Commissioner Initiated Investigation into Uber Technologies, Inc. & Uber B.V. (Privacy) [2021] AICmr 34 (30 June 2021)

Decision and reasons for decision of
Australian Information Commissioner and Privacy Commissioner, Angelene Falk

Respondent 1	Uber Technologies, Inc.
Respondent 2	Uber B.V.
Decision date	30 June 2021
Catchwords	Privacy — *Privacy Act 1988* (Cth) — Australian Privacy Principles — APP 11.1 — APP 11.2 — APP 1.2 — Extraterritorial jurisdiction — Unauthorised access to personal information by third party — Whether reasonable steps taken to protect personal information from unauthorised access — Whether reasonable steps taken to delete or de-identify personal information — Whether reasonable steps taken to implement practices, procedures and systems to ensure compliance with the APPs — Breaches substantiated – Requirement to prepare compliant Policies and Programs — Independent review of Policies and Programs

Determination

1. I find that the respondents, Uber Technologies, Inc. (**UTI**) and Uber B.V. (**UBV**) (collectively, **the Uber Companies**), have each:

   a. interfered with the privacy of approximately 1.2 million Australians by failing to comply with the following Australian Privacy Principles (**APPs**) in Schedule 1 of the *Privacy Act 1988* (Cth) (the **Privacy Act**):

      i. APP 11.1: requirement to take reasonable steps to protect personal information against unauthorised access

      ii. APP 11.2: requirement to take reasonable steps to delete or de-identify personal information that is no longer needed for a permitted purpose.

b. failed to comply with the requirement in APP 1.2 in Schedule 1 of the Privacy Act, to take reasonable steps to implement practices, procedures and systems relating to the entity's functions or activities, to ensure compliance with the APPs.

Declarations

2. I make the following declarations under s 52(1A) of the Privacy Act:

   a. In the period 13 October 2016 to 15 November 2016, the Uber Companies interfered with the privacy of approximately 1.2 million Australian riders and drivers by:

      i. failing to take reasonable steps in the circumstances to protect personal information they held from unauthorised access, in breach of APP 11.1

      ii. failing to take reasonable steps in the circumstances to destroy or de-identify personal information they held in breach of APP 11.2.

   b. The Uber Companies must not repeat the acts and practices referred to in paragraph 2(a).

   c. In the period 13 October 2016 to 15 November 2016, the Uber Companies failed to comply with the requirements of APP 1.2 to take reasonable steps in the circumstances to implement practices, procedures and systems relating to the Uber Companies' functions and activities that would ensure that they complied with the APPs.

   d. The Uber Companies must prepare the following policies, programs and plans (together, the **Policies and Programs**) within 3 months of the date of this Determination (**Determination Date**):

      i. a data retention and destruction policy that will, when implemented, enable and ensure compliance by the Uber Companies with APP 11.2.

      ii. an information security program that will, when implemented, enable and ensure compliance by the Uber Companies with APP 11.1, and which, at minimum:

         A. identifies risks to the security or integrity of personal information of Australian users collected and/ or held by the Uber Companies, that could result in misuse, interference or loss or unauthorised access, modification or disclosure of this information

         B. contains administrative, technical, and physical controls and procedures that are appropriate to the Uber Companies' circumstances (having regard to the factors set out in paragraph 82 of this Determination), to address the identified risks referred to in paragraph 2(d)(ii)(A)

         C. provides for regular testing and monitoring of the effectiveness of the above safeguards

         D. designates an employee or employees to coordinate and be responsible for the information security program

E. requires initial and regular refresher training in relation to the Information Security Program for personnel with access to Australian users' personal information, to the extent it is relevant to their role and responsibilities.

iii. an incident response plan that will, when implemented, enable and ensure compliance by the Uber Companies with APP 1.2, APP 11.1 and Part IIIC of the Privacy Act, and which, at minimum:

A. provides a clear explanation of what constitutes a data breach

B. outlines the roles and responsibilities of personnel when there is a data breach, or suspected data breach, including escalation triggers and pathways

C. requires testing and review of the incident response plan at least annually and following any notifiable data breach under Part IIIC, and the evaluation and revision of the incident response plan in light of such testing and review

D. includes a strategy for containing, assessing and managing data breaches, including remedial actions

E. includes a clear communications strategy that allows for notification of data breaches, where required by the Privacy Act and within the time limits required by the Privacy Act, to affected individuals and other relevant entities

F. outlines how the Uber Companies will record data breach incidents, including those that are not escalated to a data breach response team

G. establish a process for assessment of the Uber Companies post-breach response and the effectiveness of the Incident Response Plan.

e. Within 3 months of the Determination Date, the Uber Companies must engage an independent third party or third parties (the **Independent Expert**), that each have:

i. Certified Information Systems Security Professional (CISSP) or Certified Information Systems Auditor (CISA) certification, or a similarly qualified person or organisation

ii. at least five years' experience evaluating the effectiveness of computer systems or information system security

iii. demonstrated capacity in relation to assessing the requirements for compliance with the Privacy Act

iv. demonstrated capacity and sufficient available resources to complete tasks assigned in accordance with this declaration.

f. The Uber Companies must engage the Independent Expert to prepare a written report within 5 months of the Determination Date (the **Expert Report**) that:

i. specifies whether the Policies and Programs have been prepared in accordance with paragraph 2(d)

ii. if the Policies and Programs have not been prepared in accordance with paragraph 2(d):

A. specifies actions for the Uber Companies to complete, to ensure that the Policies and Programs are prepared in accordance with paragraph 2(d) (the **Policy Preparation Actions**)

B. sets out a plan, including reasonable timeframes, for the Uber Companies to complete the Policy Preparation Actions (with all Policy Preparation Actions to be completed within 3 months of the date of the Expert Report).

g. The Uber Companies must provide a copy of the Expert Report to my office, together with a document setting out any other actions proposed by the Uber Companies, within 14 days from the date of the Expert Report.

h. If the Expert Report specifies any Policy Preparation Actions for the Uber Companies to take, the Uber Companies must complete all Policy Preparation Actions within the timeframes specified in the Expert Report, but in any event, within 3 months of the date of the Expert Report.

i. The Uber Companies must provide my office with written confirmation from the Independent Expert when all Policy Preparation Actions have been completed.

j. The Uber Companies must implement the Policies and Programs within 12 months of the Determination Date, and will continue to implement and maintain the Policies and Programs for the purpose of ensuring that:

i. in respect of the Data Retention and Destruction Policy, such steps are taken by the Uber Companies as are reasonable in the circumstances to destroy or de-identify personal information they hold of Australian Users (where such information is no longer needed for a purpose under the APPs and which the Uber Companies are not required to retain by or under an Australian law or a court or tribunal order)

ii. in respect of the Information Security Program, such steps are taken by the Uber Companies as are reasonable in the circumstances to protect the personal information they hold of Australian Users from misuse, interference and loss and from unauthorised access, modification or disclosure

iii. in respect of the Incident Response Plan, such steps are taken by the Uber Companies to enable the Uber Companies to comply with their obligations in APPs 1.2 and Part IIIC of the Privacy Act.

k. The Uber Companies must engage the Independent Expert to:

i. complete a review, commencing on or about 30 months after the Determination Date, of the implementation and maintenance of the Policies and Programs, for the purposes of preparing the Supplementary Report (as defined in paragraph 2(k)(ii))

ii. prepare a supplementary written report (the **Supplementary Report**) within 36 months of the Determination Date which:

A. specifies whether the Policies and Programs, as at that time, are being maintained and implemented in accordance with paragraph 2(j)

B. if the Policies and Programs are not, as at that time, being maintained and implemented in accordance with paragraph 2(j), specifies actions for the Uber

Companies to complete, to ensure that the Policies and Programs are maintained and implemented in accordance with paragraph 2(j) (the **Implementation Actions**)

C. sets out a plan, including reasonable timeframes, for the Uber Companies to complete any Implementation Actions (with all Implementation Actions to be completed within 6 months of the date of the Supplementary Report).

l. The Uber Companies must provide a copy of the Supplementary Report, together with a document setting out any other actions proposed by the Uber Companies, to my office within 14 days of the date of the Supplementary Report.

m. If the Supplementary Report specifies any Implementation Actions for the Uber Companies to take, the Uber Companies must complete all Implementation Actions within the timeframes specified in the Supplementary Report, but in any event, within 6 months of the date of the Supplementary Report.

n. The Uber Companies must provide my office with written confirmation from the Independent Expert, when all Implementation Actions have been completed.

Findings and Reasons

3. This is a determination made under s 52(1A) of the Privacy Act in which I have made the findings set out in paragraph 1. This is my statement of findings as required by s 52(2) of the Privacy Act.

Background

4. In Australia, UBV offers a ride hailing service through a mobile application (the **Uber app**).[1] The service permits registered users to make requests for trips which are matched to nearby drivers on the Uber app. To use the Uber app, Australians must register via the Uber app, and provide their personal information including their name and email address, and in certain circumstances, a mobile phone number or a credit card number. Someone who wishes to drive on the Uber platform may also provide their driver's licence number.

