Australian Government

Office of the Australian Information Commissioner

Digital Platforms: Government consultation on ACCC's regulatory reform recommendations

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

20 February 2023

OAIC

Contents

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to respond to Treasury's consultation on regulatory reform for digital platforms (the Consultation 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 Consultation Paper invites feedback on proposed reforms that seek to address competition and consumer issues identified in relation to digital platform services, as recommended by the ACCC in the fifth interim report of the *Digital Platform Services Inquiry* (Regulatory Reform Interim Report).

4. Digital platforms have helped to transform the daily lives of Australians, changing the way that individuals interact socially, conduct business, and receive services in the 21st century. The Consultation Paper acknowledges the benefits that digital platform services provide to consumers and businesses.

5. However, the ACCC has found that the importance and widespread use of large digital platforms creates opportunities and incentives for these platforms, and parties using their services, to engage in conduct that harms consumers, competition, and the economy.[1] The market power of large digital platforms has, in part, resulted from the significant amounts of data and personal information that they collect, use, and share, both in Australia and internationally.

6. The ACCC's past inquiries into digital platform services have identified the competitive advantages that established digital platforms derive from access to large data holdings.[2] In recognition of those advantages, the Regulatory Reform Interim Report proposed reforms that seek to address the data volume and quality advantages held by established digital platforms (incumbents) to address competition concerns in the supply of digital platform services.

7. The Consultation Paper acknowledges that privacy impacts need to be considered before implementing proposals that would increase competitors' access to user data, which highlights the distinct but complementary roles of competition, consumer and privacy laws.[3] This

---

[1] ACCC, *Digital platform services inquiry - Interim report No. 5 - Regulatory reform*, ACCC, 11 November 2022, accessed 12 January 2023, p 6.

[2] For our previous submissions to these inquiries see: OAIC, *Digital Platforms Inquiry — submission to the Australian Competition and Consumer Commission*, OAIC, 17 April 2018, accessed 12 January 2023; OAIC, *Digital Platforms Inquiry Preliminary Report — submission to the Australian Competition and Consumer Commission*, OAIC, 15 May 2019, accessed 12 January 2023; OAIC, *Digital Advertising Services Inquiry – Interim Report: Submission by the Office of the Australian Information Commissioner*, OAIC, 31 March 2021, accessed 12 January 2023; OAIC, *Digital Platform Services Inquiry Discussion Paper for Interim Report No 5 – submission to the ACCC*, OAIC, 22 April 2022, accessed 12 January 2023.

[3] Treasury, *Digital Platforms: Government consultation on ACCC's regulatory reform recommendations - Consultation Paper*, Treasury, 20 December 2022, accessed 12 January 2023, p 7. These issues were also explored in the ACCC's Digital Platforms Inquiry, which considered the data practices of digital platforms and recognised the important intersections between

submission focusses on the proposed measures that are likely to intersect with privacy considerations.

Co-ordination with other government policies and processes

8. The Consultation Paper seeks feedback on how the recommendations of the ACCC's Regulatory Reform Interim Report align with other Government policies and processes, including the best way to ensure coherence between Government policies relating to digital platforms.[4]

9. The OAIC has observed growing intersections between the privacy, competition and consumer law regulatory frameworks, particularly in relation to the handling of data. As noted in the Regulatory Reform Interim Report, the goals of promoting competition and protecting consumer privacy and security online often complement each other.

10. While there are synergies between these frameworks, it is important to note that there are also variances given that each regulatory framework is designed to address different economic, societal and policy issues. In this way, both regimes are essential and complementary components in the ring of defence that is being built to address the risks and harms faced by Australians in the online environment.

