Australian Government

Office of the Australian Information Commissioner

Digital Platform Services Inquiry – March 2024 report on data brokers – Issues Paper

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

11 September 2023

OAIC

Contents

Introduction 2

Privacy risks and harms 3

Application of the Privacy Act 5

- The definition of personal information 5
- De-identification 6
- Collection, use and disclosure of personal information 7
- Privacy policies and collection notices 10
- Security and quality of personal information 11

Reform of the Privacy Act 13

- Definition of personal information 13
- Fair and reasonable personal information handling 13
- Individual rights 14

Regulatory co-operation 15

Conclusion 16

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to submit to the Australian Competition and Consumer Commission's (ACCC) *Digital Platform Services Inquiry – March 2024 report on data brokers – Issues Paper* (the Issues Paper).

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 *Australian Information Commissioner Act 2010* (Cth)).

3. The Issues Paper considers competition and consumer issues in relation to the data collection, storage, supply, processing, and analysis services supplied by third-party data brokers in Australia. Third-party data brokers are defined in the Issues Paper as businesses that collect data about consumers from a range of third-party sources and sell or share that data with others.[1] Unlike first party data brokers,[2] third-party data brokers do not have a direct relationship with the consumers from whom they collect, process and analyse information.

4. Data brokers are a key part of the data supply chain that fuels a range of online and offline products and services. By combining information acquired from a range of sources, data brokers provide products and services including tools and reports prepared for a variety of purposes such as customer profiling, marketing, risk management, consumer credit reports or scores,[3] and fraud or crime prevention. The Issues Paper observes that despite the central role that data brokers play in providing data products and services to a range of businesses, as well as the wide variety and volume of information that they collect, analyse and process, there is currently little transparency, awareness and understanding of how data brokers operate in Australia.[4]

5. While the operation of Australian privacy law is outside the scope of the Digital Platform Services Inquiry, the topics considered by the Issues Paper intersect with the OAIC's existing regulatory role and responsibilities under the Privacy Act. The Privacy Act places important guardrails around the handling of personal information to minimise privacy risks and enhance consumer welfare. For this reason, the privacy framework is a relevant consideration in considering whether regulatory reform is required to address consumer protection issues in the data brokerage sector. An integrated approach to policy development is necessary to ensure

[1] ACCC, *Digital Platform Services Inquiry – March 2024 report on data brokers – Issues Paper*, 10 July 2023, accessed 27 July 2023, p 4.

[2] The Issues Paper defines first-party data brokers as businesses that collect data on their own consumers and sell or share that data with others. See, ACCC, *Digital Platform Services Inquiry – March 2024 report on data brokers – Issues Paper*, 10 July 2023, accessed 27 July 2023, p 4.

[3] The Issues Paper does not focus on consumer and commercial credit reporting products and services, including the supply of credit reports and scores, as they are regulated separately under the Privacy Act. The Issues Paper notes that consumer and commercial credit reporting products and services are a key category of data products and services supplied by third-party data brokers. See, ACCC, *Digital Platform Services Inquiry – March 2024 report on data brokers – Issues Paper*, 10 July 2023, accessed 27 July 2023, p 5.

[4] ACCC, *Digital Platform Services Inquiry – March 2024 report on data brokers – Issues Paper*, 10 July 2023, accessed 27 July 2023, p 2-3.

that the distinct but complementary roles of privacy, competition and consumer laws work cohesively to address risks and harms in the data brokerage sector.

6. To assist the ACCC with its consideration of these issues, this submission highlights some of the privacy risks and harms that may arise in relation to the data-handling practices of third-party data brokers, our views on how the Privacy Act may apply to these activities, as well as measures that can strengthen the existing privacy framework through the ongoing Privacy Act Review.[5]

7. The OAIC has an effective, collaborative and longstanding working relationship with the ACCC, including through a memorandum of understanding on exchanges of information[6], as co-regulators of the Consumer Data Right and through our participation in the Digital Platform Regulators Forum (DP-REG).[7] The OAIC looks forward to continuing to work with the ACCC and portfolio agencies on these issues.