5. UBV has offered the Uber app in Australia since September 2012. It also has a website available in Australia and has collected Australian rider and driver personal information through the Uber app and website since 2012. During the period in which the Data Breach occurred (as defined in paragraph 6), this personal information was provided directly to UTI, which was contractually required to process the information in accordance with UBV's instructions under a 2016 data processing agreement (the **2016 DPA**).[2]

6. In the period 13 October 2016 to 15 November 2016, data that UTI stored in a cloud-based storage service, was subject to an external cyberattack (the **Data Breach**) by individuals (the **Attackers**). The data was stored in Amazon Web Service's Simple Storage Service

[1] https://www.uber.com/legal/en/document/?name=general-terms-of-use&country=australia&lang=en-au.

[2] Letter from the Uber Companies' representative to the OAIC dated 24 January 2020 p 4, 8.

(**S3**), which enables businesses to store large quantities of data in a collection of cloud-based 'buckets' (**S3 buckets**). The Attackers obtained access to a private UTI repository on GitHub.[3] They appeared to have obtained GitHub credentials for some UTI employees from a different data breach, which was unrelated to UTI.[4]

7. The Attackers identified an active Amazon Web Services (**AWS**) credential in one of UTI's GitHub repositories. The Attackers used this credential to obtain programmatic access and download the contents of 16 files from the AWS S3. Some of the files contained archived driver and rider data stored by UTI in the AWS S3.[5] Those files had not been encrypted.[6] They were backup files that had been created outside UTI's usual processes, in connection with migrating UTI's data to a new system.[7]

8. The accessed and downloaded files related to approximately 57 million individuals worldwide. Approximately 1.2 million Australian accounts were affected (the **Affected Australian users**). Of these, approximately 960,000 of those accounts were used only as rider accounts and the remaining approximately 240,000 accounts were driver accounts (or both driver and rider accounts).[8]

9. In October 2017 (approximately 11 months after the Data Breach), UTI's external counsel engaged a forensic IT consultant firm, Mandiant, to conduct an analysis of the data in the files that were downloaded by the Attackers.[9] Mandiant's reports, provided to UTI on 10 January 2018 and 18 October 2018 (the **Mandiant Reports**), identified that the following types of personal information were accessed and downloaded by the Attackers:[10]

    a. names, email addresses and mobile phone numbers of users of the Uber app (both riders and drivers), administrative information about users' accounts and UTI's internally assigned unique identifiers for users

    b. driver licence numbers for some drivers (applicants and active drivers). These numbers were able to be linked to specific drivers through the driver's internally assigned unique identifier. UTI identified 23 individuals with a connection to Australia who may have had their driver licence numbers exposed (though only 15 of those individuals had both an Australian country code, as determined by UTI,[11] and Australian driving records)

---

[3] GitHub is a third-party software development platform that was used by software engineers at UTI to store code for collaboration and development.
[4] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 5.
[5] S3 enables the storage of large quantities of data in the cloud.
[6] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 17; letter from the Uber Companies' representative to the OAIC dated 21 January 2019 p 16.
[7] Letter from the Uber Companies' representative to the OAIC dated 21 January 2019 p 16.
[8] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 3.
[9] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 3.
[10] I note that not all types of information were disclosed in relation to each individual who was impacted by the Data Breach.
[11] Country codes are assigned to each of the users of the Uber app. A country code may not reflect where the relevant user lives. For example, a country code may be assigned from the location where the user first registers to use the Uber app, the country code of the phone number of the mobile device associated with the user's account or the location of the user's

c. one-time locational information, such as the latitude and longitude corresponding to where a user first registered to use the Uber app

d. processing information needed to create receipts, such as cost and date of a trip but not trip location history

e. short driver-related notes

f. high level summaries of rides performed by drivers, including how much drivers were paid over a week, high level summaries of trips and type of ride

g. salted and hashed versions of then-current user passwords and of previous passwords[12] and user tokens.

10. The Mandiant Report found no evidence that trip history, credit card numbers, bank account numbers, dates of birth or government related identification numbers were downloaded.

11. UTI became aware of the unauthorised access and downloading through an anonymous email from one of the Attackers on 14 November 2016. The anonymous individual claimed to have been able to access certain Uber data. The individual also demanded payment from UTI.[13]

12. By 15 November 2016, using information provided by the Attackers, UTI identified the cause of the Data Breach.[14]

13. In response to the Attackers' communications, UTI submits that after the Data Breach, it:

a. rotated the compromised access key[15]

b. began requiring two-factor authentication for all of its private GitHub repositories on or around 15 November 2016[16]

c. paid US$100,000 to the Attackers under a 'bug bounty' program in December 2016. This programme, established in 2014, invites outside information security experts to search for vulnerabilities in Uber's systems and disclose the method of compromise, in exchange for a payment[17]

---

first use of the Uber app. See letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 3.

[12] That is, essentially, non-plain text versions of passwords.

[13] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 4.

[14] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 5.

[15] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 9.

[16] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 7.

[17] Email correspondence between UTI and the Attackers provided with the letter from the Uber Companies' representative to the OAIC dated 21 December 2018. See also https://hackerone.com/uber

d. obtained written assurances in January 2017 from the Attackers that the downloaded data had been destroyed and that they would not disseminate the data.[18]

14. UTI has found no evidence of further access to, or downloading of, the personal information stored by UTI in AWS S3 by the Attackers after 15 November 2016.[19]

15. UBV was notified by UTI of the Data Breach on 4 November 2017, following discussion of a 2016 incident on 25 October 2017.[20]

16. UTI publicly announced the Data Breach on 21 November 2017. From 21 November 2017, the Uber Companies contacted drivers with driver's licence numbers included in the downloaded files, including the 23 drivers with an Australian connection. UTI did not separately contact any individuals who had been impacted by the Data Breach who used the Uber app solely as riders.[21]

17. At the time of the Data Breach, UTI enabled users of the Uber app and/or website who were located in Australia (**Australian users**) to provide feedback and raise concerns and ask questions in the Uber app or on the Uber website. In addition, Australian drivers were able to contact a customer support centre phone line. UTI did not keep separate records of complaints received in relation to the Data Breach, but based on a review of its Uber app, website, phone and social media records, was advised that only one complaint was received from an Affected Australian user.[22]

18. UTI tagged the accounts that had been compromised in the Data Breach for additional fraud protection.[23]

19. UTI submits that it has implemented a number of additional security measures since the Data Breach, including:

    a. implementing multi factor authentication for nearly all service accounts that had programmatic access to UTI's AWS S3 repository[24]

    b. implementing multi-factor authentication for access to UTI's private repositories in GitHub[25]

    c. migrating all remaining source code off GitHub onto internal code storage (with some limited exceptions)[26]

    d. revising training provided to UTI engineers to reference the Data Breach as an example of why it is important not to copy secrets, including AWS keys, into UTI source code[27]

---

[18] Email correspondence between UTI and the Attackers provided with the letter from the Uber Companies' representative to the OAIC dated 21 December 2018.
[19] As determined by Mandiant, see letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 5.
[20] Letter from the Uber Companies' representative to the OAIC dated 29 January 2021 p 8.
[21] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 4.
[22] Letter from the Uber Companies' representative to the OAIC dated 21 January 2019 p 3.
[23] Letter from the Uber Companies' representative to the OAIC dated 21 January 2019 p 3.
[24] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 8.
[25] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 7.
[26] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 7.
[27] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 10.

e. implementing written security guides for the security measures that it requires for using AWS, including AWS S3[28]

f. [redacted][29]

g. adopted a revised incident response approach [redacted][30]

h. modifying UTI's bug bounty program requirements, to emphasise that it is intended only for good faith reports of suspected vulnerabilities and not extortion attempts, and provide specific instructions on what researchers should do if they come into contact with user data while researching vulnerabilities.[31]

20. The Uber Companies also submit that since the Data Breach, they have:

a. completed an independent assessment of its Information Security Program, and appointed a senior executive to oversee the security program [32]

b. obtained ISO 27001 certification of its information systems that process data related to its core rides business.[33]

Investigation

21. On 18 December 2017, the OAIC notified UTI's representatives that the then Privacy Commissioner, had commenced an investigation under s 40(2) of the Privacy Act in relation to the unauthorised access and download, in late 2016, of archived driver and rider information stored by UTI in an Amazon Web Services account. That correspondence noted that the OAIC was considering whether UTI had complied with APP 11.

22. On 18 December 2019, the OAIC notified the Uber Companies' representatives, that, under s 40(2) of the Privacy Act, I would also be examining the conduct of UBV and that I was considering whether the Uber Companies had complied with APP 1.2, APP 11.1 and APP 11.2.

23. On 14 December 2020, the OAIC notified UBV that I would also be investigating its compliance with APP 8 when it provided personal information of Affected Australian users to UTI.

24. To ensure that the Uber Companies had the opportunity to explain their positions, the OAIC issued the requests for information, and took into account the Uber Companies' responses, listed at **Attachment A**.

Material considered

25. In making this determination, I have had regard to:

---

[28] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 10.
[29] Letter from the Uber Companies' representative to the OAIC dated 21 January 2019 p 13.
[30] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 9.
[31] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 10.
[32] Letter from the Uber Companies' representative to the OAIC dated 27 April 2021 p 2.
[33] Letter from the Uber Companies' representative to the OAIC dated 27 April 2021 p 2.

a. information and submissions provided by the Uber Companies as referred to in **Attachment A**

b. information obtained from online sources by officers of the OAIC

c. the *Australian Privacy Principles Guidelines*, issued by the Australian Information Commissioner, March 2014 (**APP Guidelines**).[34]

The Law

26. All references to provisions in this determination are to those contained in the Privacy Act unless indicated otherwise.