11. As the Consultation Paper observes, the Attorney-General's Department has undertaken a review of the *Privacy Act 1988* (Cth) (Privacy Act Review). The proposals of the Privacy Act Review are intended to ensure that Australia's privacy framework empowers consumers, protects their data, and best serves the Australian economy.[5]

12. The ACCC noted in the Regulatory Reform Interim Report that before data portability or access measures are considered for inclusion in any codes (discussed further below), consideration will need to be given to changes that result from the Privacy Act Review and whether there is a need for further safeguards.[6]

13. The OAIC is supportive of an approach that considers the outcomes of the Privacy Act Review in the development of competition and consumer regulatory reform, which recognises the intersections between privacy, competition and consumer law. A coordinated approach will continue to ensure that the distinct but complementary roles of privacy, competition and consumer laws work cohesively and comprehensively to address online risks and harms.

14. The intersection of competition, consumer and privacy law also highlights the importance of regulatory cooperation. Where different regulators exercise different functions under various

---

privacy, competition and consumer law. See ACCC, *Digital Platforms Inquiry – Final Report*, ACCC, June 2019, accessed 12 January 2023, pp 434-435.

[4] Treasury, *Digital Platforms: Government consultation on ACCC's regulatory reform recommendations - Consultation Paper*, Treasury, 20 December 2022, accessed 12 January 2023, p 7.

[5] See Attorney General's Department (AGD), *Privacy Act Review Report*, AGD, February 2023, accessed 20 February 2023. See also, OAIC, *Privacy Act Review – Discussion Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2021, accessed 12 January 2023.

[6] ACCC, *Digital platform services inquiry - Interim report No. 5 - Regulatory reform*, ACCC, 11 November 2022, accessed 12 January 2023, p 165, 174.

laws, it is important for regulators to work together to avoid unnecessary or inadvertent overlap 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.

15. An effective approach requires complementary expertise, and collaboration and coordination between regulators to ensure proportionate, efficient and cohesive regulation of digital platforms.

16. The OAIC has an effective, collaborative and longstanding working relationship with the ACCC and other domestic regulators, including through the memorandum of understanding on exchanges of information and our participation in the Digital Platform Regulators Forum (DP-REG).

17. DP-REG is an initiative between the OAIC, ACCC, Australian Communications and Media Authority (ACMA) and Office of 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.

Recommendation 1 – Consider the outcomes of the Privacy Act Review in the development of competition and consumer reform measures to ensure the distinct but complementary roles of privacy, competition and consumer laws continue to work cohesively and comprehensively to address online risks and harms.

Consumer recommendations

18. The Consultation Paper invites comment on the recommendations of the Regulatory Reform Interim Report that seek to address consumer harms that are attributable to digital platforms. This submission focusses on proposals to improve dispute resolution processes for consumers.

Effective dispute resolution processes

19. The Regulatory Reform Interim Report recommended that digital platforms should be subject to minimum internal dispute resolution standards and that an independent ombudsman scheme should be established to resolve complaints and disputes between consumers and digital platforms, as well as between businesses and digital platforms. This is in response to concerns around the persistent lack of accountability and effective redress for complaints and disputes arising on digital platforms.[7]

20. The Privacy Act encourages resolution of complaints by the individual and the entity where an individual alleges an entity has mishandled their personal information. Digital platforms

[7] ACCC, *Digital platform services inquiry - Interim report No. 5 - Regulatory reform*, ACCC, 11 November 2022, accessed 12 January 2023, pp 88-91.

regulated by the Privacy Act must take such steps as are reasonable to implement practices, procedures and systems that will enable them to deal with inquiries or complaints from individuals about the platform's compliance with the Australian Privacy Principles or a registered APP code that binds them.[8]

21. Minimum internal dispute resolution standards could help to facilitate the resolution of privacy complaints in addition to other complaints about digital platform services by promoting robust processes that resolve complaints quickly and efficiently.