Privacy risks and harms

8. The Issues Paper seeks views on potential consumer and small business harms and benefits associated with the collection, processing and analysis of information by data brokers.[8] It lists a range of potential harms that could be relevant to the collection and use of personal information or data and notes that the ACCC is concerned that consumers are generally unaware of the practices of data brokers and of associated harms.[9]

9. The OAIC's Australian Community Attitudes to Privacy Survey 2023 demonstrated a significant level of discomfort in the community about the sale and sharing of personal information. The survey found that 78% of parents were uncomfortable with a business selling personal information about a child to third parties and that 90% of individuals believed that they should have a right to object to certain data practices, including the selling of their personal information, while still being able to access and use the service.[10] Furthermore, 83% of respondents considered that their personal information should not be shared without their consent.[11]

10. The sharing and sale of personal information presents a range of potential privacy impacts. As noted in the Issues Paper, data brokers collect information about individual consumers from a wide range of offline and online sources and combine it for the purpose of customer profiling,

---

[5] Attorney-General's Department, *Privacy Act Review Report*, February 2022, accessed 4 August 2023.

[6] OAIC, *MOU with the ACCC: exchange of information*, 11 August 2020, accessed 18 March 2021.

[7] DP-REG is an initiative between the OAIC, ACCC, Australian Communications and Media Authority (ACMA) and the eSafety Commissioner (eSafety) 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 in order to proportionate, cohesive, well-designed and efficiently implemented digital platform regulation.

[8] ACCC, *Digital Platform Services Inquiry – March 2024 report on data brokers – Issues Paper*, 10 July 2023, accessed 27 July 2023, p 11.

[9] ACCC, *Digital Platform Services Inquiry – March 2024 report on data brokers – Issues Paper*, 10 July 2023, accessed 27 July 2023, p 10.

[10] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2023*, 8 August 2023, accessed 8 August 2023, p 37 and 92.

[11] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2023*, 8 August 2023, accessed 8 August 2023, p 14.

marketing, risk management, credit reporting or fraud or crime prevention services.[12] The combination of this information allows for the creation of highly detailed profiles of consumers or the creation of consumer segments or 'audiences' based on attributes, interests and purchasing intentions.[13] The combination of datasets across contexts can increase the granularity, detail and sensitivity of consumer profiles, which presents privacy risks.

11. As observed in the Issues Paper, this may be particularly problematic where incomplete or inaccurate information is used in the creation of a consumer profile or where this information is used to discriminate against a consumer.[14]

12. Personal information may also be collected and used in ways that the individual does not reasonably expect, such the use of data analytics to generate unexpected inferences or outcomes or the use of personal information in an unrelated context to the setting in which it was provided.[15] In this regard, individuals may lose control of their personal information as it is distributed across the data supply chain.

13. An individual's risk of having their information compromised in a data breach can also increase as their personal information or de-identified data is disseminated and stored by a larger number of entities. The distribution of data to many parties increases the potential number of targets for malicious actors who may cause a data breach. Furthermore, information that is de-identified in the hands of one party may be re-identified when made publicly available,[16] such as through a data breach. When cyber security settings fail, the risk of harm to individuals whose information is compromised can be devastating. These potential harms that may follow a data breach include identity theft, financial loss, increased likelihood of being targeted by scams, threats to physical safety, humiliation and damage to reputation or relationships.[17]

14. The use of privacy enhancing technologies may mitigate the privacy impacts of data sharing in the data brokerage context. In particular, the de-identification of personal information can be an important privacy protective measure to assist in managing risk in certain circumstances. However, this must be balanced against the risks of re-identification and the difficulties in robustly de-identifying personal information in some circumstances. This is discussed in further detail, below.

---

[12] ACCC, *Digital Platform Services Inquiry – March 2024 report on data brokers – Issues Paper*, 10 July 2023, accessed 27 July 2023, p 3. See also, Attorney-General's Department, *Privacy Act Review Report*, February 2022, accessed 4 August 2023, 204-205.

[13] Kayleen Manwaring, Katharine Kemp and Rob Nicholls, (Mis)informed Consent in Australia, 31 March 2021, accessed 7 August 2023, p 97-98.

[14] ACCC, *Digital Platform Services Inquiry – March 2024 report on data brokers – Issues Paper*, 10 July 2023, accessed 27 July 2023, p 10. Note that the Privacy Act contains requirements in relation to quality of personal information. Under APP 10, APP entities must take such steps as a reasonable in the circumstances to ensure that the personal information they collect, use or disclose are accurate, up-to-date and complete.

[15] See, OAIC, *Guide to data analytics and the Australian Privacy Principles*, 1.3: Benefits and challenges of data analytics, 21 March 2019, accessed 1 August 2023.

[16] See, OAIC, De-identification and the Privacy Act, 21 March 2018, accessed 4 August 2023.

[17] OAIC, Part 4: Notifiable Data Breach (NDB) Scheme, Data breach preparation and response, July 2019, accessed 28 August 2023.