27. The law relevant to this investigation is set out at **Attachment B**.

Determination Power

28. Section 52(1A) of the Privacy Act provides that, after investigating an act or practice of a person or an entity under s 40(2) of the Act, I may make a determination that includes one or more of the following:

a. a declaration that the act or practice is an interference with the privacy of an individual and must not be repeated or continued

b. a declaration that the person or entity must take specified steps within a specified period to ensure that the act or practice is not repeated or continued

c. a declaration that the person or entity must perform any reasonable act or course of conduct to redress any loss or damage suffered by one or more of those individuals

d. a declaration that one or more of those individuals are entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice

e. a declaration that it would be inappropriate for any further action to be taken in the matter.

Australian Privacy Principles

29. The APPs, which are set out in Schedule 1 to the Privacy Act, regulate the collection, use, disclosure, and security of personal information held by Australian government agencies and certain private sector organisations (**APP entities**).

30. The OAIC has published *Australian Privacy Principles Guidelines*, July 2014 (**APP Guidelines**).[35] While not legally binding, the APP Guidelines outline the mandatory requirements of the APPs, how the OAIC interprets the APPs, and matters that I may take into account when exercising functions and powers under the Act.

[34] July 2019 version.

31. Under s 13(1) of the Privacy Act, an act or practice of an APP entity is an interference with the privacy of an individual if the act or practice breaches an APP in relation to personal information about the individual.

32. Section 15 prohibits an APP entity from doing an act, or engaging in a practice, that breaches an APP.

Jurisdiction

Organisation

33. Subsection 6(1) defines an APP entity as an 'agency or organisation'. An 'organisation' is further defined in s 6C to include a body corporate that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.

34. UTI is a body corporate incorporated in the United States and is the parent company of UBV. UBV is a body corporate incorporated in the Netherlands. There is no evidence before me to show that UTI or UBV are 'small business operators' for the purposes of the Act.

35. I am satisfied that the Uber Companies meet the definition of 'organisation' in s 6C.

Extraterritorial operation of the Privacy Act

Law

36. The Privacy Act extends to an act done, or practice engaged in, outside Australia and the external Territories by an organisation, or small business operator, that has an Australian link: s 5B(1A).

37. Subsection 5B(3) provides that an organisation has an 'Australian link' if all of the following apply:

    a. the organisation is not described in subsection (2): s 5B(3)(a)

    b. the organisation carries on business in Australia or an external Territory: s 5B(3)(b)

    c. the personal information was collected or held by the organisation in Australia or an external Territory, either before or at the time of the act or practice: s 5B(3)(c).

38. As UTI is a body corporate incorporated in the United States and UBV is a body corporate incorporated in the Netherlands, the Uber Companies do not fall within s 5B(2). For each Uber Company to have an "Australian link", all of the conditions in ss 5B(3)(b) and (c) of the Privacy Act must apply.

Carrying on business in Australia

39. The phrase 'carries on business in Australia' in s 5B(3)(b) is not defined in the Privacy Act. The Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (the **Explanatory Memorandum**), which introduced the concept of an 'Australian link' in s 5B(3), explains that 'entities … who have an online presence (but no

physical presence in Australia) and collect personal information from people who are physically in Australia, carry on a 'business in Australia or an external Territory''.[36]

40. The phrase also arises in other areas of law, including corporations and consumer law. Guidance may be drawn from judicial consideration of the phrase in those contexts.[37]

41. The relevant principles with respect to the phrase 'carries on business in Australia' within the meaning of s 5B(3)(b) of the Privacy Act were described by Thawley J in *Australian Information Commissioner v Facebook Inc (No 2)* (***Facebook No 2***).[38] In particular:

    a. In *Valve Corporation v Australian Competition and Consumer Commission*,[39] the Full Federal Court did not accept that there is an 'inflexible rule or condition' that carrying on business in Australia requires 'some physical activity in Australia through human instrumentalities.' Rather, the Court emphasised that 'the territorial concept of carrying on business involves acts within the relevant territory that amount to, or are ancillary to, transactions that make up or support the business.'[40]

    b. In *Tiger Yacht Management Ltd v Morris,*[41] the Full Federal Court considered that the expression 'carrying on business' may have different meanings in different contexts, though when it is used to ensure a jurisdictional nexus, its meaning will be informed by the requirement to ensure there is a sufficient connection with the country asserting jurisdiction. It requires resort to the ordinary meaning of the phrase and invites a factual inquiry. The Court further noted that:

        i. In order to be carrying on business, the activities must form a commercial enterprise.[42]

        ii. The words 'carrying on' imply the repetition of acts and activities which suggest a permanent character rather than participating in a single transaction or a number of isolated transactions.[43]

        iii. A company may be carrying on business in Australia even though it does not have an identifiable place of business within Australia.[44]

    c. Thawley J stated that 'the present context is the application of Australian privacy laws to foreign entities ... the present statutory context includes the object of protecting the privacy of individuals and the responsible handling of personal information collected from individuals in Australia.' Section 2A of the Privacy Act identifies the following as express statutory objects:

        i. to promote the protection of the privacy of individuals (s 2A(a))

---

[36] Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, Schedule 4, Item 6.
[37] APP guidelines [B.13].
[38] [2020] FCA 1307 (***Facebook No 2***) at [40]-[46].
[39] (2017) 258 FCR 190 (***Valve Corporation***).
[40] *Valve Corporation* at [149], after considering the analysis in *Campbell v Gebo Investments (Labuan) Ltd* (2005) 190 FLR 209.
[41] Tiger Yacht Management Ltd v Morris [2019] FCFCA 8 at [50] (**Tiger Yacht**).
[42] *Tiger Yacht* at [51].
[43] *Tiger Yacht* at [52].
[44] *Tiger Yacht* at [53].

ii. to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities (s 2A(b); and

iii. to promote responsible and transparent handling of personal information by entities (s 2A(d))

iv. to facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected (s 2A(f)

v. to provide a means for individuals to complain about an alleged interference with their privacy (s 2A(g)

vi. to implement Australia's international obligation in relation to privacy (s 2A(h).[45]

Collecting personal information in Australia or an external Territory

42. Section 6 of the Privacy Act provides that an APP entity collects personal information 'only if the entity collects the personal information for inclusion in a record or generally available publication'.

43. The concept of 'collection' applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means, including from, relevantly:

a. individuals

b. other entities

c. information associated with web browsing, such as personal information collected by cookies.[46]

44. The definition of 'record' in s 6(1) includes a document or an electronic or other device.

45. The Explanatory Memorandum states in respect of collecting personal information 'in Australia':

> The collection of personal information 'in Australia' under paragraph 5B(3)(c) includes the collection of personal information from an individual who is physically within the borders of Australia or an external territory, by an overseas entity.
>
> For example, a collection is taken to have occurred 'in Australia' where an individual is physically located in Australia or an external Territory, and information is collected from that individual via a website, and the website is hosted outside of Australia, and owned by a foreign company that is based outside of Australia and that is not incorporated in Australia.

46. '[T]he personal information' referred to in s 5B(3)(c) concerns the personal information that is the subject of the determination.[47]

---

[45] *Facebook No 2* at [42].

[46] https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/#collects

[47] *Facebook No 2* at [164] and [172].

Holding personal information in Australia or an external Territory

47. There is no evidence before me to indicate that the Uber Companies *held* personal information *in Australia* before or at the time of the act or practice. Accordingly, I have not considered whether s 5b(3)(c) is satisfied on that ground.

Consideration

Uber Companies' submissions on jurisdiction

48. The Uber Companies did not dispute that at the time of the Data Breach, UBV was within the jurisdiction of the Privacy Act.[48]

49. UTI submitted that at the time of the Data Breach it was not an APP entity for the purposes of the Privacy Act and, accordingly, that I do not have jurisdiction to find a breach or make a determination.[49]

50. In particular, UTI disputed that it 'carrie[d] on business in Australia'. UTI stated that at that time, it:

    a. did not have any direct contractual or other relationship with riders or drivers in Australia

    b. was not involved in facilitating the transaction between Australian riders and driver partners

    c. was not involved in collecting or remitting payments in respect of Australian riders or drivers.[50]

51. UTI submitted that as a consequence, it was not involved in, or conducting any form of, commercial enterprise systematically and with a view to profit in Australia at the time of the Data Breach.[51]

52. As discussed in paragraph 5 above, under the 2016 DPA, UTI submitted that it was contractually required to process the information in accordance with UBV's instructions.[52] The 2016 DPA includes a non-exhaustive list of data processing activities that UTI could provide on behalf of UBV. According to UTI, these activities were undertaken by UTI 'on a global basis on behalf of UBV, and so only related to Australian users' personal information in that they related to all users' personal information.'[53] UTI submits that none of these activities occurred in Australia.[54]

53. UTI also submitted that, at the time of the Data Breach, it was only authorised to collect, store and use personal information of Australian users on UBV's instructions. It claims that it received such information only after it was submitted to UBV through the Uber app

---

[48] For example, the letter from the Uber Companies' representative to the OAIC dated 3 July 2020 p 6-7 disputes that UTI has an Australian link but does not dispute that UBV has an Australian link.
[49] Letter from the Uber Companies' representative to the OAIC dated 3 July 2020, p 6-7.
[50] Letter from the Uber Companies' representative to the OAIC dated 3 July 2020, p 6-7.
[51] Letter from the Uber Companies' representative to the OAIC dated 3 July 2020 p 7.
[52] Letter from the Uber Companies' representative to the OAIC dated 24 January 2020 p 4, 8.
[53] Letter from the Uber Companies' representative to the OAIC dated 18 January 2021 p 5.
[54] Letter from the Uber Companies' representative to the OAIC dated 18 January 2021 p 8.

or website. On this basis, UTI asserted that it did not collect or hold this personal information in Australia at that time.[55]

Did UTI carry on business in Australia at the time of the Data Breach?