22. The Regulatory Reform Interim Report also recommends that an external digital platforms ombudsman could assist with handling complaints and disputes where they have not been resolved to the consumer or business user's satisfaction. The Regulatory Reform Interim Report suggests that 'an industry-specific ombuds would be preferable given that an existing body may not have the capability and capacity to undertake this role.'[9]

23. The OAIC has previously submitted that careful consideration should be given to whether the functions of an existing body could be expanded rather than establishing a new body.[10] However, whether this is appropriate will depend on the scope of complaints the body will receive and whether there is a sufficient connection with its remit. It will be important for the scope of any ombudsman or industry complaints body to be clearly defined through public terms of reference so that individuals and regulated entities understand when it is appropriate to go the ombudsman.

24. There may also be an intersection between complaints about digital platforms and privacy complaints. In the OAIC's experience, depending on their terms of reference, an advantage of industry complaint bodies is an ability to address the full range of issues in a complaint. This can assist consumers in the context of digital platforms, where an individual may have a privacy concern as one component of a broader complaint.

25. The Privacy Act already contemplates that privacy complaints may be dealt with by an external dispute resolution (EDR) scheme and includes a mechanism for the Commissioner to recognise these schemes. We consider that any industry complaints body should have jurisdiction to receive consumer privacy complaints connected to the broader jurisdiction of the ombudsman and the capacity to be recognised as an EDR scheme under the Privacy Act. This recognition would enable the industry complaints body to use the established referral and information sharing procedures under the Privacy Act.[11]

Recommendation 2 – Mandatory minimum internal dispute resolution standards for digital platforms should be progressed.

---

[8] *Privacy Act 1988* (Cth) sch 1, APP 1.2(b).

[9] ACCC, *Digital platform services inquiry - Interim report No. 5 - Regulatory reform*, ACCC, 11 November 2022, accessed 12 January 2023, p 103.

[10] OAIC, *Digital Platform Services Inquiry Discussion Paper for Interim Report No 5 – submission to the ACCC*, OAIC, 22 April 2022, accessed 12 January 2023.

[11] See *Privacy Act 1988* (Cth) ss 35A, 50; OAIC, *Guidelines for recognising external dispute resolution schemes*, OAIC, 29 September 2013, accessed 13 January 2023.

Recommendation 3 – Any industry complaints body for digital platforms should have jurisdiction to manage consumer privacy complaints connected to the broader jurisdiction of the ombudsman and the capacity to be recognised as an EDR scheme under the Privacy Act.

Competition recommendations

26. The Consultation Paper invites views on the ACCC's recommendation for the introduction of mandatory service-specific codes that would apply to designated digital platforms that hold a 'critical position in the Australian economy and that have the ability and incentive to harm competition'. The service-specific codes would create targeted obligations to promote competition in markets for digital platform services.

27. This submission focusses on the proposed measures that seek to address data-related barriers to entry and expansion contemplated by Recommendation 4 of the Regulatory Reform Interim Report. The ACCC expressed concern that a lack of access to data is a substantial barrier to entry and expansion in the supply of some digital platform services, including search and ad tech services.[12]

Data access obligations

28. Section 6.6.2 of the Regulatory Reform Interim Report proposes data access obligations, which would require designated digital platforms to provide access to specific data sources on an agreed basis to rivals (including in adjacent markets) as a way to address the incumbents' competitive advantage derived from data.[13]

29. The ACCC considered that data access obligations could promote competition in search and ad tech services, and that codes of conduct for search services and ad tech services could include obligations on designated digital platforms to share click-and-query data and first-party data, respectively.[14]

30. The Regulatory Reform Interim Report acknowledges that data access requirements, especially those involving access to personal information, can raise privacy concerns.

31. For instance, data access obligations will lead to increased data flows between digital platforms. The combination of these data sets may generate more granular insights and profiles of individuals, which gives rise to an increased privacy risk. Search and ad tech data has the

[12] ACCC, *Digital platform services inquiry - Interim report No. 5 - Regulatory reform*, ACCC, 11 November 2022, accessed 12 January 2023, p 165.

