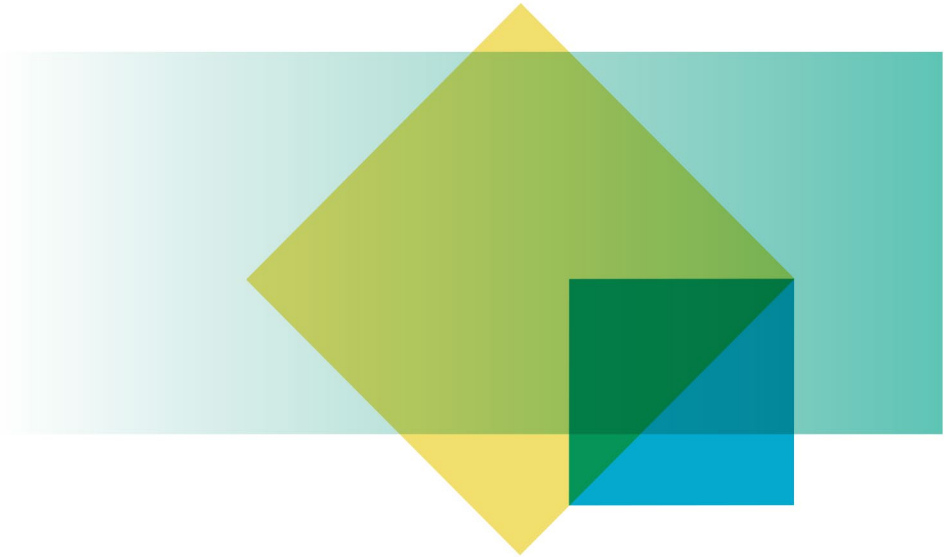
Australian Government

Office of the Australian Information Commissioner

Digital Platform Services Inquiry – Discussion Paper for Interim Report No 5

Submission by the Office of the Australian Information Commissioner



Angelene Falk

Australian Information Commissioner and Privacy Commissioner

22 April 2022

OAIC

Contents

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to respond to the Australian Competition and Consumer Commission's (ACCC) *Digital Platform Services Inquiry Discussion Paper for Interim Report No 5: Updating competition and consumer law for digital platform services* (the Discussion Paper).

2. The Discussion Paper considers whether the *Competition and Consumer Act 2010* and the Australian Consumer Law are sufficient to address the competition and consumer harms that have been identified in relation to digital platform services. This follows the findings and recommendations made in the ACCC's *Digital Platforms Inquiry*, *Digital Advertising Services Inquiry* and ongoing *Digital Platform Services Inquiry*.[1]

3. 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 Discussion Paper acknowledges the significant benefits digital platform services provide consumers and businesses.

4. However, the ACCC has also found that the concentration of market power amongst a few large digital platforms can have harmful consequences for competition as well as businesses and consumers.[2] The market power of large digital platforms has, in part, resulted from the significant increase in the amount of data and personal information collected, used, and shared, both in Australia and globally.

5. The ACCC's past inquiries into digital platform services have identified the competitive advantages established digital platforms derive from access to large data holdings. In recognition of those advantages, the Discussion Paper considers whether measures to address the data advantages leveraged by established digital platforms (incumbents) would be effective in addressing competition concerns in the supply of digital platform services.

6. The Discussion Paper acknowledges that consumer and privacy impacts need to be carefully considered before implementing proposals to increase data access, which highlights the distinct but complementary roles of competition, consumer and privacy laws.[3] While the operation of privacy law is excluded from this Inquiry, this submission focusses on the proposed measures in the Discussion Paper that are likely to intersect with privacy considerations.

---

[1] 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 7 April 2022; OAIC, *Digital Platforms Inquiry Preliminary Report — submission to the Australian Competition and Consumer Commission*, OAIC, accessed 15 May 2019, accessed 7 April 2022, OAIC, OAIC, *Digital Advertising Services Inquiry – Interim Report: Submission by the Office of the Australian Information Commissioner*, OAIC website, 31 March 2021, accessed 5 April 2022.