54. I accept that UTI did not have a physical presence in Australia and was headquartered in the United States at the time of the Data Breach.

55. I also accept that at the time of the Data Breach, UTI did not have a direct contractual relationship with Australian riders and drivers and was not involved in collecting or remitting payments in respect of Australian riders or drivers.

56. Notwithstanding this, the following activities which were undertaken by UTI on a global basis as data processor for UBV under the 2016 DPA, indicate that UTI carried on business in Australia at that time:

    a. UTI installed and managed authentication, security and localisation cookies and similar technologies on Australian users' devices for the purpose of enabling users to log-in and remain logged-in to the Uber app and to enable security features on the Uber app.[56]

    b. Where a new service, product or safety feature was developed in the United States (such as by the product engineering team), UTI would roll this out internationally, including to Australia.[57]

    c. UTI carried out troubleshooting of general bugs or issues with the Uber app in the United States, for example by its product engineering teams, and it then rolled out these solutions internationally, including to Australia.[58]

    d. UTI used centralised and global tools to enable UBV to carry out ad campaigns for Australian users, including by providing advertisements developed by local Uber entities for display to Australian users to third party sites such as Google and Facebook.[59] This included UTI centrally managing, on a global basis, the Uber group's global pixel.[60]

57. For the purposes of considering whether the acts listed in paragraph 56 were done in Australia, it is not determinative that some or all of these activities may have been instituted or controlled remotely (such as from the US), or that they were done on behalf of UBV. The fact that an activity which occurs in Australia might be controlled or facilitated by actions of the entity taken remotely and without the need for employees in Australia, does not necessarily mean that no relevant activity is performed by the entity in Australia.[61]

---

[55] Letter from the Uber Companies' representative to the OAIC dated 3 July 2020 p 7.
[56] Letter from the Uber Companies' representative to the OAIC dated 18 January 2021 p 9.
[57] Letter from the Uber Companies' representative to the OAIC dated 18 January 2021 p 5.
[58] Letter from the Uber Companies' representative to the OAIC dated 18 January 2021 p 6.
[59] Letter from the Uber Companies' representative to the OAIC dated 18 January 2021 p 10.
[60] Letter from the Uber Companies' representative to the OAIC dated 18 January 2021 p 5, 12.
[61] *Facebook No 2* at [148].

58. It is also not determinative that the acts and practices listed in paragraph 56 were performed pursuant to a contract with UBV, or whether they facilitated UBV's provision of services to Australian users.

59. In my view, the available information establishes that at the time of the Data Breach, UTI was involved in several activities in Australia that amounted to, or were ancillary to, transactions that made up or supported UTI's business of providing data processing services to UBV under the 2016 DPA. This includes the activities set out at paragraph 56 and evidence that UTI collected riders and drivers' personal information in Australia at the time of the Data Breach (see paragraphs 61 – 65). When considered together, they provide clear evidence that at that time, UTI was engaging in activity in Australia, which was in the nature of a commercial enterprise, and which had a repetitive and permanent character.

60. For these reasons, I am satisfied that UTI carried on business in Australia at the time of the Data Breach.

Did UTI collect the personal information in Australia before or at the time of the Data Breach?

61. As stated in paragraph 46, for s 5b(3)(c) to be satisfied, 'the personal information' collected (or held) in Australia is the personal information that is the subject of the determination.[62]

62. The Uber Companies made the following submissions as to how UTI obtained Australian users' personal information for processing under the 2016 DPA.

    a. Collection of Australian users' personal information 'occurred when Australian users submitted personal information to UBV through, and in connection with, their use of the Uber app and Uber website. On collection, Australian users' personal information was transferred to internal servers of UTI, located in the United States ('UTI Servers').[63]

    b. At the time of the 2016 data incident, UTI was only authorised to collect, store and use personal information of Australian users on the instructions of UBV, and received such information only after it was submitted to UBV through the Uber app or website. Such personal information was therefore not, at the time, collected or held by UTI in Australia.[64]

    c. 'When an Australian user submits his or her personal information, it is transferred directly to servers controlled by UTI on behalf of UBV'.[65] The Uber Companies further explained this process as follows:

> During the period between 13 October to 14 November 2016 … [s]uch collection occurred when Australian Users submitted personal information to UBV through, and in connection with, their use of the Uber App and Uber website. **As a matter of practice, we note that such collection by UBV occurred indirectly via these platforms. That is, on collection, Australian Users' personal information was**

[62] *Facebook No 2* at [164] and [172].
[63] Letter from the Uber Companies' representative to the OAIC dated 18 January 2021 p 4.
[64] Letter from the Uber Companies' representatives to the OAIC dated 3 July 2020 p 7.
[65] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 2.

> **transferred directly to servers owned by UTI, located in the United States** …[66] [emphasis added]
>
> When Australian Users submitted personal information in the Uber App or Uber website (as transmitted through their personal device), **the information was collected by UBV but was, in practice, transferred directly into, and stored in, databases running on the UTI Servers**, [redacted].[67] [emphasis added]

63. I have considered the above submissions. In my view, the fact that UTI might have collected Australians' personal information pursuant to a contract with UBV is not determinative. As discussed in paragraph 71, it is possible for more than one APP entity to simultaneously collect the same personal information under the Privacy Act.

64. I note that the explanation referred to in paragraph 62(c) describes, with some specificity, how the collection of Australians' personal information occurred 'as a matter of practice'. I accept this explanation that in practice, Australians' data was directly transferred to servers controlled and owned by UTI in the US.

65. On that basis, I am satisfied that UTI collected personal information of Affected Australian Users, when they submitted their personal information via the Uber app or website in Australia. I am therefore satisfied that UTI collected 'the personal information' in Australia before or at the time of the Data Breach.

Did UBV carry on business in Australia at the time of the Data Breach?

66. Although UBV is incorporated in the Netherlands and there is no evidence before me that suggests it had a physical presence in Australia at the time of the Data Breach, this is not determinative.

67. The following factors indicate that UBV carried on business in Australia at the time of the Data Breach:

    a. UBV was, for regions outside of the United States, both the data controller and licensor of the Uber app, and entered into direct contractual arrangements with both Australian riders and drivers.[68]

    b. UBV was the entity with contractual responsibility for the collection of personal information of Australian users at the time of the Data Breach.[69]

    c. As I conclude in paragraphs 69 to 72 below, UBV collected personal information in Australia.

68. For these reasons, I am satisfied that UBV carried on business in Australia at the time of the Data Breach.

---

[66] Letter from the Uber Companies' representative to the OAIC dated 24 January 2020 p 3.
[67] Letter from the Uber Companies' representative to the OAIC dated 24 January 2020 p 7.
[68] Letter from the Uber Companies' representative to the OAIC dated 24 January 2020 p 3.
[69] Letter from the Uber Companies' representative to the OAIC dated 24 January 2020 p 3.

Did UBV collect personal information in Australia before or at the time of the Data Breach?

69. UBV submitted that it was the entity with contractual responsibility for the collection of personal information of Australian users at the time of the Data Breach. Such collection occurred when Australian users submitted personal information to UBV through, and in connection with, their use of the Uber app and Uber website.[70]

70. The Uber Companies submitted that, under the 2016 DPA, UTI was only authorised to collect, store and use personal information of Australian users on the instructions of UBV.[71]

71. I consider that it is possible for more than one APP entity to simultaneously collect the same personal information under the Privacy Act. In this case, I have found that UTI collected personal information of Australian users, because when Australian users submitted personal information to UBV through, and in connection with, their use of the Uber app and Uber website, it was transferred directly to UTI's servers. I also consider that UBV collected that same information, because UTI was required to hold and use Australian Users' personal information in accordance with UBV's instructions only. This indicates that UBV had control of the record in which the personal information was held.

72. On that basis, I am satisfied that UBV collected personal information in Australia before or at the time of the Data Breach.

Finding – jurisdiction

73. Based on the information before me, I am satisfied that the Uber Companies were both organisations with an 'Australian link', at the time of the Data Breach.

74. As such, under s 5B(1A), the Privacy Act extends to the acts done, and practices engaged in, by the Uber Companies during the period the Data Breach occurred.

APPs and breach

75. As mentioned above, section 15 of the Privacy Act provides that an APP entity must not do an act, or engage in a practice, that breaches an APP. The APPs, which are contained in Schedule 1 of the Privacy Act, regulate the collection, use, disclosure and security of personal information held by APP entities.

76. Having formed the view that the Privacy Act applies to the Uber Companies in respect of the Data Breach for the reasons set out above, it is then necessary to consider the following APPs relevant to my investigation of the Data Breach:

    a. APP 1.2

    b. APP 11.1

    c. APP 11.2.

77. These are set out in full in **Attachment B**.

---

[70] Letter from the Uber Companies' representative to the OAIC dated 24 January 2020 p 3.
[71] Letter from the Uber Companies' representative to the OAIC dated 3 July 2020 p 7.

