



**Australian Government**

**Office of the Australian Information Commissioner**

# Mandatory news media bargaining code – Concepts paper

Submission by the Office of the Australian Information Commissioner



Angelene Falk

Australian Information Commissioner and Privacy Commissioner

5 June 2020

OAIC

## Executive summary

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the Australian Competition and Consumer Commission's (ACCC) *Mandatory news media bargaining code – Concepts paper* (the concepts paper).
2. The OAIC acknowledges the policy objective behind the development of a mandatory code of conduct (the bargaining code), which is to address bargaining power imbalances between Australian news media businesses and digital platforms. We note that the bargaining code will initially apply to Google and Facebook with the potential for it to be expanded to other digital platforms in the future. The concepts paper outlines key issues that may be covered by the bargaining code, including the sharing of user data between digital platforms and news media businesses. We note that the bargaining code is one of the key competition-related commitments from the Australian Government's response to the Digital Platforms Inquiry (DPI) final report.<sup>1</sup>
3. The Government's response to the DPI final report also confirmed its commitment to strengthening and enhancing online privacy protections for consumers. This includes the development of a binding online privacy code, which will apply to digital platforms including Facebook and Google. The Government will also consult on reforms to the *Privacy Act 1988* (Cth) (Privacy Act) that include strengthening notice and consent requirements to ensure entities meet best practice standards, and will commence a broader review of the Privacy Act to ensure that it empowers consumers, protects their data and best serves the Australian economy.
4. We note that the accelerated timeframes for the mandatory bargaining code mean that it will be implemented before the planned public consultation on reforms to the Privacy Act and the online privacy code. The concepts paper indicates that the bargaining code may cover key matters that are to be considered as part of these reforms, including what constitutes personal information and the role and form of notice and consent. Consequently, we recommend that the ACCC take a cautious approach to setting specific requirements in the code around these key issues to avoid pre-empting or conflicting with any policy changes that are to be carefully examined ahead of the proposed privacy reforms.
5. Proposals to share user data, or increase the amount and types of user data that are currently being shared, as set out in the concepts paper, raise a number of important privacy issues that warrant careful consideration to ensure the handling of user data is consistent with the Privacy Act and community expectations.
6. Digital platforms collect large amounts of user data about individuals, including 'personal information'<sup>2</sup> and anonymised, pseudonymised or aggregated data.<sup>3</sup> Privacy protections in the Privacy Act and the Australian Privacy Principles (APPs) apply to the handling of 'personal information'. However, it is not always possible to draw a bright line between personal information and de-identified information. Whether information can 'reasonably identify' an

---

<sup>1</sup> The Treasury, *Government Response and Implementation Roadmap for the Digital Platforms Inquiry*, 12 December 2019, <https://treasury.gov.au/publication/p2019-41708>.

<sup>2</sup> 'Personal information' means 'information or an opinion about an identified individual, or an individual who is reasonably identifiable. See *Privacy Act 1988* (Cth), s 6(1).

<sup>3</sup> As outlined in the ACCC's *Digital Platforms Inquiry final report*, pg. 407

individual requires a contextual consideration of the particular circumstances and the entities that hold the information.

7. While the concepts paper contains limited detail around the type or amount of user data that may be shared, user data is likely to include personal information, and even where anonymised or aggregated information is shared, the risks of re-identification may remain.
8. If the ACCC considers that the bargaining code should include data sharing measures, any limitation on the right to privacy resulting from these measures must be reasonable, necessary and proportionate to achieving a legitimate policy objective of the code.<sup>4</sup> This submission discusses some of the limitations associated with the consent-based approach proposed in the concepts paper, and makes high level recommendations for measures that could be included in the bargaining code to ensure that there are appropriate limitations on data sharing and help to mitigate the risks of re-identification when sharing de-identified user data.
9. In particular we recommend that the ACCC conduct a privacy impact assessment (PIA) for any proposals to share user data under the bargaining code. A PIA will assist the ACCC to identify the privacy impacts that the proposed data sharing mechanisms may have on individuals, and identify measures for managing, minimising or eliminating those impact. The *Privacy (Australian Government Agencies – Governance) APP Code 2017* requires agencies to undertake PIAs for all high privacy risk projects.
10. The OAIC is available to provide advice and consult with the ACCC on the operation of the Privacy Act and reforms to Australia’s broader privacy framework during the development of the bargaining code.