[13] We note that the Regulatory Reform Interim Report uses 'data access' as a generic term to capture a range of mechanisms to transfer, exchange, share or otherwise provide a third party digital platform with access to data. This differs from the meaning of information access in the Privacy Act, where it generally refers to an individual's right to obtain information about them that is collected or created by others. Both the Privacy Act and the FOI Act provide rights of access to information. In this submission, we use data access in the sense that it is used in the Regulatory Reform Interim Report.

[14] ACCC, *Digital platform services inquiry - Interim report No. 5 - Regulatory reform*, ACCC, 11 November 2022, accessed 12 January 2023, p 168.

potential to reveal highly sensitive information if it is provided in such a way that it can be linked to an individual. Furthermore, mandatory data access obligations may require data to be transferred without the consent of the individuals concerned.[15] Without appropriate safeguards in place, individuals may be subjected to an increased privacy risk, and higher risk of data breach, discrimination, exclusion or profiling.[16]

32. While the Privacy Act recognises that the right to privacy is not absolute and that privacy rights may give way to compelling public interest reasons, whether this is appropriate will depend on whether any privacy impacts are reasonable, necessary and proportionate to achieving a legitimate objective.

33. We consider that data access obligations ought to be approached cautiously due to the potential privacy impacts involved. We recommend that additional consultation is undertaken on potential privacy risks and impacts if this proposal is developed further. This will allow stakeholders to provide targeted comments about the privacy risks of the specific use cases, whether any impacts are reasonable, necessary and proportionate to the competition-enhancing objectives, how any privacy risks can be mitigated or eliminated, and whether it is in fact possible to adequately minimise or eliminate them.

34. The ACCC has also noted that data access obligations should not be introduced unless privacy and security risks can be appropriately managed, and that they should not be considered until after the introduction of any privacy law reforms that result from the Privacy Act Review.[17]

35. If the proposed data access measures are further developed, consideration should be given to safeguards that can be put in place to mitigate or eliminate privacy risks. For instance, the codes could require robust de-identification of click-and-query, third party data or any other data that may be shared and include additional safeguards, such as testing for risk of possible re-identification or technical standards as to how the information is to be de-identified. [18]

36. Information that has undergone an appropriate and robust de-identification process is not personal information and is not currently subject to the Privacy Act.[19] This requires there to be no reasonable likelihood of re-identification occurring in the context that the data will be made available.

---

[15] We note that the proposed data access obligation (as distinct from the proposed data portability obligation) would not likely be initiated by consumers. See, ACCC, *Digital platform services inquiry - Interim report No. 5 - Regulatory reform*, ACCC, 11 November 2022, accessed 12 January 2023, p 170, which stated that 'In some circumstances, data portability measures may raise fewer privacy concerns than data access measures, as data portability measures generally involve consumers initiating such data transfers.'

[16] ACCC, *Digital platform services inquiry - Interim report No. 5 - Regulatory reform*, ACCC, 11 November 2022, accessed 12 January 2023, p 173.

[17] ACCC, *Digital platform services inquiry - Interim report No. 5 - Regulatory reform*, ACCC, 11 November 2022, accessed 12 January 2023, p 168. See also, AGD, *Review of the Privacy Act 1988 – Discussion Paper*, AGD, October 2021, accessed 12 January 2023.

[18] We discussed these principles in the context of advertising services in our submission to the ACCC's Advertising Services Inquiry Interim Report. See OAIC, *Digital Advertising Services Inquiry – Interim Report: Submission by the Office of the Australian Information Commissioner*, OAIC, 31 March 2021, accessed 19 January 2023.

[19] Note however that the Privacy Act Review Report has proposed that de-identified information be granted new protections by the Privacy Act, including in relation to security, cross-border disclosures and targeting. See, AGD, *Privacy Act Review Report*, AGD, February 2023, accessed 20 February 2023, pp 38-39.