78. I have decided not to make a finding in relation to APP 8. For the reasons set at paragraphs 86 to 88, I am satisfied that UBV did not 'disclose' Australians' personal information to UTI, but continued to 'hold' that information under the 2016 DPA.

APP 11.1

Law

79. APP 11.1 in the Privacy Act requires APP entities to take such steps as are reasonable in the circumstances to protect personal information held by the entity from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

80. Unauthorised access for the purposes of APP 11.1 occurs when personal information that an entity holds is accessed by someone who is not permitted to do so. This extends to unauthorised access by an external third party, including by hacking.[72]

81. The level of protection required varies depending on the circumstances, including the nature and sensitivity of the information held.

82. In assessing the 'circumstances' referred to in APP 11.1, it is relevant to consider:

    a. the nature of the APP entity including an APP entity's size, resources, the complexity of its operations and its business model

    b. the amount and sensitivity of the personal information held

    c. potential risk of harm to individuals should the security of the information in question be compromised

    d. the practical implications of implementing the security measure, including time and cost involved

    e. whether a security measure is in itself privacy invasive.[73]

83. APP entities are required to consider compliance with APP 11.1 at all stages of the information lifecycle. The reasonable steps should include, where relevant, taking steps and implementing strategies in relation to the following:

    a. governance, culture and training

    b. internal practices, procedures and systems

    c. ICT security

    d. access security

    e. data breaches.[74]

84. APP 11.1 applies to the personal information that an APP entity 'holds'.

---

[72] APP Guidelines [11.18].
[73] APP Guidelines [11.7].
[74] APP Guidelines [11.8].

85. An entity 'holds' personal information 'if the entity has possession or control of a record that contains the personal information.'[75] This means the term 'holds' applies to personal information that an APP entity has the right or power to deal with, even if that APP entity does not physically possess the personal information.[76]

Consideration

Holds

86. At the time of the Data Breach, UTI controlled the backup file stored in AWS S3, containing Australians' personal information.

87. At that time, UBV also had a right to deal with that personal information, through its contractual rights to instruct UTI in the 2016 DPA.[77]

88. For these reasons, I am satisfied that both Uber Companies 'held' the personal information of the Affected Australian users in AWS S3 at the time of the Data Breach. Consequently, both had responsibilities to comply with APP 11.1.

Steps taken by the Uber Companies to protect Australians' personal information

89. UTI submitted that the steps it took to protect the personal information it held from unauthorised access by third parties, which were in place at the time of the Data Breach, included:

    a. In April 2015, UTI had launched a proprietary secrets management tool to enable UTI's employees to securely manage and restrict distribution of AWS service credentials, encryption keys and other sensitive information.[78]

    b. At the time of the data breach, UTI 'encouraged' engineers to rotate AWS access keys used for programmatic access to AWS on a regular basis.[79]

    c. UTI had a range of processes in place to back up its databases, as well as to encrypt and delete back up files.[80]

    d. UTI had in place multi-factor authentication for individual user account access to the AWS S3 repository. For programmatic access, UTI used access keys, comprising an 'access key ID' and 'secret access key'.[81]

    e. All UTI employees worldwide were given privacy and data security training that substantively covered the APPs. This training was required to be undertaken as part of an employee's onboarding process and was not repeated.[82]

---

[75] s 6(1) of the Privacy Act.
[76] APP Guidelines [B.79] - [B.81].
[77] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 2.
[78] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 9 and 11.
[79] Letter from the Uber Companies' representative to the OAIC dated 21 January 2019 p 15.
[80] Letter from the Uber Companies' representative to the OAIC dated 21 January 2019 p 16.
[81] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 12-13.
[82] Letter from the Uber Companies' representative to the OAIC dated 21 January 2019 p 6.

f. In addition to the initial training referred to in subparagraph (e) above, UTI provided new employees with security training within one month of commencing employment. This was repeated annually. UTI has not advised that this training specifically addressed the requirements of the Privacy Act.[83]

90. UBV submitted that, as expressly contemplated in the 2016 DPA, it relied on UTI's skill and knowledge to assess and implement the technical and organisational measures appropriate to protect Australian users' personal information against unauthorised access and disclosure.[84]

91. UBV also submitted that it may have given ad hoc instructions or directions to UTI in respect of the 2016 DPA, such as in relation to specific jurisdictional requirements in relation to the information security policy established by UTI. However, UBV was unable to provide evidence about any particular instructions or directions it gave to UTI, citing the passage of time since the Data Breach and the approximate 6-week period given to respond to my office's request for information.[85]

Did the Uber Companies take reasonable steps in the circumstances?

92. It has previously been found that 'reasonable steps' must include both documented policies and procedures, and behaviours consistent with those policies and procedures.[86] Employee behaviour can be reinforced through training staff and management in security awareness, practices and procedures.

93. I acknowledge that the Uber Companies took the steps outlined in paragraph 89 above. I also accept that the Uber Companies had contractual arrangements in place that required UTI to implement measures to prevent and safeguard Australians' personal information from unauthorised processing.

94. However, in my view, there were deficiencies in the Uber Companies' security processes and practices that ought to have been addressed by taking at least the following steps:

a. Multi-factor authentication should have been implemented for UTI's private repositories in GitHub, particularly given UTI did not have a written policy in place that prevented employees from hardcoding access keys in plain text in code in GitHub.

b. Multi-factor authentication should have been implemented for programmatic access to UTI's AWS S3 repository. This would have ensured that the Attackers would not have been able to access the compromised files unless they had also been able to obtain access to UTI's network.[87]

c. UTI has been unable to explain why the AWS access credential obtained by the Attackers had not been rotated.[88] At the time of the Data Breach, there was no

[83] Letter from the Uber Companies' representative to the OAIC dated 21 January 2019 p 6-7.
[84] Letter from the Uber Companies' representative to the OAIC dated 29 January 2021 p 6.
[85] Letter from the Uber Companies' representative to the OAIC dated 29 January 2021 p 4.
[86] Telstra Corporation Limited: Own motion investigation report dated 1 June 2012, available at https://www.oaic.gov.au/privacy/privacy-decisions/investigation-reports/telstra-corporation-limited-own-motion-investigation-report-2012/
[87] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 8.
[88] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 16.

mandatory requirement for the rotation of AWS access keys. In my view, written policies should have been implemented that required UTI employees:

i. not to make functional access keys available in plain text in code, in GitHub or elsewhere

ii. to rotate access keys on a regular basis using UTI's secrets management tool.

d. The backup files that were the subject of the Data Breach were not created as part of UTI's ordinary processes. Thus, UTI's usual backup, encryption and deletion processes were not applied to these files.[89] UTI has not advised the OAIC of any policies it had in place to deal with the protection or deletion of backup files containing personal information that are created outside of UTI's ordinary processes. In my view, UTI should have adopted and implemented a policy to encrypt backup files containing personal information that were created in this way for a particular purpose like migrating to a new system.

e. The policies referred to in subparagraphs (c) and (d) should have been operationalised, in particular, by requiring regular training of relevant UTI employees in relation to those policies and implementing processes to monitor compliance with those policies.

95. In my view, it is not a reasonable step for UBV to rely almost entirely on the 2016 DPA contractual arrangements and the skill and expertise of UTI, in the following circumstances:

a. UBV entrusted UTI to process a substantial number of Australians' personal information, which included many different kinds of personal information (including contact details, transaction information and geolocation information).[90]

b. There was a foreseeable risk of adverse consequences to individuals if this information was subject to unauthorised access.

c. There were multiple deficiencies in UTI's information handling practices, as outlined in paragraph 94.

96. Taking into account the matters outlined above, I consider that the Uber Companies did not take reasonable steps to protect Affected Australian users' personal information from unauthorised access.

Finding – APP 11.1

97. It is my view that, at the time of the Data Breach, the Uber Companies interfered with the privacy of the Affected Australian users by failing to take reasonable steps in the circumstances to protect their personal information from unauthorised access, in breach of APP 11.1.

[89] Letter from the Uber Companies' representative to the OAIC dated 21 January 2019 p 16.
[90] 2016 DPA, [redacted].

APP 11.2

Law

98. APP 11.2 in the Privacy Act requires an APP entity that no longer needs personal information it holds for any purpose for which it may be used or disclosed by the entity under the APPs, to take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified (subject to certain exceptions).

99. Whether reasonable steps have been taken for the purposes of compliance with APP 11.2 will depend upon circumstances including:

a. the nature of the APP entity including an APP entity's size, resources, the complexity of its operations and its business model

b. the amount and sensitivity of the personal information held

c. the potential risk of harm to individuals should their personal information not be destroyed or de-identified

d. the entity's information handling practices, such as how it collects, uses and stores personal information, including whether personal information handling practices are outsourced to third parties

e. the practical implications of implementing measures to destroy or de-identify personal information (whether this makes it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances)[91]

100. In order to ensure compliance with the requirement to take reasonable steps to destroy or delete information under APP 11.2, an APP entity should have practices, procedures and systems in place to identify personal information that needs to be destroyed or de- identified.[92]

101. APP 11.2 applies to personal information that an APP entity 'holds' (see paragraph 85). Where an APP entity is required to destroy or de-identify personal information, it must take reasonable steps to destroy or de-identify all copies it holds of that personal information, including copies that have been archived or are held as back- ups.[93]

Consideration

Holds

102. For the reasons set out in paragraphs 86 to 88 above, I am satisfied that each of the Uber Companies held the personal information of Affected Australian users at the time of the Data Breach.