Application of the Privacy Act

15. Entities that have an annual turnover of $3 million or more are regulated by the Privacy Act and are required to manage personal information in accordance with the APPs. Entities that collect or disclose personal information from, or to, anyone else for 'benefit, service or advantage' are required to comply with the Privacy Act regardless of their annual turnover, in recognition of the heightened privacy risks associated with trading in personal information.[18]

16. The APPs govern how entities are permitted to handle personal information and contain requirements that apply across the information lifecycle, including in relation to collection, use, disclosure, storage and destruction or de-identification of personal information.

17. The principles-based framing of the APPs enables entities to take a risk-based approach to compliance, based on their particular circumstances including size, resources and business model. It also enables the obligations in the APPs to scale proportionally to the volume and type of personal information that an entity holds. 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.

The definition of personal information

18. The definition of personal information is a key concept that delineates the scope of what is regulated and protected by the Privacy Act.

19. The Privacy Act defines personal information as information or an opinion about an identified individual, or an individual who is reasonably identifiable.[19] Information is 'about' an individual where there is a connection between the information and the individual. This is ultimately a question of fact and will depend on the context and circumstances of each particular case.[20]

20. In the general sense, an individual is 'identified' when, within a group of persons, they are distinguished from all other members of a group. In the context of the Privacy Act, an individual will be 'identified' or 'reasonably identifiable' where a link can be established between the information and a particular person. This may not necessarily involve identifying the individual by name. Even if a name is not present other information, such as a detailed description, may also identify an individual. The key factor to consider is whether the information can be linked back to the specific person that it relates to.[21] The definition of personal information is intended to apply to a broad range of information.

21. Importantly, whether information is personal information should be determined on a case-by-case basis, with reference to the specific circumstances and context of the situation. Some information may not be personal information when considered on its own. However, when

[18] *Privacy Act 1988* (Cth) s 6D(4)(c) and (d). See also, OAIC, Trading in personal information, accessed 28 August 2023. Note that per s 6D(7) and (8), an entity is not considered to be trading in personal information for the purposes of s 6D(4)(c) and (d) if the collection or disclosure is undertaken with the consent of all individuals concerned or is authorised or required by law.

[19] *Privacy Act 1988* (Cth) s 6.

[20] OAIC, What is personal information?, 5 May 2017, accessed 4 August 2023.

[21] OAIC, What is personal information?, 5 May 2017, accessed 4 August 2023.

combined with other information held by (or accessible to) an organisation, the individual may be reasonably identifiable, and it may become personal information. Information holdings can therefore be dynamic, and the character of information, including whether it is personal or de-identified information, can change over time or in the hands of different parties.

22. As noted in the Issues Paper, data brokers collect, use and disclose a broad range of data types from a wide range of sources in order to provide their products and services.[22] The complex data handling practices that take place in the data supply chain can make it difficult to draw a bright line between personal and de-identified information in all cases. Therefore, careful consideration must be given to whether information may constitute personal information in the particular context in which it is collected, used and disclosed. Where there is uncertainty, the OAIC considers that entities should err on the side of caution, by treating the information as personal information, and handle it in accordance with the APPs.[23]

23. In the context of a data supply chain, the character of data and whether it falls within the definition of personal information may therefore change as it is shared between third-party data brokers and the users of data products and services.[24]

De-identification

24. The de-identification of personal information can be an important privacy protective measure. When carried out appropriately, it can allow APP entities to harness the benefits of data in a privacy protective way, which helps to build community trust. However, APP entities must be cognisant of re-identification risks and the difficulties of robustly de-identifying personal information in some circumstances.

25. Information that has undergone an appropriate and robust de-identification process is not personal information and is not currently subject to the Privacy Act.[25] This requires there to be no reasonable likelihood of re-identification occurring in the context that the data will be made available.[26]

26. Appropriate de-identification may be complex, especially in relation to detailed datasets that may be disclosed widely or combined with other data sets. 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. Choosing appropriate de-identification techniques and controls may

[22] ACCC, *Digital Platform Services Inquiry – March 2024 report on data brokers – Issues Paper*, 10 July 2023, accessed 27 July 2023, p 3.

[23] OAIC, What is personal information?, 5 May 2017, accessed 4 August 2023.

[24] In referring to first-party data brokers, third-party data brokers and data product and service users, we are adopting the categorisation put forward in the Issues Paper. See ACCC, *Digital Platform Services Inquiry – March 2024 report on data brokers – Issues Paper*, 10 July 2023, accessed 27 July 2023, p 4, 9.

[25] *Privacy Act 1988* (Cth) s 6.