## Interaction with the Australian privacy framework

11. As outlined above, strengthening and enhancing online privacy protections for consumers is a key objective of the privacy reform measures announced in the Government’s response to the DPI final report.
12. The Government will consult on draft legislation to amend the Privacy Act to require the development of a binding privacy code that will apply to social media platforms and other online platforms that trade in personal information.<sup>5</sup> The online privacy code will include a definition of the online platforms that the code applies to, and will require these entities to:
  - be more transparent about data sharing
  - meet best practice consent requirements when collecting, using and disclosing personal information

---

<sup>4</sup> All Bills and disallowable legislative instruments must also be accompanied by a [Statement of Compatibility](#), which must contain an assessment of the Bill or legislative instrument's compatibility with the rights and freedoms recognised in the seven core international human rights treaties which Australia has ratified. This includes the International Covenant on Civil and Political Rights, which states that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence, nor to unlawful attacks on their honour and reputation (article 17).

<sup>5</sup> The joint media release from the Attorney General and Minister for Communications and the Arts is available at: <https://www.minister.communications.gov.au/minister/mitch-fifield/news/tougher-penalties-keep-australians-safe-online>

- stop using or disclosing personal information on request, and
  - comply with specific rules to protect the personal information of children and vulnerable groups.
13. The Government also confirmed its commitment to consult on reforms to the Privacy Act to seek input on amending the definition of personal information and strengthening notice and consent requirements economy-wide, and to commence a broader review of the Privacy Act to identify any areas where consumer privacy protection can be improved while allowing for innovation and growth of the digital economy.<sup>6</sup>
  14. The privacy issues raised by the user data sharing proposals in the concepts paper therefore raise matters that are to be considered as part of these reforms, including what constitutes personal information and the role and form of notice and consent.
  15. To ensure that the data sharing mechanisms in the bargaining code do not pre-empt or conflict with these forthcoming changes to Australia’s privacy framework, we recommend that the bargaining code does not introduce new policies or requirements on matters to be considered as part of the privacy reforms, but instead generally relies on the existing Privacy Act framework to protect user data that may be shared under the code.
  16. The issues raised in the concepts paper highlight the value of the ongoing cooperative approach between the OAIC and the ACCC in the regulation of digital platforms. We remain committed to working with the ACCC and lending our data protection expertise during the development of the bargaining code.

## Sharing user data under the bargaining code

17. The concepts paper notes that digital platforms obtain a benefit from the data they collect due to users’ interactions with news content published or distributed on their services. As such, the paper notes that it may be reasonable from a commercial perspective for digital platforms to share this data with relevant news media businesses.
18. However, the paper also notes that comprehensive data sharing between digital platforms and news media businesses may not be appropriate or desirable given that Facebook and Google track users’ interactions with multiple websites, apps and platforms unrelated to news content. Further, the DPI final report found that the sharing of user data with third parties in the digital environment was a data practice of key concern for consumers, a finding consistent with the preliminary findings from the OAIC’s 2020 Australian Community Attitudes to Privacy survey, which found that 70% of Australians were uncomfortable with businesses sharing their personal information with other businesses. Eighty-three percent of Australians feel that an organisation revealing their personal information to another organisation is a misuse of that personal information.
19. Should the ACCC proceed with proposals to share user data under the bargaining code, data sharing should be consistent with the Privacy Act and community expectations.

---

<sup>6</sup> The Treasury, Government Response and Implementation Roadmap for the Digital Platforms Inquiry, 12 December 2019.