[91] APP Guidelines [11.33].
[92] APP Guidelines [11.30].
[93] APP Guidelines [11.29].

Was personal information no longer needed for any purpose for which it may be used or disclosed under the APPs?

103. The Affected Australian users' personal information that was accessed by the Attackers was contained in backup files created in connection with an internal process that was completed in approximately 2015. Once that internal process was complete, the backup files were no longer needed for any purpose.

104. Accordingly, I consider that the Uber Companies no longer needed that personal information for any purpose for which the information may have been used or disclosed under the APPs.

Steps taken by the Uber Companies to destroy or de-identify personal information

105. UTI submitted that, at the time of the Data Breach, it took the following steps to comply with APP 11.2:

a. UTI had a data deletion policy in place that set out retention and deletion schedules for different types of personal information.[94]

b. Prior to November 2016, user data was retained for the lifetime of a user's account. Upon receipt of a request for account deletion, Uber deleted or de-identified personal information associated with the account, unless retention was required for legal purposes (e.g., such as tax requirements or minimum retention obligations under transportation regulations) or legitimate business purposes (such as investigations, dispute resolution, safety and security, and fraud prevention and detection).[95]

c. In the ordinary course of business, UTI automatically backed up its databases and automatically deleted backup files after a specified period.[96]

d. From 2015, UTI also worked to delete or encrypt old database backups.[97]

106. However, the files accessed by the Attackers were not created as part of UTI's ordinary processes and fell outside the processes in subparagraph (c) above. According to UTI, it is difficult to clearly identify the origins and handling of these files, or why they were not deleted when no longer required, that is, after the internal process referred to in paragraph 103 was completed.[98]

107. UBV submitted that, as expressly contemplated in the 2016 DPA, it relied on UTI's skill and knowledge to assess and implement the technical and organisational measures appropriate to destroy or de-identify Australian riders and drivers' personal information when it was no longer needed. UBV also submitted that relevant policies were 'implemented on a day-to-day basis by UTI, with input from UBV or local entities as warranted and as required by domestic law.'[99]

---

[94] Letter from the Uber Companies' representative to the OAIC dated 21 January 2019 p 17.
[95] Letter from the Uber Companies' representative to the OAIC dated 21 January 2019 p 17.
[96] Letter from the Uber Companies' representative to the OAIC dated 21 January 2019 p 16.
[97] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 12.
[98] Letter from the Uber Companies' representative to the OAIC dated 21 January 2019 p 16-17.
[99] Letter from the Uber Companies' representative to the OAIC dated 29 January 2021 p 6.

Did the Uber Companies take reasonable steps in the circumstances?

108. There is no evidence that the Uber Companies implemented policies and procedures to deal with the destruction or de-identification of backup files containing personal information that were created manually outside of UTI's ordinary processes. In fact, the evidence indicates that the Uber Companies were unaware until after the Data Breach that the files that were the subject of the Data Breach were still stored on AWS S3. In my view, the matters raised in this paragraph indicate deficiencies in implementing reasonable steps as required by APP 11.2.

109. Having regard to the matters set out in paragraph 99, in my view the Uber Companies ought to have taken at least the following reasonable steps to destroy or de-identify the personal information the subject of the Data Breach:

a. adopt and implement a policy and procedure to identify whether manually created backup files containing personal information were needed for a permissible purpose under the APPs

b. adopt and implement a policy and procedures to ensure that, for any backup files created in the way these files were created, that were no longer needed for a purpose permitted under the APPs, reasonable steps were taken to delete or de-identify these files

c. operationalise the policies and procedures referred to in subparagraphs (a) and (b) above, in particular, by requiring regular and appropriate training of employees who may create backup files in this way containing personal information, and also implementing processes to monitor compliance with the policy and procedures.

110. In my view, it was not reasonable for UBV to rely almost entirely on the 2016 DPA contractual arrangements and the skill and expertise of UTI, in the following circumstances:

a. UBV entrusted UTI to process a substantial number of Australians' personal information, which included many different kinds of personal information (including contact details, transaction information and geolocation information).[100]

b. There was a foreseeable risk of adverse consequences to individuals if this information was subject to unauthorised access.

c. There were multiple deficiencies in UTI's information handling practices, as outlined in paragraph 109.

111. Taking into account the above matters, I consider that the Uber Companies did not take reasonable steps to destroy or de-identify personal information of Affected Australian users as required by APP 11.2.

Finding – APP 11.2

112. It is my view that, at the time of the Data Breach, the Uber Companies interfered with the privacy of the Affected Australian users by failing to take reasonable steps in the circumstances to destroy or de-identify their personal information, in breach of APP 11.2.

[100] 2016 DPA, [redacted].

APP 1.2

Law

113. APP 1.2 in the Privacy Act requires APP entities to take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

a. will ensure compliance with the APPs; and

b. will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the APPs.

114. APP 1.2 imposes a distinct and separate obligation on APP entities, as well as being a general statement of its obligation to comply with the other APPs. Its purpose is to require an entity to take proactive steps to establish and maintain internal practices, procedures and systems that ensure compliance with the APPs, having regard to the requirement to manage personal information in an open and transparent way.[101]

115. The APP Guidelines set out the following as examples of the practices, procedures and systems that an APP entity should consider implementing to comply with APP 1.2:

a. procedures for identifying and managing privacy risks at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction or de- identification

b. security systems for protecting personal information from misuse, interference and loss and from unauthorised access, modification or disclosure, such as IT systems, internal access controls and audit trails

c. procedures for identifying and responding to privacy breaches, handling access and correction requests and receiving and responding to complaints and inquiries

d. governance mechanisms to ensure compliance with the APPs (such as a designated privacy officer and regular reporting to the entity's governance body)

e. regular staff training and information bulletins on how the APPs apply to the entity, and its practices, procedures and systems developed under APP 1.2. [102]

116. The reasonable steps that an APP entity should take for the purposes of APP 1.2 will depend on circumstances that include:

a. the nature, including amount and sensitivity, of the personal information held

b. the possible adverse consequences for an individual if their personal information is not handled as required by the APPs

c. the nature of the APP entity, taking into consideration factors such as the APP entity's size, resources and business model

[101] APP Guidelines [1.5].
[102] APP Guidelines [1.7].

d. the practicability, including time and cost involved. This does not mean an APP entity will not be required to implement practices, procedures or systems because it would be inconvenient, time-consuming or involve costs. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all of the circumstances. [103]

117. At the time of the Data Breach, the Notifiable Data Breaches Scheme in Part IIIC of the Privacy Act was not in effect. However, APP 1.2 required regulated entities to implement practices, procedures and systems to manage data breaches. This included an obligation to put in place processes to assess whether affected individuals should be notified. Whether notification was a reasonable step under APP 1.2 depended on the particular circumstances, having regard to the factors set out in paragraph 116 above, including the nature of the personal information accessed in a data breach and the risk of adversity to affected individuals.

118. Since 22 February 2018, Part IIIC of the Privacy Act has expressly required organisations and government agencies covered by the Privacy Act to notify affected individuals and my office when a data breach is likely to result in serious harm to an individual whose personal information is involved.

Consideration

Steps taken by the Uber Companies

119. In its submissions, UTI described the physical, technological and organisational safeguards in place in relation to its personal information security systems at the time of the Data Breach. UTI also provided documents, including policies, procedures, technical documentation and training manuals, in support of its submissions.

120. In its submissions, UBV referenced certain policies and procedures provided to my office by UTI, and provided additional policies and procedures in relation to security and the Uber environment which it claims were reflective of Uber practices at the time of the Data Breach.[104]

121. In respect of policies and procedures that relate to identifying and responding to data breaches, UBV submitted that it reviewed certain Uber group data breach response policies that were owned by UTI, before they were implemented, to ensure compliance with local data handling and privacy requirements.[105]

122. UBV also submitted that it was not informed of the Data Breach until approximately 12 months after the Data Breach.[106] It is UBV's position that any additional steps or measures taken by UBV in relation to policies for the identification and response to data breaches would not have led to it learning of the incident when it occurred in 2016.'[107]

[103] APP Guidelines [1.6].
[104] Letter from the Uber Companies' representative to the OAIC dated 29 January 2021 p 4-6.
[105] Letter from the Uber Companies' representative to the OAIC dated 29 January 2021 p 4-5.
[106] Letter from the Uber Companies' representative to the OAIC dated 29 January 2021 p 8.
[107] Letter from the Uber Companies' representative to the OAIC dated 29 January 2021 p 5.

Did the Uber Companies take reasonable steps in the circumstances?

123. As stated at paragraph 115, the practices, procedures and systems that an APP entity should consider implementing to comply with APP 1.2 include procedures for identifying and responding to privacy breaches. Such procedures are important to prevent any ongoing unauthorised access to personal information, and to limit further access to unsecured personal information by unauthorised third parties. These are also an important component of the overarching obligation in APP 1.1 to manage personal information in an open and transparent way.