[26] OAIC, De-identification and the Privacy Act, 21 March 2018, accessed 4 August 2023.

require organisations to balance data utility and the level of data modification required to achieve de-identification.[27]

27. In addition to de-identification techniques, the OAIC notes that entities can consider the context or environment in which data is held and made available, under an approach known as 'functional de-identification'.[28] This approach has the objective of ensuring that de-identified data remains de-identified once it is shared or released within or into a new data environment, and takes into account other data that exists in the data environment, access controls, governance processes and infrastructure.[29]

28. De-identification is not a fixed or end state. De-identified data may become personal information as the context changes. Managing this risk requires regular re-assessment, particularly if an entity receives and assimilates additional data, or shares or releases data into a new context or environment.

29. Robust de-identification may therefore be particularly challenging for some parties in the data supply chain who may have a commercial incentive to build detailed consumer profiles, maximise their data holdings and increase the granularity of their data products and services. The risk that datasets can be re-identified increases as they are combined, released into a new data access environment, and as data analytics technologies become more advanced.[30]

30. The OAIC and CSIRO's Data 61 have released a De-Identification Decision-Making Framework[31] to assist organisations to de-identify their data effectively. The De-Identification Decision-Making Framework is a practical and accessible guide for Australian organisations that handle personal information and are considering sharing or releasing it to meet their ethical responsibilities and legal obligations, such as those under the Privacy Act.

31. As noted above, where there is uncertainty, the OAIC considers that entities should err on the side of caution, by treating the information as personal information, and handle it in accordance with the APPs.[32]

Collection, use and disclosure of personal information

32. APP 3 and APP 6 of the Privacy Act regulate the collection, use and disclosure of personal information by APP entities.

33. APP 3 governs when personal information, including sensitive information, may be collected by organisations. It places obligations on organisations to:

---

[27] OAIC, De-identification and the Privacy Act, 21 March 2018, accessed 4 August 2023. See also, OAIC and CSIRO Data61, The De-identification Decision-Making Framework, 18 September 2017, accessed 4 August 2023.

[28] OAIC and CSIRO Data61, The De-identification Decision-Making Framework, 18 September 2017, accessed 4 August 2023, p x and 18.

[29] For further details see OAIC and CSIRO Data61, The De-identification Decision-Making Framework, 18 September 2017, accessed 4 August 2023, p x and 18.

[30] ACCC, Customer loyalty schemes – final report, 3 December 2019, accessed 28 August 2023, p 78.

[31] OAIC and CSIRO Data61, The De-identification Decision-Making Framework, 18 September 2017, accessed 4 August 2023.

[32] OAIC, What is personal information?, 5 May 2017, accessed 4 August 2023.

- Collect personal information only where it is reasonably necessary for one or more of the organisation's functions or activities
- Collect sensitive information only with the individual's consent (unless an exception under APP 3.4 applies)
- Collect personal information only by lawful and fair means, and
- Collect personal information directly from the individual unless it is unreasonable or impractical to do so.[33]

34. APP 6 outlines when an entity may use or disclose personal information. It provides that personal information may only be used or disclosed for the purpose for which it was collected (known as the 'primary purpose'), and that personal information may only be used for another purpose (a 'secondary purpose') with the individual's consent or if an exception under APP 6.2 applies.

Third-party data brokers

35. As acknowledged in the Issues Paper, third-party data brokers may collect information about individuals from a wide range of offline and online sources, which could include an individual's name, home and work address, date of birth, marital or family status, education level, income, purchasing history, search and browsing habits, location data, and financial information.[34]

36. To the extent that third-party data brokers collect personal information, they must comply with the requirements of APP 3 in the Privacy Act, as set out above. It is important to note that APP 3 and other privacy obligations apply to the collection of personal information from publicly available sources,[35] such as web pages. It also includes the 'generation' or 'creation' of personal information, such as inferences in relation to an individual's characteristics, behaviours or preferences.[36] The concept of 'collection' applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means.[37]

37. Data brokers do not generally collect personal information directly from individuals.[38] As a result, the requirements of APP 3.5 and APP 3.6 must be given close consideration in this context.

38. APP 3.5 requires the collection of personal information to take place by lawful and fair means. A 'fair means' of collection will depend on the circumstances but is ordinarily one that does not

---

[33] *Privacy Act 1988* (Cth), APP 3.2-3.6.

[34] ACCC, *Digital Platform Services Inquiry – March 2024 report on data brokers – Issues Paper*, 10 July 2023, accessed 27 July 2023, p 3, 8. See also, Attorney-General's Department, *Privacy Act Review Report*, February 2022, accessed 4 August 2023, 204-205.

[35] OAIC, Chapter B: Key concepts, Australian Privacy Principles guidelines, 22 July 2019, accessed 28 August 2023, [B.30].