37. Appropriate de-identification may be complex, especially in relation to detailed datasets that may be disclosed widely and 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. This may be particularly challenging in the context of digital platforms that have strong incentives to build detailed profiles of their users.

38. In addition, de-identification is not a fixed or end state. Data may become personal information as the context changes. Managing this risk will require regular re-assessment, particularly if an entity receives and assimilates additional data, even at an aggregate level, through other proposed data access mechanisms. If this proposal is to be considered further, the OAIC recommends that digital platforms be prohibited from re-identifying these data sets as a way to manage the re-identification risk that can emerge over time. Similar protections have been contemplated by the Privacy Act Review Report, which recommended that APP entities be prohibited from re-identifying de-identified information obtained from a source other than the individual to whom the information relates, with appropriate exceptions. [20]

39. If aggregated, de-identified or anonymised data access measures are considered, the OAIC also recommends that Treasury have regard to the OAIC's guidance on de-identification as well as the De-Identification Decision-Making Framework, produced jointly by the OAIC and CSIRO-Data61.[21]

40. Finally, consideration should be given to transparency measures that may be needed to inform digital platform users of the data access arrangements. Transparency measures are 'intended to ensure that individuals have knowledge of, and choice and control over, how information about them is handled' by entities.[22] For example, the proposed reforms could require users to be informed that their personal information will be de-identified and that the de-identified information will be shared with other digital platforms, in addition to details on how the de-identification process is undertaken.

Recommendation 4 – Data access obligations ought to be approached cautiously due to the potential privacy impacts involved. Additional consultation should be undertaken on potential privacy risks and impacts if this proposal is developed further and whether it is in fact possible to adequately minimise or eliminate them.

Recommendation 5 – Consideration should be given to safeguards that would require robust de-identification of data, such as testing for risk of possible re-identification or technical standards as to how the information is to be de-identified. Treasury should have regard to the

[20] AGD, *Privacy Act Review Report*, AGD, February 2023, accessed 20 February 2023, pp 40-41.

[21] See OAIC, *De-identification and the Privacy Act*, OAIC, 21 March 2018, accessed 19 January 2023; CM O'Keefe, S Otorepec, M Elliot, E Mackey, and K O'Hara, *The De-Identification Decision-Making Framework*, OAIC and the CSIRO's Data61, 18 September 2017, accessed 19 January 2023.

[22] Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021) [109].

OAIC's guidance on de-identification as well as the De-Identification Decision-Making Framework, produced jointly by the OAIC and CSIRO-Data61.

Recommendation 6 – If this proposal is considered further, digital platforms should be prohibited from re-identifying data sets that are provided to them in a de-identified state.

Recommendation 7 – Consideration should be given to appropriate transparency measures that may be needed to inform digital platform users of the data access arrangements.

High-risk data sets

41. When considering proposals that would increase access to data between digital platforms, it is important to examine the privacy risks that would attach to the particular types of data involved.

42. The Privacy Act defines certain categories of information as sensitive information due to its higher risk and potential to give rise to unjustified discrimination. This includes information about an individual's racial or ethnic origin, religious beliefs, sexual orientation and health information.[23] This kind of information may be included in or inferred from data sets held by digital platforms. For example, an individual's search history may reveal information about their sexual orientation or health conditions.

43. Sensitive information is generally afforded a higher level of privacy protection under the APPs. Sensitive information may only be handled under certain conditions, such as where an individual's consent has been obtained.[24] Additional limitations are also placed on secondary uses and disclosures of sensitive information.[25] This recognises that inappropriate handling of sensitive information can have adverse consequences for an individual or those associated with the individual.

44. Location information may also pose high privacy risks. Location information is often considered particularly invasive by the community where its collection, use or disclosure is not reasonably necessary for the operation of the relevant service or product or is not reasonably expected by the user.

45. Nearly two-thirds (62%) of Australians are uncomfortable with digital platforms or online businesses tracking their location through their mobile or web browser.[26] While the level of privacy risk depends on the precision of the information, location information is capable of revealing categories of sensitive information, for example, through tracking attendance at a place of worship or medical centre. Location information can also be very difficult to de-identify and carries a high re-identification risk.