124. Uber publicly acknowledged that there were deficiencies in its response to the Data Breach.[108] UTI submitted that 'Uber terminated two of the individuals who led the response to the data incident … [redacted]. … Executives and management at Uber deeply regret that this incident occurred and that Uber did not publicly disclose it at the time.'[109]

125. I make the following observations about the Uber Companies' response to the Data Breach:

a. Rather than identifying the vulnerability and disclosing it responsibly, UTI's immediate response was to pay the Attackers – who had intentionally acquired personal information and exploited a vulnerability to extort funds – under a bug bounty program.

b. UTI did not appoint Mandiant to conduct a forensic analysis of the kinds of data in the files that were accessed by the Attackers until approximately 11 months after it became aware that the Data Breach occurred. In my view, this analysis was necessary for the Uber Companies to understand the scope of the Data Breach and adopt appropriate strategies for responding to it. Although it is acknowledged that UTI's security team took some action to determine what data was accessed by the Attackers,[110] the Uber Companies should have acted promptly to conduct a full assessment of all personal information that may have been accessed by the Attackers, either internally through UTI's security team or by engaging an external expert to do so.

c. The Uber Companies did not make a public statement about the Data Breach or notify affected Australian drivers until approximately 12 months after the Data Breach had occurred. This was not reasonable, as after so much time had elapsed, affected individuals were not afforded a meaningful opportunity to take steps to protect their compromised personal information from further unauthorised access or misuse. Instead, the Uber Companies should have promptly determined whether Affected Australian users ought to be notified, based on a prompt assessment of what personal information had been accessed by the Attackers (as discussed in paragraph 125(b)).

126. I accept that at the time of the Data Breach, the Uber Companies generally had in place various internal policies, procedures, technical documentation and training materials. However, [redacted] (the **Incident Response Plans**), are the only policies provided to my office that were in place at the time of the Data Breach, which expressly dealt with data breach responses.

---

[108] https://www.uber.com/en-CA/newsroom/2016-data-incident

[109] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 10.

[110] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 p 5.

127. While the Incident Response Plans discussed assessing the impact of data breaches and notifying individuals in a general sense, they did not include clear processes for how the assessment should occur or for determining whether, when and how to notify impacted individuals. [111]

128. In my view, it would have been reasonable for the Uber Companies to have had in place an incident response plan that included at least the following:

a. processes for promptly assessing the impact of a data breach, including who would have responsibility for the assessment, and procedures for gathering and evaluating necessary information about what personal information was involved in a breach and potential risks

b. thresholds and processes for determining which individuals and/or entities should be notified, if any (noting that notification of affected individuals may, in some circumstances, be a reasonable step to comply with APP 1.2)

c. timeframes for any notification to occur, having regard to the nature of the breach and the personal information accessed.

129. In particular, while it is not a requirement under APP 1.2 that APP entities seek external assessments of data breaches, I consider that as part of the measure outlined in paragraph 128(a), the Uber Companies should have had procedures in place to:

a. conduct an initial evaluation of whether the Uber Companies had adequate internal technical capability to assess the impact of the Data Breach

b. promptly engage a qualified third party to conduct the assessment in circumstances where it was determined that the Uber Companies did not have such capability.

130. It would also have been reasonable for the Uber Companies to have operationalised the policy referred to in paragraph 128, including by providing training to relevant staff in relation to the policy.

131. There is no evidence before me to suggest that it would have been impracticable for the Uber Companies to take the above steps.

132. With regard to UBV, I do not accept that taking additional steps in relation to the policies for the identification and response to data breaches would not have led to UBV learning of the Data Breach when it occurred. In my view, UBV could have taken steps to ensure that UTI was complying with its obligations under the 2016 DPA on an ongoing basis.

133. For example, the contractual arrangements between UBV and UTI at the time of the Data Breach required UTI to promptly notify UBV of data breaches, and keep UBV informed of developments.[112] [redacted].[113]

---

[111] Letter from the Uber Companies' representative to the OAIC dated 21 December 2018 Annex 6; Letter from the Uber Companies' representative to the OAIC dated 3 July 2020 p 9.
[112] E.g., 2016 DPA, [redacted].
[113] 2016 DPA, [redacted]/

134. In my view, UBV could have conducted independent assessments or audits to confirm that UTI was promptly notifying it about any data breaches.[114] For example, UBV could have asked UTI questions to understand if any data breaches involving Australian users' personal information had not been duly reported, or sought documentation in relation to any security incidents that UTI had deemed not reportable under the 2016 DPA.

135. These are examples of reasonable minimum steps UBV could have taken in the circumstances, as part of implementing procedures for identifying and responding to privacy breaches. However, there is no evidence that UBV took any such steps to ensure ongoing compliance by UTI.

136. In my view, the Uber Companies did not take steps as were reasonable in the circumstances to implement practices, procedures and systems relating to their functions or activities that would ensure that they complied with the APPs, as required in accordance with APP 1.2.

Finding – APP 1.2

137. It is my view that, at the time of the Data Breach, the Uber failed to take reasonable steps in the circumstances to implement practices, procedures and systems relating to the Uber Companies' functions and activities, to ensure that the Uber Companies comply with the APPs, in breach of APP 1.2.

Remedies

138. There are a range of regulatory options that I may take following an investigation commenced on my own initiative. For example, I have powers to accept an enforceable undertaking, make a determination which may include declarations requiring the entity to take certain steps, or apply to the court for a civil penalty order.

139. In determining what form of regulatory action to take, I have considered the factors outlined in the OAIC's Privacy Regulatory Action Policy[115] and the OAIC's Guide to Privacy Regulatory Action.[116] In my view, the following factors weigh in favour of making a determination that finds the Uber Companies have interfered with individuals' privacy and breached APP 1.2, and must not repeat the conduct:

a. The objects in s 2A of the Act include promoting the protection of the privacy of individuals and promoting responsible and transparent handling of personal information by entities.

b. The incident was serious. The conduct involved personal information of approximately 1.2 million Australians.

c. The burden on the Uber Companies likely to arise from the regulatory action is justified by the risk posed to the protection of personal information.

d. There is specific and general educational, deterrent or precedential value in making a determination in this matter, for the reasons discussed at paragraph 142

[114] 2016 DPA, [redacted].
[115] Privacy Regulatory Action Policy [38].
[116] Guide to Privacy Regulatory Action [4.9].

e. There is a disagreement about whether an interference with privacy has occurred, and this determination allows this question to be resolved.

140. There is a public interest in making a declaration setting out my reasons for finding that an interference with privacy has occurred, and the appropriate response by the Uber Companies.

141. I am aware that the Uber Companies have been the subject of regulatory action in relation to this Data Breach in other jurisdictions. For example, certain Uber companies were fined £385,000 by the UK Information Commissioner's Office[117] and €600,000 by the Dutch Data Protection Authority[118] in relation to the Data Breach. In addition, under its consent agreement with the US Federal Trade Commission (FTC) – which was negotiated partly in response to this Data Breach – UTI was required to make certain forward-looking changes to its privacy practices, such as implementing a comprehensive privacy program and obtaining biennial third-party assessments for 20 years.[119]

142. I consider it appropriate and proportionate to take regulatory action in respect of the Uber Companies in Australia, despite the orders made overseas, for the following reasons:

a. The investigations conducted in other jurisdictions did not consider whether personal information of Australian individuals had been handled in contravention of the Privacy Act.

b. The declarations are intended to ensure that the Uber Companies protect and handle Australians' personal information in accordance with the Privacy Act in future.

c. This matter raises complex issues that are specific to the Australian legislative context, including the application of the extraterritorial jurisdiction provisions in the Privacy Act to companies that outsource the handling of Australians' personal information to companies within their corporate group through 'data processing' agreements or similar arrangements.

Declarations requiring the Uber Companies to take 'specified steps'

143. Under s 52(1A)(b) I may declare that an entity must take specified steps within a specified period to ensure that such conduct is not repeated or continued.

144. I have decided to require the Uber Companies to take specified steps to ensure the conduct set out in paragraphs 97, 112 and 137 is not repeated.

145. In determining the content of the steps the Uber Companies are required to take, I have considered:

a. the Uber Companies' submissions in relation to proposed declarations in the preliminary view

b. the Uber Companies' current activities in Australia

---

[117] https://ico.org.uk/media/action-weve-taken/mpns/2553890/uber-monetary-penalty-notice-26-november-2018.pdf

[118] https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-fine-data-breach-uber

[119] https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_decision_and_order.pdf

c. the steps the Uber Companies have taken since the Data Breach (see paragraph 19).

Uber Companies' submissions

146. The Uber Companies submitted that:

a. I do not have the power to make a declaration requiring the Uber Companies to develop an incident response plan, as the proposed declarations do not relate to any act or practice that was, at the time of the Data Breach, an interference with the privacy of one or more individuals.[120]

b. It is not possible for an act or practice of the Uber Companies at the time of the Data Breach to have constituted an interference with the privacy of an individual by virtue of it purportedly breaching Part IIIC of the Privacy Act, so there should be no reference to Part IIIC in my declarations as set out in paragraph 2 of this Determination.[121]

c. I do not have the power to make declarations requiring an independent expert to determine that certain steps must be taken by the Uber Companies on the basis that this is an impermissible delegation of my power under s 52(1A) of the Privacy Act.[122]

d. The substantial steps the Uber Companies have taken both prior to the commencement of my investigation, and on an ongoing basis, mean that the imposition of additional specified steps which overlap those already undertaken by the Uber Companies would not be proportionate to the situation or the conduct concerned.[123]

147. I do not accept these submissions.

148. In respect of my power to make declarations, s 40(2) of the Privacy Act states that I may, on my own initiative, investigate an act or practice if:

a. the act or practice may be an interference with the privacy of an individual or a breach of APP 1; and

b. I think it is desirable that the act or practice be investigated.