[36] OAIC, Guide to data analytics and the Australian Privacy Principles, 21 March 2018, accessed 7 August 2023.

[37] OAIC, Chapter 3: APP 3 Collection of solicited personal information, Australian Privacy Principles guidelines, 22 July 2019, accessed 28 August 2023, [3.5].

[38] Information Commissioner's Office (UK), Investigation into data protection compliance in the direct marketing data broker sector, October 2022, access 18 August 2023, 12

involve intimidation or deception, and is not unreasonably intrusive.[39] The Australian Privacy Principles Guidelines note that 'it would usually be unfair to collect personal information covertly without the knowledge of the individual.'[40]

39. APP 3.6 requires that organisations collect personal information directly from the individual unless it is unreasonable or impractical to do. Whether it is 'unreasonable or impracticable' to collect personal information only from the individual concerned will depend on the circumstances of the particular case, and it may be relevant to consider:

    - whether the individual would reasonably expect personal information about them to be collected directly from them or from another source
    - the sensitivity of the personal information being collected
    - whether direct collection would jeopardise the purpose of collection or the integrity of the personal information collected
    - any privacy risk if the information is collected from another source, and
    - the time and cost involved of collecting directly from the individual. However, an APP entity is not excused from collecting from the individual rather than another source by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable or impracticable will depend on whether the burden is excessive in all the circumstances.[41]

40. There is an underlying tension between the data minimisation requirements of APP 3 and the activities of data brokers, whose business model is reliant on maximising the amount of data that they collect in order to find correlations between disparate datasets.[42] The OAIC's guidance on data analytics observes that the collection of 'all data' that is available for 'unknown purposes' may expose entities to privacy compliance risks.[43]

41. To the extent that third-party data brokers use or disclose personal information, they are also required to comply with APP 6 and are prohibited from using or disclosing personal information for a secondary purpose without the individual's consent, or unless another exception in APP 6 applies. This principle may present a challenge in the context of data brokers, as the secondary use and disclosure of personal information may be common in order to conduct data analytics.[44] In practice, entities should determine whether their planned uses and disclosures of personal

[39] OAIC, Chapter 3: APP 3 Collection of solicited personal information, Australian Privacy Principles guidelines, 22 July 2019, accessed 28 August 2023, [3.62].

[40] OAIC, Chapter 3: APP 3 Collection of solicited personal information, Australian Privacy Principles guidelines, 22 July 2019, accessed 28 August 2023, [3.62].

[41] OAIC, Chapter 3: APP 3 Collection of solicited personal information, Australian Privacy Principles guidelines, 22 July 2019, accessed 28 August 2023, [3.65].

[42] See relatedly, OAIC, Guide to data analytics and the Australian Privacy Principles, 21 March 2018, accessed 7 August 2023.

[43] OAIC, Guide to data analytics and the Australian Privacy Principles, 21 March 2018, accessed 7 August 2023.

[44] OAIC, Guide to data analytics and the Australian Privacy Principles, 21 March 2018, accessed 7 August 2023.

information are compatible with the original purpose it was collected for, and the privacy policy and collection notice given to the individual.[45]

Data product and service users

42. The Issues Paper notes that data product and service users may engage with third-party data brokers for a range of purposes, including customer profiling, consumer credit scores, marketing, risk management and fraud or crime prevention.[46] These entities may collect, use and disclose personal information in the process of engaging with these data products and services, which enlivens their obligations under the Privacy Act.

43. For example, data product and service users may use third-party data brokers to 'enrich' or 'enhance' their existing customer databases or profiles with additional data or inferences.[47] In certain circumstances, the provision of a customer database by a data product and service user to a third-party data broker may constitute a disclosure of personal information for the purposes of APP 6. Once the customer dataset is returned to the data product and service user, any newly created inferences in relation to a particular individual's characteristics, behaviours or preferences or information that has been appended to a customer profile will likely constitute a new collection of personal information for the purposes of APP 3.

44. Data product and service users should therefore consider whether these data flows are compliant with the requirements of APP 3 and 6, including whether the collection of personal information was reasonably necessary for the organisation's functions and activities,[48] has taken place by lawful and fair means,[49] whether it was unreasonable or impractical to collect that personal information directly from the individual,[50] and whether any secondary uses or disclosures were lawful under APP 6.

45. Data product and service users should also consider whether they have taken appropriate transparency measures, discussed further below.

Privacy policies and collection notices

46. The Issues Paper asks how consumers are made aware that their data is being collected and used by data brokers. [51] To the extent that data brokers may handle personal information, they are required to maintain a privacy policy under APP 1 and provide a collection notice to individuals under APP 5.