[23] *Privacy Act 1988* (Cth) s 6(1).

[24] See *Privacy Act 1988* (Cth) sch 1, APPs 3.3, 3.4, 7.4.

[25] See *Privacy Act 1988* (Cth) sch 1, APPs 6.1, 6.2.

[26] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to OAIC, September 2020, p 79.

46. If the proposed data access obligations may cover data sets that include sensitive information or location data, careful consideration will be needed about the controls and safeguards that would appropriately limit the associated privacy risks. Examples of additional protections could include purpose limitations or prohibitions, limits on the types of personal information that the recipient is permitted to combine and requiring that personal information is handled in a manner that is fair and reasonable in the circumstances, as proposed by the Privacy Act Review Report.[27]

47. The OAIC's submission to the Privacy Act Review Discussion Paper also considered the introduction of a restricted and prohibited practices regime under the Privacy Act.[28] The restricted practices regime would require entities that engage in certain prescribed activities to take steps to identify privacy risks and implement measures to mitigate those risks.

48. Restricted practices could include, inter alia, the collection, use or disclosure of sensitive information on a large scale and location data on a large scale, the collection, use or disclosure of personal information for the purposes of online personalisation and targeted advertising, the sale of personal information and any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual.

Recommendation 8 – The privacy risks and impacts associated with particular types of data sets being subject to data access mechanisms should be carefully considered. Consideration should also be given to whether appropriate limitations, controls and safeguards can be implemented to mitigate those risks and impacts.

Data portability requirements

49. The Regulatory Reform Interim Report contemplated data portability measures to address the anti-competitive effects of consumer lock-in and by facilitating consumer switching between competing digital platform services.[29] The ACCC noted that this would allow a consumer to request that a designated digital platform transfer their data to them or a third party in a structured, commonly used and machine-readable format, either on an ad-hoc or continuous basis.[30]

50. When considering data portability proposals, it is relevant to note the significant community concern about the data handling activities of digital platforms. For example, the OAIC's 2020 Australian Community Attitudes to Privacy Survey found that Australians consider the social media industry the most untrustworthy in how they protect or use personal information.[31] We

[27] AGD, *Privacy Act Review Report*, AGD, February 2023, accessed 20 February 2023, pp. 116-120, Proposals 12.1 and 12.2.

[28] OAIC, *Privacy Act Review – Discussion Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2021, accessed 12 January 2023, pp 96-114.

[29] ACCC, *Digital platform services inquiry - Interim report No. 5 - Regulatory reform*, ACCC, 11 November 2022, accessed 12 January 2023, section 6.6.2.

[30] ACCC, *Digital platform services inquiry - Interim report No. 5 - Regulatory reform*, ACCC, 11 November 2022, accessed 12 January 2023, p 168.

[31] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to OAIC, September 2020, p 56.

note that the effectiveness and consumer uptake of any data portability right may depend on whether third parties that receive data have sufficient privacy and security protections in place.

51. As noted above, there have also been a range of inquiries that have examined the privacy and consumer harms that may arise from the data handling activities of digital platforms. In particular, we note the findings of the ACCC's Digital Platforms Inquiry, which identified a range of potential consumer harms arising from the collection, use and disclosure of personal information by digital platforms.[32]

52. While the Regulatory Reform Interim Report indicated that any data portability right would be exercised on request by the consumer, we consider that this should require that the consent be voluntary, express, informed, specific, time limited and easily withdrawn. The data portability scheme should also include appropriate privacy safeguards and be consistent with the Privacy Act and other data portability frameworks, such as the Consumer Data Right (CDR).[33]

A consumer-led approach

53. It is important for the consumer to retain choice and control over how their personal information is handled in data portability schemes. This is consistent with Australia's CDR and international data portability mechanisms.[34]

54. As part of facilitating choice and control, it will be relevant to consider what controls are available to the consumer at the time of consenting to the disclosure of their personal information and after the information has been disclosed. For example, the CDR scheme enables CDR consumers to provide access to data for limited purposes and time periods, includes mechanisms to withdraw consent, and confers rights to request erasure of their personal information in certain circumstances.

