to clearly understand their rights and obligations. In this regard, a baseline cyber security obligation is a mechanism that may provide certainty to regulated entities, as noted in the report.

51. In particular, as the Report identifies, business may face multiple reporting requirements for a single cyber security incident, depending on its operations and the nature of the breach. This can place unnecessary burdens on businesses that are focused on recovering from the cyber incident. More coordination between government agencies and streamlining of reporting requirements could assist in reducing reporting burdens on businesses.

52. A single online interface for reporting, as proposed by the Productivity Commission, may be beneficial in this respect if securely and effectively administered.

Coordinating the policy and regulatory environment

Improved coordination

53. The Report suggests that the Australian regulatory response to emerging digital and data uses and emerging technology requires greater coordination between different government agencies, including between domestic policymakers and regulators, as well as improved engagement with international counterparts and with industry. At the same time, the Report notes that the benefits of increased coordination and engagement need to be weighed against the costs.

54. The OAIC has observed growing intersections between domestic frameworks relating to data and digital technologies, including privacy, competition and consumer law, and online safety and online content regulation. While there are synergies between these frameworks, there are also variances given each regulatory framework is designed to address different economic and societal issues.

55. The OAIC supports efforts to strengthen coordination amongst agencies to ensure greater efficiency and reduce duplication or inconsistency in government approaches to emerging technologies and data uses.

56. A key focus for the OAIC is working with international and domestic regulators, government, entities, and civil society to help ensure that privacy policy and legislation are interoperable, address contemporary privacy and data protection risks to Australians, and support the Australian economy.

57. Where different regulators exercise different functions under various laws, we agree that it is important for regulators to work together to avoid any unnecessary or inadvertent overlap and uncertainty for consumers and industry. At the same time, we do not consider that regulatory overlap is necessarily a negative outcome, particularly where it is well managed. It is more problematic if regulatory gaps expose individuals to harm or lead to inconsistent and inefficient regulatory approaches.

58. An effective approach must address the importance of institutional coordination between different regulatory bodies in different areas, given the need for complementary expertise. Regulatory cooperation can involve informal actions, such as engaging with networks like the

ACCC's Scams Awareness Network, to more formal actions, such as collaboration on compliance activities. To this end, the OAIC has entered into MOUs with other regulators including the ACCC, Australian Communications and Media Authority (ACMA), Australian Digital Health Agency and the Inspector-General of Intelligence and Security.

59. As discussed in the Report, the OAIC is a member of the Digital Platform Regulators Forum (DP-REG), together with the ACCC, ACMA and Office of the eSafety Commissioner. DP-REG is an initiative of Australian independent regulators to share information about, and collaborate on, cross-cutting issues and activities on the regulation of digital platforms. This includes consideration of how competition, consumer protection, privacy, online safety and data issues intersect and provides members with an opportunity to promote proportionate, cohesive, well-designed and efficiently implemented digital platform regulation.

60. DP-REG assists the OAIC in the exercise of its own regulatory powers by bringing a great depth to its assessment of new and emerging areas of risk arising from Australians' increasing engagement with the digital economy. Working with co-regulators that have complementary, but different experience, skills and powers, ensures domestic regulators are able to address a broader scope of issues, and achieve holistic consumer protection outcomes.

Reforming Australia's Privacy Act

61. The Attorney-General's Department is currently reviewing Australia's Privacy Act to consider whether its scope and enforcement mechanisms are fit-for-purpose and to ensure that its privacy settings better empower consumers, protect their data and support the digital economy.

62. We consider that the Privacy Act Review presents an opportunity to ensure that the Privacy Act remains fit for purpose in an increasingly global, digital world. We take this opportunity to highlight some key recommendations of relevance to the scope of the Commission's inquiry.

Increased organisational accountability

63. As acknowledged in the Report, entities in the digital economy are collecting more information than ever before. Many are basing their business model around the collection, use and disclosure of personal information. Data handling is increasingly complex, making it difficult for individuals to understand and control the ways in which their personal information is being handled.

64. In an environment where there has been an exponential increase in the collection, use and disclosure of personal information as part of standard business models, and where consumer information about those practices is long, complex and difficult to navigate, it is inappropriate for businesses to rely on that asymmetry to place the full responsibility on individuals to protect themselves from harm.