[2] ACCC, *Digital Platform Services Inquiry – Discussion Paper for Interim report No. 5: Updating competition and consumer law for digital platform services*, ACCC, February 2022, accessed 28 February 2022, p 4.

[3] 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 privacy, competition and consumer law. See ACCC, *Digital Platforms Inquiry – Final Report*, ACCC, June 2019, pp 434-435.

7. As the ACCC considers reforms to address competition and consumer issues in relation to digital platform services, it will also be important to consider developments in privacy law and regulation domestically and internationally. [4]

8. The intersection of competition, consumer and privacy laws also highlights the importance of regulatory cooperation. The OAIC has an effective, collaborative and longstanding working relationship with the ACCC, including through the memorandum of understanding on exchanges of information and our participation in the Digital Platform Regulators Forum.[5] We look forward to continuing our engagement with the ACCC to facilitate a consistent and coordinated response to the regulation of digital platforms.

Addressing data advantages

Increased access to data for rivals or potential rivals

9. Section 8.2.1 of the Discussion Paper considers measures to increase access to data for incumbent digital platforms' rivals or potential rivals as a way to address the incumbents' competitive advantage derived from data. The Discussion Paper seeks feedback on the benefits and risks of various data access measures, when they would be appropriate and the safeguards required to ensure they do not compromise consumers' privacy.[6]

10. Increasing access to personal information impacts privacy. While 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 this is appropriate will depend on whether any privacy impacts are reasonable, necessary and proportionate to achieving a legitimate objective.

11. Part of taking a proportionate approach is also considering what safeguards can be put in place to mitigate privacy risks. Accordingly, as noted in the Discussion Paper, 'any sharing and use of personal data should be accompanied by robust consumer-level controls that limit the privacy risks of data sharing and use'.[7]

12. There are relevant considerations for assessing the privacy impacts for each data access measure, which we have set out below. In assessing the privacy impacts, it will also be important to consider the combined impact of the proposed measures and existing policies. Measures to increase access to data for rivals or potential rivals of digital platforms will lead to increased data flows between digital platforms. The combination of these data sets or

---

[4] See AGD, *Review of the Privacy Act 1988 – Discussion Paper*, AGD, October 2021; OAIC, *Privacy Act Review – Discussion Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2021, accessed 19 January 2022. We note these proposals are subject to change subject to completion of the Review of the Privacy Act.

[5] OAIC, *MOU with ACCC — exchange of information*, OAIC website, August 2020, accessed 5 April 2022; Digital Platform Regulators Forum (DP-REG), *Terms of Reference* [PDF], DP-REG, 11 March 2022, accessed 8 April 2022.

[6] We note that the Discussion Paper 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 Discussion Paper.

[7] ACCC, *Digital Platform Services Inquiry – Discussion Paper for Interim report No. 5: Updating competition and consumer law for digital platform services*, ACCC, February 2022, accessed 28 February 2022, p 92.

combination of a single data set with a digital platform's existing data may provide richer insights and profiles of individuals, which may give rise to an increased privacy risk.

13. Accordingly, we consider that data access measures ought to be approached cautiously to ensure privacy impacts are minimised or eliminated. We recommend that if more defined proposals are developed further consultation is undertaken on the privacy risks. 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 benefits, and whether and how any privacy risks can be mitigated.

Recommendation 1 – The ACCC conducts further consultation on the privacy risks and impacts associated with any proposed data access measures if these proposals are further developed.

Data portability measures

14. The Discussion Paper contemplates data portability measures, which are intended to facilitate transfers of data at a consumer's request. Data portability could address the competitive advantage of large digital platforms by facilitating consumer switching between competing digital platform services.

15. In considering data portability 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, which may impact the effectiveness of any data portability right.[8]

16. 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.[9]

17. 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 Consumer Data Right (CDR).[10]

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

[9] ACCC, *Digital Platforms Inquiry – Final Report*, ACCC, July 2019, p 373-501.

[10] 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 website, 31 March 2021, accessed 5 April 2022.