20. As noted above, user data collected by digital platforms includes personal information, anonymised, pseudonymised and aggregated information. Anonymised, pseudonymised and aggregated information will only be considered to be de-identified – and therefore no longer personal information for the purposes of the Privacy Act – where there is no reasonable likelihood of re-identification occurring, having regard to all the circumstances.<sup>7</sup>
21. The concepts paper asks whether it is appropriate for digital platforms to provide news media businesses with access to additional data associated with individual users (based on anonymised user IDs) such as whether a visit to a news media business’s website follows previous interaction with this business’s content on a digital platform. However, it is not clear from the concepts paper what ‘additional data’ could be provided to news media businesses. It is important to note that information, such as anonymised user IDs, may not be personal information when considered on its own. However, when combined with other information held by (or accessible to) an entity, or through the application of data analytics or other techniques, it may become ‘personal information’.
22. Information holdings can therefore be dynamic, and the character of information can change over time. It is essential to consider the aggregate impacts of data collection, which may increase the risks of re-identification of de-identified information.
23. As such, it is important to recognise that there are privacy risks inherent in sharing any user data, whether in identified, anonymised, pseudonymised or aggregated form. Proposals to share data that has been gathered by tracking users across platforms and websites also raise particular privacy risks that need to be carefully considered.
24. The Australian privacy framework recognises that the protection of individuals’ privacy is balanced with the interests of entities in carrying out their functions or activities. The Privacy Act provides a framework within which to balance the protection of individuals’ privacy with other legitimate objectives, provided that restrictions on privacy are reasonable, necessary and proportionate to achieving those objectives.<sup>8</sup>
25. Accordingly, if the bargaining code proposes to include mechanisms that may require or promote the sharing of identifiable or potentially identifiable user data between entities, the OAIC recommends that the ACCC ensure that these mechanisms are reasonable, necessary and proportionate to achieving the code’s policy objectives. To this end, the discussion below raises some of the limitations associated with the consent-based approach proposed in the concepts paper, and makes recommendations for additional measures that would assist in ensuring any data sharing mechanisms are reasonable, necessary and proportionate.
26. The concepts paper notes that, ‘any mechanisms in the code related to sharing of user data should be calibrated to prevent any increase to the collection and distribution of personally identifiable information without a user’s informed consent.’ The OAIC recognises that consent can support transparency, choice and control for consumers. These measures help individuals

---

<sup>7</sup> Section 6(1) of the Privacy Act defines ‘de-identified’ as: ‘personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable’. For more information on de-identification under the Privacy Act, see OAIC, *De-identification and the Privacy Act*, <https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/>

<sup>8</sup> *Privacy Act 1988* (Cth), s 2A.

to make informed decisions about their personal information, while ensuring that entities are accountable for how it is handled.

27. However, while consent is part of Australia's privacy framework, the challenges and complexities created by digital technologies in the online environment mean that individuals are not always well placed to assess the risks and benefits of allowing their personal information to be shared.
28. Consent must be freely given, specific, unambiguous, and informed, which can be particularly difficult to achieve in the digital environment where data flows and data practices are increasingly complex and difficult to understand.
29. Consent is only a meaningful and effective privacy self-management tool where the individual actually has a choice and can exercise control over their personal information. In many cases, consumers may feel resigned to consenting to the use of their information in order to access online services, as they do not consider there is any alternative.<sup>9</sup> Seeking consent for numerous purposes may also undermine the quality of consents obtained and result in consent fatigue for consumers.
30. The burden of understanding and consenting to complicated practices should not fall on individuals but must be supported by appropriate accountability obligations for digital platforms. Rather than relying on individual consent for additional data sharing between digital platforms and news media businesses, the OAIC recommends that the following measures are considered for inclusion in the bargaining code to ensure appropriate limitations on data sharing are in place and mitigate the risks of re-identification of user data.
31. The bargaining code could:
  - Require that all data that is shared under the bargaining code be anonymised, pseudonymised or aggregated, using appropriate technologies to minimise the risk of re-identification by the receiving parties.
  - Clearly set out the types and/or categories of user data that are permitted to be shared under the bargaining code to ensure clarity for regulated entities and consumers, noting that the parties should only be able to share the minimum amount of de-identified data necessary to achieve the defined purpose.
  - Clearly and narrowly define the purposes for which the user data may be used and disclosed by the parties under the bargaining code, and set limits on the acceptable purposes for which data may be shared (e.g. the code could prohibit on-sharing of the data to third parties, which could increase the risk of re-identification and be inconsistent with the expectations of digital platform users).
  - Include requirements around how the data should be secured, where it will be stored and when it must be destroyed.
  - Explicitly note that if user data shared by parties under the bargaining code is re-identified, it is subject to the Privacy Act.

---

<sup>9</sup> UK ICO, Big Data, AI, Machine Learning and Data Protection, 2017, page 24.

32. Finally, we recommend that the ACCC conduct a PIA for any proposed data sharing arrangements under the bargaining code. A PIA will assist the ACCC to identify the privacy impacts that the proposed data sharing mechanisms may have on individuals, and identify measures for managing, minimising or eliminating those impacts. In particular, the PIA should assess any risks posed to individual privacy arising from the collection of de-identified user data by news media companies, the subsequent uses it may be put to, and the potential for re-identification when held by different entities. Under the *Privacy (Australian Government Agencies – Governance) APP Code 2017*, agencies must conduct a PIA for all high privacy risk projects. A project may be a high privacy risk project if the agency reasonably considers that the project involves any new or changes ways of handling personal information that are likely to have a significant impact on the privacy of individuals.