65. In our submission to the Privacy Act Review, the OAIC submitted that the burden of understanding and consenting to complicated information handling practices should not fall on individuals. Instead, we consider that the general standard of personal information handling across the

economy needs to be raised – government and businesses should be expressly required to take proactive steps to ensure their practices are appropriate, fair and proportionate.[23]

66. The OAIC recommended establishing a positive duty on organisations to handle personal information fairly and reasonably and to require regulated entities to take a proactive approach to meeting their obligations as the parties best equipped to understand their complex information handling flows and practices.

67. The OAIC views this proposed reform as a new keystone for the Privacy Act. The introduction of a central obligation to collect, use and disclose personal information fairly and reasonably would provide a new baseline for privacy practice that meets community expectations, and helps to restore and build trust.

68. The OAIC also suggested changes to privacy self-management mechanisms like notice and consent. Raising the standard of data handling provides individuals with greater confidence that they will be treated fairly when they choose to engage with a service. This would prevent consent being used to legitimise handling of personal information in a manner that, objectively, is unfair or unreasonable.

69. In our view these proposed reforms, while placing some additional responsibilities on regulated entities, will ultimately support greater productivity growth. By removing the privacy burden from individuals, the changes will allow them to engage with products and services with confidence that—like a safety standard—privacy protection is a given. The proposed reforms also provide the flexibility needed by entities to use personal information to innovate and contribute to a thriving digital economy.

70. The risk-based governance approach discussed by the Productivity Commission also aligns with a recommendation made by the OAIC that entities regulated under the Privacy Act be required to implement a risk-based privacy management program, which ensures that entities have internal structures and systems in place to effectively address current and emerging privacy risks and harms.

71. While a privacy management program will help to facilitate compliance with privacy obligations, it can also improve business productivity and help to develop more efficient business processes, for example, by providing certainty and confidence for employees around the appropriate way to handle personal information, reducing the number and cost of data breaches, and improving overall operational efficiencies. Entities with established internal processes are also better able to anticipate, adapt and respond to changing business circumstances and regulatory challenges.

72. In designing and implementing a risk-based privacy management program, entities are required to consider the risks associated with their personal information handling activities and their compliance policies and processes holistically and proportionally, and this should result in a more coherent, comprehensive and systematic approach to accountability. In other words, entities have the flexibility to design and implement a privacy management program in a way that best suits their circumstances.

73. The OAIC also recommended the introduction of a restricted and prohibited practices regime within the Privacy Act to enable a more proactive, outcome focused regulatory approach for

[23] Privacy Act Review – Discussion Paper (oaic.gov.au), pp. 79 to 87.

certain higher risk activities.[24] This regime would include developing a set of restricted practices for which entities must take reasonable steps to identify privacy risks and implement measures to mitigate those risks. Examples of proposed restricted practices include direct marketing, the large-scale collection, use or disclosure of sensitive information, location data or children's personal information, and the collection, use or disclosure of biometric or genetic data, including the use of facial recognition software.

74. Our submission also recommended the introduction of clear prohibitions on certain practices, subject to limited and tailored exceptions in the public interest. This recommendation reflects our regulatory experience that there will be some activities for which the privacy risks cannot be appropriately mitigated. Examples include profiling, online personalisation and behavioural advertising using children's personal information, and the surveillance or monitoring of an individual through their own mobile phone or other personal device.

Interoperable frameworks

75. As the digital economy develops and data increasingly flows across borders, it is important to create appropriate and interoperable frameworks that enable the efficient movement of data across borders while providing strong protections for individual's personal information. Getting these settings right is essential to creating trusted overseas data flows, which in turn supports Australian engagement in the global economy. The importance of trust in this context is highlighted by the OAIC's ACAP Survey, which shows that 92% of Australians are concerned about their data being sent overseas.[25]

76. In our submission to the Privacy Act Review, the OAIC has encouraged consideration of international privacy frameworks to ensure that Australia's framework is comparable, whilst also ensuring it reflects the unique circumstances and expectations of Australians.[26] Incorporating elements of other legal frameworks into Australian domestic law, where appropriate, will facilitate global consistency, ensure high privacy standards and that the protections afforded in Australia follow our personal information wherever it flows. This will also facilitate safe and efficient disclosure of personal information from overseas entities to entities based in Australia. Interoperability does not necessarily mean adopting other laws but instead considering how to create consistently high privacy standards globally.