A consumer-led approach

18. Where access is given to personal information it is important for the consumer to retain choice and control over the handling of their personal information. This is consistent with data portability mechanisms in Australia such as the CDR and internationally.[11] An important part of the CDR is that it generally requires consumers to expressly consent to any disclosures, collections and uses of their CDR data.

19. 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.

20. Different data sets may raise different considerations in relation to how choice and control should be implemented, due to their nature (this is discussed further below under 'High risk data sets'). Additionally, for data sets that contain the personal information of more than one individual the ACCC may need to consider 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

21. 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 mechanisms should include other appropriate privacy safeguards, including data minimisation.[12] The robustness of the safeguards should be proportionate to any risks arising from the transfer of the data.

22. Relevant considerations include narrowly defining the scope of what data 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.

23. By way of example, the CDR scheme seeks to address privacy risks through obligations around 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, the ACCC could consider the privacy-enhancing features of the CDR as a model.

---

[11] 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.

[12] 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 website, 9 June 2021, accessed 7 April 2022.

Interaction with the Privacy Act and CDR

24. The OAIC suggests the ACCC consider whether any new data portability right could be established within an existing regime such as the CDR scheme or 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.[13] This includes considering what additional limits should be placed on the data that digital 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. The scope of data access and disclosure should be carefully considered to mitigate the privacy risks arising from digital platforms combining data from multiple sources.

25. We acknowledge that there are policy considerations that will justify separate regimes and different privacy protections in certain circumstances. If a separate regime is created, it should not be unnecessarily duplicative with the Privacy Act or the CDR, minimise additional regulatory burden on entities and reduce complexity for consumers to activate their data portability rights.

26. As the ACCC considers these issues further, it is important to also consider the intersection with existing privacy risks to individuals arising from excessive online tracking and the use of their data.[14] These privacy risks exist independently of whether individuals have a data portability mechanism for their digital platform data and are important to address as a way of managing the privacy risk from the increased access to data by digital platforms that data portability would facilitate.

27. The OAIC's submission to the Discussion Paper for the Review of the Privacy Act contains recommendations relevant to mitigating these privacy risks. For example, enhancing privacy self-management mechanisms through strengthened notice and consent requirements, rights to object to the handling of personal information and rights to request erasure of personal information.[15]

28. 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. 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.[16]

[13] 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.

[14] ACCC, *Digital Platform Services Inquiry – Discussion Paper for Interim report No. 5: Updating competition and consumer law for digital platform services*, ACCC, February 2022, accessed 28 February 2022 pp 43-45.

[15] OAIC, *Privacy Act Review – Discussion Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2021, accessed 19 January 2022, pp 64-78; 128-144.

[16] OAIC, *Privacy Act Review – Discussion Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2021, accessed 19 January 2022, pp 79-95.

Recommendation 2 – 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 3 – Consider whether any new data portability right could sit appropriately in an existing regime such as the Privacy Act or CDR and what additional restrictions are needed to address the privacy risks of digital platform's access to data. If a new data portability right is created, the interaction of the scheme with the Privacy Act and the CDR scheme is considered.

Data interoperability

29. The Discussion Paper notes that data interoperability encourages the use of common frameworks and open systems to store and process data in ways that are technically compatible between services, including services offered by competing digital platform firms. Data interoperability can facilitate data portability, data sharing and data access measures.[17]

30. To the extent data interoperability permits third party digital platforms to access personal information, the principles set out above in relation to the need for privacy impacts to be reasonable, necessary and proportionate, for access to be consumer-led and for there to be appropriate privacy protections remain relevant.

31. Where data interoperability measures contemplate providing a third party platform with access to aggregated, anonymised or de-identified information it is important to carefully consider whether the information has been appropriately de-identified.[18]

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

33. 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, which have strong incentives to build detailed profiles of their users.

---

[17] ACCC, *Digital Platform Services Inquiry – Discussion Paper for Interim report No. 5: Updating competition and consumer law for digital platform services*, ACCC, February 2022, accessed 28 February 2022 pp 89-90.