---

[45] OAIC, Guide to data analytics and the Australian Privacy Principles, 21 March 2018, accessed 7 August 2023.

[46] ACCC, *Digital Platform Services Inquiry – March 2024 report on data brokers – Issues Paper*, 10 July 2023, accessed 27 July 2023, p 9.

[47] See relatedly, Katharine Kemp, Australia's forgotten privacy principle: Why common 'enrichment' of customer data for profiling and targeting is unlawful, 20 September 2022, accessed 30 August 2023.

[48] *Privacy Act 1988* (Cth) APP 3.2.

[49] *Privacy Act 1988* (Cth) APP 3.5.

[50] *Privacy Act 1988* (Cth) APP 3.6.

[51] ACCC, *Digital Platform Services Inquiry – March 2024 report on data brokers – Issues Paper*, 10 July 2023, accessed 27 July 2023, p 11.

47. The objective of APP 1 is to ensure organisations manage personal information in an open and transparent way. APP 1.3 requires APP entities to maintain a 'clearly expressed' and 'up to date' APP Privacy Policy that describes how it manages personal information. APP 1.4 contains a non-exhaustive list of information an APP entity must include in its APP Privacy Policy, including:

    - the kinds of personal information collected and held by the entity
    - how personal information is collected and held
    - the purposes for which personal information is collected, held, used and disclosed
    - how an individual may access their personal information and seek its correction
    - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled, and
    - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), and if so, the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

48. APP 5 requires entities to take such steps (if any) as are reasonable in the circumstances to notify individuals about the collection of their personal information. The collection notice must be provided at or before the time an APP entity collects personal information (or as soon as practicable afterwards) and must address the matters listed in APP 5.2.

49. The APP Guidelines provide examples of 'reasonable steps' that an APP entity could take to notify or ensure awareness of the APP 5 matters, including a prominent display of the matters in a sign-up form, providing a readily accessible link to an APP 5 notice or verbal communication of the matters over a telephone call. The APP Guidelines acknowledge that in certain circumstances, it may not be reasonable to provide notice to an individual.[52]

Security and quality of personal information

50. The Issues Paper seeks feedback on the processes and controls that data brokers have in place to protect consumers, including verification processes to ensure data is accurate and measures to protect stored data.[53] The OAIC notes that to the extent that data brokers handle personal information, they are subject to mandatory requirements under the Privacy Act in relation to the security and accuracy of personal information.

51. APP 11 requires APP entities 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.[54] Entities must also take reasonable steps to destroy or de-identify the personal

[52] OAIC, APP 5 Notification of the collection of personal information, Australian Privacy Principles guidelines, 22 July 2019, accessed 4 August 2023.

[53] ACCC, *Digital Platform Services Inquiry – March 2024 report on data brokers – Issues Paper*, 10 July 2023, accessed 27 July 2023, p 11.

[54] *Privacy Act 1988* (Cth) APP 11.1.

information they hold once it is no longer needed for any purpose for which it may be used or disclosed under the APPs.[55]

52. The steps that an APP entity should take to ensure the security of personal information will depend upon circumstances including the nature of the APP entity, the amount and sensitivity of the personal information held, possible adverse consequences for an individual in the case of a breach, among other factors.[56] As compliance with APP 11 is context dependent, the OAIC has published a 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.[57]

53. Data brokers that handle personal information are also subject to the Notifiable Data Breaches (NDB) scheme. The NDB scheme requires regulated entities to notify individuals and the OAIC about 'eligible data breaches'. A data breach is an eligible data breach if it is likely to result in serious harm to any of the individuals to whom the information relates.

54. The key objective of the NDB scheme is to enable individuals whose personal information has been compromised in a data breach to take remedial steps to lessen the adverse impact that might arise from the breach. By arming individuals with the necessary information, they will have the opportunity to take appropriate action, such as monitoring their accounts and credit reports or taking preventative measures such as changing passwords and cancelling credit cards.

55. Under APP 10, entities must take reasonable steps to ensure that the personal information they collect is accurate, up-to-date and complete.[58] APP entities must also take reasonable steps to ensure that the personal information it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.[59]

56. Ensuring accuracy and quality in data analytics is particularly important where personal information is used to create a consumer profile or to make automated or data-driven decisions about an individual. The use of inaccurate or poor-quality personal information can have significant privacy impacts for individuals or may subject them to erroneous or unjustified decisions. In these situations, it would be prudent for entities to take additional and more rigorous steps to ensure the quality of both personal information collected, as well as any additional personal information that is generated by analytics tools.[60]

---

[55] *Privacy Act 1988* (Cth) APP 11.2.