77. Achieving improved interoperability can be greatly assisted by engagement with international counterparts and in global and regional forums. For example, the OAIC's active involvement in international forums such as the Global Privacy Assembly and Asia Pacific Privacy Authorities helps us to work towards the interoperability of Australia's privacy framework with other data protection frameworks around the world, influence the global debate on privacy issues, and exchange information to make the best use of our resources whilst ensuring consistency in the system of regulatory oversight. We have also entered into MOUs with international counterparts, including

[24] Privacy Act Review – Discussion Paper (oaic.gov.au), pp. 96-114.

[25] Lonergan Research, Australian Community Attitudes to Privacy Survey 2020, report to OAIC, September 2020, accessed October 2022, p 67

[26] Privacy Act Review – Discussion Paper (oaic.gov.au), pp 179-180, December 2021

the UK Information Commissioner's Office, the Data Protection Commissioner of Ireland and the Personal Data Protection Commission of Singapore.

78. Consideration should also be given to the consistency and interoperability of federal, state and territory laws. For example, Commonwealth, state and territory governments are increasingly working together on national initiatives that involve sharing data and personal information across jurisdictions. In many instances, these initiatives rely on jurisdictions across Australia having privacy frameworks that are equivalent to the protections afforded by the Commonwealth Privacy Act. Ensuring that state and territory privacy laws align with rights and obligations under the Privacy Act would ensure that Australians' personal information is subject to similar requirements whether that personal information is handled by an Australian Government agency, a state or territory government agency, or private sector organisations.

79. Consistency in regulation across domestic jurisdictions will reduce compliance burdens and cost and provide clarity and simplicity for regulated entities and the community.

Removal of small business exemption

80. Our submission to the Privacy Act Review also recommends the removal of the small business exemption, subject to an appropriate transition period to aid with awareness of, and preparation for compliance with, the Privacy Act.[27]

81. The small business exemption was originally introduced in recognition of the potentially unreasonable compliance costs for small businesses that may pose little or no risk to the privacy of individuals. The OAIC is of the view that the exemption is no longer appropriate given the increased privacy risks posed by small businesses in the online environment and the regulatory uncertainty created by the application of the exemption.

82. In recommending the removal of the exemption, we acknowledge the concerns of small business representatives about increased compliance costs, and the imposition of an unjustified regulatory burden on small businesses that do not pose a privacy risk.

83. However, although extending the Privacy Act to small businesses will create additional obligations and some compliance costs, the principles-based nature of the APPs enables businesses to take a risk-based approach to compliance. This will ensure that the compliance burden is proportionate to the risk posed by the particular personal information handling practices of the business. Small businesses will be able to take account of the safeguards placed on personal information by their service providers when considering the reasonable steps required to comply with relevant APPs.

84. Additionally, compliance with the Privacy Act can increase the competitiveness of small businesses seeking to engage with larger organisations. Compliance with the APPs may remove the need for larger organisations to impose additional contractual controls and audit requirements, thereby removing complexity and improving the position of small businesses in the marketplace.

85. Removing the small business exemption would also bring Australia in line with comparable international privacy regimes. The small business exemption has proved to be one of the major

[27] Privacy Act Review – Discussion Paper (oaic.gov.au), pp. 48-53, December 2021

issues for Australia in seeking adequacy under the European Union's General Data Protection Regulation (GDPR). Adequacy would allow entities subject to the GDPR to transfer personal data to entities in Australia without any specific authorisation or further steps. Streamlined data sharing processes are likely to support more efficient and consistent business practices and promote greater productivity for Australian businesses.

Conclusion

86. As increasing digitisation leads to an exponential growth in the production and transmission of data, there is a corresponding increase in community expectations that their personal information will be collected, used appropriately and protected. Privacy is integral to ensuring the Australian public has confidence in the way that businesses and governments are handling their personal information.

87. Community trust in the collection, handling and storage of data, including personal information, will assist the widespread adoption of digital and data applications which have the potential to enhance productivity and create significant opportunities and efficiencies for society. In this way, privacy supports innovation by enabling Australia to realise the productivity benefits of emerging technologies and new data uses.