55. Different data sets may raise different considerations in relation to the level of consumer choice and control that is appropriate, due to their nature or sensitivity. Additionally, for data sets that contain the personal information of more than one individual, consideration should be given as to whether a consumer-led approach can be implemented and, if so, what mechanisms are needed to ensure appropriate control over joint data.

Appropriate privacy protections

56. It is important for data portability mechanisms to be designed with privacy in mind. The reliance of data portability regimes on individual requests requires appropriate transparency measures and controls to ensure that consent is fully informed and voluntary. In addition, data portability

---

[32] ACCC, *Digital Platforms Inquiry – Final Report*, ACCC, June 2019, accessed 12 January 2023, p 373-501.

[33] We discussed these principles in the context of advertising services in our submission to the ACCC's Advertising Services Inquiry Interim Report. To the extent data portability measures in the advertising technology space are further considered in this review, our previous submission may be of assistance. See OAIC, *Digital Advertising Services Inquiry – Interim Report: Submission by the Office of the Australian Information Commissioner*, OAIC, 31 March 2021, accessed 19 January 2023.

[34] See for example, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection) [2016] OJ L 119/1 (GDPR), art 20; European Parliament, *Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector* (Digital Markets Act), European Parliament, 15 December 2021, art 6(1)(h); *California Consumer Privacy Act of 2018*, 1.81.5 Cal Civ Code § 1798.100.

mechanisms should include other appropriate privacy safeguards, including data minimisation.[35] The robustness of the safeguards should be proportionate to any risks arising from the transfer of the data.

57. Relevant considerations include narrowly defining the scope of data that can be transferred, who can receive the data and appropriate limitations on the purposes for which the receiving entity can use the information it receives.

58. By way of example, the CDR scheme seeks to address privacy risks through obligations in relation to consent, transparency, accreditation and data minimisation. This scheme also expressly prohibits the use or disclosure of CDR data for certain purposes. Where appropriate, to address the risks created by any new data portability proposals in relation to digital platform services, Treasury could consider the privacy-enhancing features of the CDR as a model.

59. The OAIC's submission to the Privacy Act Review Discussion Paper also recommended privacy protections that may be relevant. For example, the OAIC recommended strengthened notice and consent requirements, rights to object to the handling of personal information and rights to request erasure of personal information.[36] The final Privacy Act Review Report has made similar proposals that seek to improve the clarity of collection notices and consent, along with the introduction of new individual privacy rights.[37]

60. More broadly, a positive duty for the collection, use and disclosure of personal information to be fair and reasonable would help to shift the burden of ensuring data handling is appropriate from individuals to regulated entities. [38] A positive obligation on digital platforms to handle personal information fairly and reasonably could help to mitigate potential privacy risks associated with digital platforms using information obtained through data access mechanisms for purposes the individual would not expect or agree to.

Interaction with the Privacy Act and CDR

61. The OAIC suggests that any new data portability right should be established within an existing regime such as the CDR or could leverage strengthened and tailored privacy protections contemplated in any reform to the Privacy Act, rather than through the establishment of a new regime. In doing so, it will be important to consider how this right aligns with the CDR and current rights to request access to personal information under the Privacy Act.[39] This should include consideration of any additional limits that should be placed on the data that digital

[35] Data minimisation is a key principle in the CDR - see Competition and Consumer (Consumer Data Right) Rules 2020 (Cth) r 1.8; OAIC, 'Chapter 3: Privacy Safeguard 3 – Seeking to collect CDR data from CDR participants', *CDR Privacy Safeguard Guidelines*, OAIC, 9 June 2021, accessed 19 January 2023.