[18] 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 interoperability measures in the advertising technology space are further considered in this review, our previous submission may be of assistance. See OAIC, OAIC, *Digital Advertising Services Inquiry – Interim Report: Submission by the Office of the Australian Information Commissioner*, OAIC website, 31 March 2021, accessed 5 April 2022.

34. 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 digital platforms be prohibited from re-identifying these data sets as a way to manage the re-identification risk that can emerge over time.

35. If aggregated, de-identified or anonymised data interoperability measures are considered, the OAIC also recommends that the ACCC 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.[19]

Recommendation 4 – If this proposal is considered further, digital platforms be prohibited from re-identifying data sets provided to them as de-identified data sets.

Recommendation 5 – If the ACCC develops a data interoperability regime or other data access measure that permits a third party digital platform to access de-identified information, the ACCC 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.

High-risk data sets

36. When considering proposals to increase access to data for digital platforms in the digital environment, it is important to consider the privacy risks attaching to the particular types of data involved.

37. Even where the proposed access mechanism is based on strong user consent, this may not provide sufficient protection for high-risk data. This is because consumers are not always well-placed to assess the risks and benefits of allowing their data to be accessed and analysed by third parties in more complex circumstances or may not feel that they are able to refuse consent. This risk increases with the sensitivity of the data, vulnerability of the individual, and where there is a lack of alternate options or pathways available. In some circumstances, further protections for the consumer should be considered.

38. The Privacy Act defines certain categories of information as sensitive information, as it is highly personal and has the potential to give rise to unjustified discrimination. This includes information such as racial or ethnic origin, religious beliefs, sexual orientation and health information.[20] This kind of information may be included in or inferred from data sets held by digital platforms. For example, the pages on social media that an individual likes or the groups they are a part of may provide information about their sexual orientation or health conditions.

---

[19] See OAIC, *De-identification and the Privacy Act*, OAIC website, 21 March 2018, accessed 6 April 2022; 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.

[20] *Privacy Act 1988* (Cth), s 6(1), definition of sensitive information.

39. Sensitive information is generally afforded a higher level of privacy protection under the APPs. These protections include consent requirements and additional limitations on secondary uses and disclosures.[21] This recognises that inappropriate handling of sensitive information can have adverse consequences for an individual or those associated with the individual.

40. Another potentially high-risk data set is location information. 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.

41. Nearly two-thirds (62%) of Australians are uncomfortable with digital platforms or online businesses tracking their location through their mobile or web browser.[22] 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 or carry a high re-identification risk.

42. If the ACCC proposes access measures for data sets that include sensitive information or location data, careful consideration will be needed 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.

43. The OAIC's submission to the Discussion Paper for the Review of the Privacy Act considers the introduction of a restricted and prohibited practices regime under the Privacy Act.[23] The restricted practices regime would require entities that engage in certain prescribed activities set out in the Privacy Act to take steps to identify privacy risks and implement measures to mitigate those risks.

44. 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 6 – That the privacy risks and impacts associated with the particular types of data sets that may be subject to data access mechanisms and whether appropriate controls and safeguards can be implemented to mitigate those risks and impacts are carefully considered.

[21] See *Privacy Act 1988* (Cth) sch 1 APPs 3.3, 6.1.

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

[23] OAIC, *Privacy Act Review – Discussion Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2021, accessed 19 January 2022, pp 96-114.

Other measures to increase data access

45. The Discussion Paper also seeks comment on other potential measures to increase access to data, including through data sharing or pooling arrangements and mandatory data access arrangements.

46. The Discussion Paper notes the ACCC's recommendation in its interim report on Search Defaults and Choice Screens that, subject to consideration of privacy impacts, certain search engine providers should provide mandatory access to click-and-query data, and potentially other data sets.[24]

47. Query, click and view data has the potential to include highly sensitive information about an individual if it is provided in such a way that it can be linked to the individual. Further, mandatory data access arrangements require data to be provided without the consent of individuals. Given the potential impacts on the privacy of the individual, it is critical that this data is appropriately de-identified.

48. If this proposal is further developed, we recommend that consideration is given to what safeguards can be put in place to appropriately de-identify click-and-query data, such as testing against possible re-identification or technical standards as to how information is to be de-identified. Key considerations in relation to the de-identification of personal information are outlined above.