[56] OAIC, APP 11 Security of personal information, Australian Privacy Principles guidelines, 22 July 2019, accessed 4 August 2023.

[57] OAIC, Guide to Securing Personal Information, 5 June 2018, accessed 4 August 2023.

[58] *Privacy Act 1988* (Cth) APP 10.1.

[59] *Privacy Act 1988* (Cth) APP 10.2.

[60] OAIC, Guide to data analytics and the Australian Privacy Principles, 21 March 2018, accessed 7 August 2023.

Reform of the Privacy Act

57. The Attorney-General's Department has undertaken a review of the *Privacy Act 1988* (Cth) (Privacy Act Review) to consider whether its scope, protections and enforcement mechanisms are fit-for-purpose.

58. We take this opportunity to highlight some of the proposals of the final Privacy Act Review Report[61] that would operate to improve privacy protections and individuals' control in relation to the handling of personal information across the economy.

Definition of personal information

59. The Privacy Act Review Report puts forward a number of proposals with the objective of clarifying that the definition of personal information is an expansive concept which may include technical and inferred information.

60. The Privacy Act Review Report has proposed to replace the word 'about' in the definition of personal information with the words 'relates to'.[62] The proposed change is intended to address uncertainty that followed the decision in *Privacy Commissioner v Telstra Corporation Ltd*[63] as to the circumstances in which technical data will fall within the definition of personal information. It would also align the definition of personal information in the Privacy Act with comparable international data protection laws such as Europe's General Data Protection Regulation (GDPR),[64] as well as with domestic privacy safeguards such as the Consumer Data Right.[65]

61. Additionally, the Privacy Act Review Report proposes to amend the Privacy Act's definition of 'collect' to expressly cover information obtained from any source and by any means, including inferred or generated information.[66] This proposed amendment would codify existing OAIC guidance on the interpretation of the term 'collect'[67] and seeks to clarify that the creation of an inference or prediction about an individual in the data analytics context is a collection that enlivens the requirements of the APPs.[68]

Fair and reasonable personal information handling

62. Notice and choice are foundational principles in privacy law across the world, including in the Privacy Act. However, our 2023 Australian Community Attitudes to Privacy Survey found that

---

[61] Attorney-General's Department, *Privacy Act Review Report*, February 2022, accessed 4 August 2023.

[62] Attorney-General's Department, *Privacy Act Review Report*, February 2022, accessed 4 August 2023, p 27.

[63] *Privacy Commissioner v Telstra Corporation Ltd* (2017) 249 FCR 24.

[64] GDPR Article 4(1). See also *California Consumer Privacy Act 2018* (California), § 1798.140(1)(o).

[65] Competition and Consumer Act 2010 (Cth) s 56AI(3).

[66] Attorney-General's Department, *Privacy Act Review Report*, February 2022, accessed 4 August 2023, p 30.

[67] OAIC, Chapter 3: APP 3 Collection of solicited personal information, Australian Privacy Principles guidelines, 22 July 2019, accessed 28 August 2023, [3.5].

[68] Attorney-General's Department, *Privacy Act Review Report*, February 2022, accessed 4 August 2023, p 30.

while the majority (96%) of Australians believe that their privacy is important when choosing a product or service,[69] only 21% of individuals always or often read privacy policies. [70]

63. Even where individuals do read privacy policies and collection notices, they may feel resigned to consent to the use of their information to access online services as they do not feel there is any alternative. As digital products and services become more entrenched in individuals' lives and in the way in which they work, study and socialise, it is increasingly difficult to avoid personal information handling practices that do not align with their preferences. In these circumstances, it is inappropriate for entities to place the full responsibility on individuals to protect themselves from harm.

64. In recognition of these challenges, the Privacy Act Review Report has proposed to establish a positive obligation that would require entities to handle personal information in a manner that is 'fair and reasonable in the circumstances.'[71]

65. The proposal would require entities to proactively consider legislative factors, including whether their personal information handling activities are proportionate, the reasonable expectations of individuals and possible risks of unjustified adverse impact or harm, among other matters.

66. The fair and reasonable test will provide a baseline level of privacy protection and will allow individuals to engage with products and services with confidence that—like a safety standard—privacy protection is a given. It would also prevent consent from being used to legitimise handling of personal information in a manner that is, objectively, unfair or unreasonable. For example, the trading in information that relates to individuals' moods or emotional states[72] may be particularly intrusive and may present a risk of harm and impact to privacy that is not proportionate, and is not considered fair and reasonable in the circumstances.