[36] OAIC, *Privacy Act Review – Discussion Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2021, accessed 12 January 2023, pp 64-78; 128-144.

[37] AGD, *Privacy Act Review Report*, AGD, February 2023, accessed 20 February 2023, Chapters 10, 11 and 18.

[38] AGD, *Privacy Act Review Report*, AGD, February 2023, accessed 20 February 2023, pp. 116-120, Proposals 12.1 and 12.2. See also, OAIC, *Privacy Act Review – Discussion Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2021, accessed 12 January 2023, pp 79-95.

[39] See *Privacy Act 1988* (Cth) sch 1, APP 12. Data portability can be thought of as an extension to an individual's access rights under APP 12.

platforms would be able to access through existing schemes such as CDR, or if data portability rights were added to or built upon the Privacy Act.

Recommendation 9 – Any data portability right in relation to digital platforms should only be with the voluntary, express, informed, specific as to purpose, time limited and easily withdrawn consent of the individual.

Recommendation 10 – Any new data portability right should be established within an existing regime such as the CDR or Privacy Act. Consider whether additional restrictions would be needed to address the privacy risks of sharing data between digital platforms.

Data use limitations

62. Section 6.6.2 of the Regulatory Reform Interim Report considers measures to limit data use as a way of addressing the data advantages of some digital platforms, such as data separation measures or by prohibiting platforms from combining certain data sets.

63. As noted in our submission to the ACCC's Advertising Services Inquiry Interim Report, we support restricting or prohibiting the combination of data sets or the use of certain information, such as health information, for targeted advertising.[40]

64. If this recommendation is taken forward, consideration will need to be given to how these prohibitions would interact with limitations on secondary use and disclosure of personal information in the Privacy Act and the proposed prohibitions on certain forms of targeting in the Privacy Act Review Report, including on the basis of sensitive information and targeting that is directed towards children.[41]

Recommendation 11 – Proposals to limit data use by digital platforms should be progressed. Consideration should be given to how this would interact with the existing principles of the Privacy Act and measures proposed in the Privacy Act Review.

Consultation with Information Commissioner

65. The Regulatory Reform Interim Report recommended that any obligations in the proposed service-specific codes should be developed in consultation with industry and other stakeholders.[42] The ACCC further noted that new competition and consumer measures for

[40] OAIC, *Digital Advertising Services Inquiry – Interim Report: Submission by the Office of the Australian Information Commissioner*, OAIC, 31 March 2021, accessed 12 January 2023.

[41] AGD, *Privacy Act Review Report*, AGD, February 2023, accessed 20 February 2023, Proposals 20.1, 20.5-20.8.

[42] ACCC, *Digital platform services inquiry - Interim report No. 5 - Regulatory reform*, ACCC, 11 November 2022, accessed 12 January 2023, p 123.

digital platforms should be developed and implemented in a way to ensure close consultation and involvement of all relevant government departments and agencies.[43]

66. The OAIC recommends that the primary legislation that allows for the creation of mandatory codes of conduct for designated digital platforms should contain a provision that requires consultation with the Information Commissioner before the creation or registration of a code, where the content of that code may intersect with privacy and data protection issues.

67. There is precedent for such consultation requirements in other legislation, for example, s 53 of the *Office of the National Intelligence Act 2018*, s 355-72 of the *Taxation Administration Act 1953* and s 56AD of the *Competition and Consumer Act 2010*.

Recommendation 12 – The primary legislation that allows for the creation of mandatory codes of conduct for designated digital platforms should contain a provision that requires consultation with the Information Commissioner before the creation or registration of a code, where the content of that code may intersect with privacy and data protection issues.

[43] ACCC, *Digital platform services inquiry - Interim report No. 5 - Regulatory reform*, ACCC, 11 November 2022, accessed 12 January 2023, p 195.