49. While we have not considered other potential measures to increase data access in detail, the principles set out above in relation to the need for privacy impacts to be reasonable, necessary and proportionate, for access to be consumer-led and for there to be appropriate privacy protections remain relevant.

Recommendation 7 – If the proposal is further developed, consideration is given to what safeguards can be put in place to appropriately de-identify click-and-query data, such as testing against possible re-identification or technical standards as to how information is to be de-identified.

Limiting data use by incumbents

50. Section 8.2.2 of the Discussion Paper considers measures to limit data use as a way of addressing the data advantages of some digital platforms, such as through data silos that prevent combining data and prohibitions on using data collected for one purpose for other purposes.

[24] ACCC, *Digital platform services inquiry: Interim report No. 3 – Search defaults and choice screens*, ACCC, 28 October 2021, p 123.

51. As noted in our submission to the ACCC's *Advertising Services Inquiry Interim Report* we support the proposal to restrict or prohibit the combination of data sets or the use of certain information, such as health information, for targeted advertising.[25]

52. If the ACCC continues to develop this proposal, consideration will need to be given to how these prohibitions would interact with the Privacy Act noting that the Act contains certain requirements and limitations around the secondary use and disclosure of personal information. However, it does not contain explicit prohibitions on the combination of data sets or the use of particular types of personal information for different purposes. Consideration should also be given to how this proposal may intersect with reforms proposed in the Review of the Privacy Act.

Recommendation 8 – The ACCC progresses proposals to limit data use by incumbent digital platforms and considers how this would interact with the Privacy Act and measures proposed in the Privacy Act Review.

Effective Dispute Resolution Processes

53. The Discussion Paper notes the ACCC's continued support for measures that would require digital platforms to 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.[26]

54. 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 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.[27]

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

56. Where internal complaints mechanisms do not resolve a complaint, the Discussion Paper supports the digital platforms ombudsman as a potential response to online scams, harmful online content such as apps that do not allow users to unsubscribe, directing gambling-like apps towards children, and fake reviews of businesses. It would be important for the scope of any ombudsman or industry complaints body to be clearly defined through public terms of

[25] OAIC, *Digital Advertising Services Inquiry – Interim Report: Submission by the Office of the Australian Information Commissioner*, OAIC website, 31 March 2021, accessed 5 April 2022.

[26] ACCC, *Digital Platform Services Inquiry – Discussion Paper for Interim report No. 5: Updating competition and consumer law for digital platform services*, ACCC, February 2022, accessed 28 February 2022, p 100.

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

reference so that individuals and regulated entities understand when it is appropriate to go the ombudsman.

57. Given the range of existing regulatory bodies operating in relation to digital platforms, careful consideration should be given to whether the functions of an existing body could be expanded rather than establishing a new body. As suggested in the ACCC's Digital Platforms Inquiry Final Report, the Telecommunications Industry Ombudsman could serve as the relevant industry complaints body.[28] Whether this is appropriate will depend on the scope of complaints the body will receive and whether there is a sufficient connection with the remit of the Telecommunications Industry Ombudsman.

58. Regardless of where these dispute resolution functions sit, there may 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 the data-driven business model is capable of giving rise to privacy concerns as a component of broader complaints.

59. The Privacy Act already contemplates privacy complaints being dealt with by an external dispute resolution (EDR) scheme, and includes a mechanism for the Commissioner to recognise these schemes. We consider 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. [29]

Recommendation 9 –Mandatory minimum internal dispute resolution standards for digital platforms be progressed.

Recommendation 10 – An industry complaints body for digital platforms continue to be part of the complaints resolution solution considered by the ACCC

[28] ACCC, *Digital Platforms Inquiry – Final Report*, ACCC, July 2019, pp 509-510.

[29] See *Privacy Act 1988* (Cth) ss 35A, 50; OAIC, *Guidelines for recognising external dispute resolution schemes*, OAIC website, 29 September 2013, accessed 22 April 2022.