67. The OAIC views this proposed reform as a new keystone for the Privacy Act. The fair and reasonable test would provide individuals with greater confidence that they will be treated fairly when they choose to engage with digital services and would help to build trust in the digital economy.

Individual rights

68. The Issues Paper seeks feedback on how consumers are made aware that their data is being collected and used by data brokers, as well as the steps that consumers can take to inspect or remove data that is held about them by data brokers. [73]

---

[69] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2023*, 8 August 2023, accessed 8 August 2023, p 25.

[70] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2023*, 8 August 2023, accessed 8 August 2023, p 21.

[71] Attorney-General's Department, *Privacy Act Review Report*, February 2022, accessed 4 August 2023, p 110-121.

[72] For a brief summary of emotion recognition technology, see, Information Commissioner's Office (UK), 'Immature biometric technologies could be discriminating against people' says ICO in warning to organisations, 26 October 2022, accessed 30 August 2023.

[73] ACCC, *Digital Platform Services Inquiry – March 2024 report on data brokers – Issues Paper*, 10 July 2023, accessed 27 July 2023, p 11.

69. The Privacy Act Review Report includes proposals that are directed at improving the transparency of personal information handling practices and the level of control that individuals have over how their information is handled. It proposes a number of individual rights modelled on the European Union's *General Data Protection Regulation* (GDPR) including a right to erasure and an enhanced right of access.

70. A right to erasure would allow individuals to request that an entity erase their personal information. The introduction of the right would be an important step in bringing the Australian privacy framework in line with other international jurisdictions, including the United Kingdom, the European Union and parts of the United States. It would also enable individuals to meaningfully withdraw their consent. Currently, even in the limited circumstances where consent may be withdrawn (that is, in situations where consent has been required under the APPs), there is no right for individuals to request destruction of their personal information. Under the proposal, an entity who has collected the information from a third party or disclosed the information to a third party must also inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort.[74] This would be of particular importance in the data broker context, whereby the individual may have limited visibility of the parties to whom their data has been disclosed.

71. The enhanced right of access would build on the existing requirements of APP 12 by allowing individuals to request an 'explanation or summary' of what the APP entity has done with their personal information. Exceptions for these rights would apply for countervailing public interests, other legal interests and to recognise where it would be technically impossible or unreasonable to comply with an individual's request. [75]

72. The OAIC submits that the measures proposed as part of the Privacy Act Review Report will enhance the existing privacy framework and present an important opportunity to ensure that the Australia's Privacy Act remains fit for purpose, including in the context of data brokers.

Regulatory co-operation

73. The OAIC has observed growing intersections between domestic frameworks in the context of data issues, 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 that each regulatory framework is designed to address different economic and societal issues. Each regime is an essential and complementary component in the ring of defence that is being built to address the risks and harms faced by Australians in the digital environment.

74. Where different regulators exercise different functions under various laws 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

[74] Attorney-General's Department, *Privacy Act Review Report*, February 2022, accessed 4 August 2023, p 176.

[75] Attorney-General's Department, *Privacy Act Review Report*, February 2022, accessed 4 August 2023, Chapter 18.

regulatory gaps expose individuals to harm or lead to inconsistent and inefficient regulatory approaches.

75. An effective approach must address the importance of institutional coordination between different regulatory bodies in different areas, given the need for complementary expertise to address the different risks and harms that can arise in the data brokerage sector.

76. To this end, and as noted at the beginning of this submission, the OAIC is a member of the Digital Platform Regulators Forum (DP-REG), together with the ACCC, ACMA and 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.

77. The OAIC is also a member of the Cyber Security Regulators Network (CSRN), along with the Australian Securities and Investment Commission (ASIC), the Australian Prudential Regulation Authority (APRA), ACMA and the ACCC. The purpose of the CSRN is to enable Australian regulators to work together to understand, respond to and share information about cyber security risks and incidents.

Conclusion

78. The Privacy Act is a principles-based and technology-neutral framework through which Australians' privacy rights are protected and privacy obligations are imposed on certain entities, including both third-party data brokers and users of data products and services. The ongoing Privacy Act Review is an important opportunity to enhance the privacy framework and to ensure Australia's privacy settings empower individuals, protect their personal information and best serve the Australian economy in the digital age. Many of these proposals would help to address the privacy risks and harms that can arise in relation to the personal information handling practices of third-party data brokers.

79. In considering potential regulatory responses to address broader issues in the data brokerage sector, the privacy framework should be taken into account to ensure Australia's consumer and privacy frameworks continue to operate effectively together to promote consumer welfare.