149. Subsection 52(1A) of the Privacy Act states that after investigating an act or practice under s 40(2), I may make a determination that includes one or more declarations, including, under s 52(1A)(b), requiring the entity to take steps to ensure that the act or practice is not repeated. I have investigated the acts and practices of the Uber Companies, and have concluded that these acts or practices were in breach of APP 1.2.

150. In making a declaration or declarations under s52(1A)(b), I do not need to be satisfied that an act or practice in breach of APP 1.2 is also an interference with privacy of more or more individuals.

151. Accordingly, I have the power to make declarations under s 52(1A)(b) requiring the Uber Companies to take steps to ensure that the breach of APP 1.2 is not repeated.

---

[120] Letter from the Uber Companies' representative to the OAIC dated 20 July 2020 p 10-11.
[121] Letter from the Uber Companies' representative to the OAIC dated 20 July 2020 p 11.
[122] Letter from the Uber Companies' representative to the OAIC dated 20 July 2020 p 11-12.
[123] Letter from the Uber Companies' representative to the OAIC dated 27 April 2021 p 2.

152. In respect of Part IIIC of the Privacy Act, the Privacy Act now includes specific requirements for identifying and responding to particular types of eligible data breaches. In my view, as part of ensuring the Uber Companies do not repeat the breaches of APP 1.2, the Uber Companies must implement an appropriate incident response plan which complies with the Privacy Act in its current form, which includes Part IIIC. It would not be reasonable or appropriate for a declaration to be made under section 52(1A)(b) requiring the Uber Companies to comply with a version of the Privacy Act that does not represent the current law.

153. In respect of the Independent Expert, I am satisfied that requiring the Uber Companies to appoint an Independent Expert to determine whether they have complied with the steps imposed by me, and specify any actions necessary to ensure that my declarations have been complied with, is not a delegation of my power. The role of the Independent Expert is not to determine the steps the Uber Companies must take, but to ensure that the Policies and Programs meet the requirements in paragraph 2 of this Determination. I am satisfied that this is reasonable and appropriate in the circumstances.

154. Lastly, I acknowledge the Uber Companies have taken some steps to prevent reoccurrence (as outlined in paragraphs 19 to 20 above). However, having regard to the factors in paragraph 142, I consider that these declarations are proportionate to ensure that Australians' personal information will be handled in accordance with the APPs.

Current activities in Australia

155. In my view, the declarations must apply to both of the Uber Companies, given that, as explained in paragraphs 155 to 159 below, both continue to carry on business in Australia and collect Australians' personal information within the meaning of ss 5B(3)(b) and (c) of the Privacy Act.

156. On 12 December 2019, Uber restructured its internal data handling responsibilities. As part of this restructuring, UBV and UTI entered into a new Data Processing Agreement (the **2019 DPA**) under which UTI became the 'controller' and UBV became the 'processor' in respect of personal data collected outside the European Union, the European Economic Area, Switzerland and the United Kingdom.[124] UTI submits that under the 2019 DPA, UTI collects the personal information of Australian users for the purposes of providing services as set out in its Privacy Notice,[125] and carries out activities in connection with these services. UTI submits that these activities are generally carried out by UTI in respect of Uber's global operations and therefore to the extent that these activities affect global riders and drivers, they would equally affect Australian users.[126]

157. Having regard to the discussion of the meanings of these terms at paragraphs 39 to 45, the following factors establish that UTI currently both carries on business in Australia and collects personal information in Australia:

a. Under the 2019 DPA, UTI carries out activities in connection with the following services as described in the 2019 Privacy Policy, as part of Uber's global operations:[127]

[124] Letter from the Uber Companies' representative to the OAIC dated 24 January 2020 p 9; 2019 DPA [redacted].
[125] Letter from the Uber Companies' representative to the OAIC dated 24 January 2020 p 9.
[126] Letter from the Uber Companies' representative to the OAIC dated 24 January 2020 p 13.
[127] Letter from the Uber Companies' representative to the OAIC dated 24 January 2020 p 13.

i. providing services and features

ii. safety and security

iii. customer support

iv. research and development

v. enabling communications between users

vi. marketing

vii. non-marketing communications

viii. legal proceedings and requirements

ix. automated decision-making.[128]

b. Since Uber's global restructure on 12 December 2019 and under the 2019 DPA, UTI is the entity responsible for the collection of personal information from Australian users. When Australian users submit personal information through the Uber app or website, that information is collected and transferred directly to, and stored, by UTI.[129]

158. Having regard to the discussion of the meanings of these terms at paragraphs 39 to 45, the following factors establish that UBV currently carries on business in Australia and collects personal information in Australia:

a. UBV is licensor of the Uber software in Australia and directly contracts with Australian users.[130]

b. As data processor for, and under instructions from UTI, UBV carries out processing activities as specified in 2019 DPA as well as the processing activities described in the data sharing agreement between UTI and UBV dated 12 December 2019, specifically:

i. accounts and records

ii. advertising, marketing and prospecting

iii. business operations

iv. communication

v. improve mapping technology and features

vi. internal operations

vii. litigation and investigation

viii. onboarding

[128] Letter from the Uber Companies' representative to the OAIC dated 24 January 2020 p 9.
[129] Letter from the Uber Companies' representative to the OAIC dated 24 January 2020 p 9.
[130] Letter from the Uber Companies' representative to the OAIC dated 24 January 2020 p 9.

ix. product development and improvement

x. transactions

xi. vendor agreements

xii. other processing activities[131]

c. UBV collects Australian users' personal information as a data processor for UTI.[132]

159. These factors show that the Uber Companies continue to be involved in several activities in Australia that amount to, or are ancillary to, transactions that make up or support their business. For each company, they provide clear evidence that the entity engages in activity which is commercial in nature with a repetitive and permanent character in Australia.

Compensation or act of redress

160. I am not authorised under the Privacy Act to award compensation simply because an organisation has breached the Act. Unless an affected individual supplies evidence of loss or damage, they are not entitled to a remedy.[133]

161. My office had not received any individual complaints about this issue.

162. There is no other evidence before me to support a declaration that the Uber Companies redress any loss or damage suffered, or that any individuals are entitled to a specified amount by way of compensation.[134]

Angelene Falk
Australian Information Commissioner and Privacy Commissioner
30 June 2021

Review rights

A party may apply under s 96 of the *Privacy Act 1988* (Cth) to have a decision under s 52(1) or (1A) to make a determination reviewed by the Administrative Appeals Tribunal (AAT). The AAT provides independent merits review of administrative decisions and has power to set aside, vary, or affirm a privacy determination. An application to the AAT must be made within 28 days after the day on which the person is given the privacy determination (s 29(2) of the Administrative Appeals Tribunal Act 1975).

---

[131] Letter from the Uber Companies' representative to the OAIC dated 24 January 2020 Annex 14.
[132] Letter from the Uber Companies' representative to the OAIC dated 24 January 2020 p 9.
[133] *'PB' and United Super Pty Ltd as Trustee for Cbus (Privacy)* [2018] AICmr 51 (23 March 2018) [91].
[134] ss 52(1A)(c) and (d) of the Privacy Act.

An application fee may be payable when lodging an application for review to the AAT. Further information is available on the AAT's website (www.aat.gov.au) or by telephoning 1300 366 700.

A party may also apply under s 5 of the *Administrative Decisions (Judicial Review) Act 1977* to have the determination reviewed by the Federal Circuit Court or the Federal Court of Australia. The Court may refer the matter back to the OAIC for further consideration if it finds the Information Commissioner's decision was wrong in law or the Information Commissioner's powers were not exercised properly. An application to the Court must be lodged within 28 days of the date of the determination. An application fee may be payable when lodging an application to the Court. Further information is available on the Court's website (www.federalcourt.gov.au/) or by contacting your nearest District Registry.

Attachment A

Matters considered in Determination

1. In reaching the conclusions set out in this Determination, I have considered and had regard to the following:

   a. written responses, including attachments, provided by the solicitors for the Uber Companies to questions asked by the OAIC, as provided by letters and emails dated:

      i. 30 November 2018;

      ii. 21 December 2018;

      iii. 21 January 2019;

      iv. 20 May 2019;

      v. 11 October 2019;

      vi. 9 December 2019;

      vii. 27 April 2021.

   b. the solicitors for the Uber Companies' written response to the Deputy Commissioner's preliminary view dated 3 July 2020

   c. written responses provided by the solicitors for the Uber Companies on, in response to the OAIC's request for information issued under subsection 44(1) of the Privacy Act, on:

      i. 24 January 2020

      ii. 18 January and 29 January 2021

   d. the *Australian Privacy Principles Guidelines*, which are available here: https://www.oaic.gov.au/assets/privacy/app-guidelines/app-guidelines-july-2019.pdf (**APP Guidelines**).

Attachment B

Relevant law – Privacy Act

Determination powers

52 Determination of the Commissioner

(1A) After investigating an act or practice of a person or entity under subsection 40(2), the Commissioner may make a determination that includes one or more of the following:

(a) a declaration that:

(i) the act or practice is an interference with the privacy of one or more individuals; and

(ii) the person or entity must not repeat or continue the act or practice;

(b) a declaration that the person or entity must take specified steps within a specified period to ensure that the act or practice is not repeated or continued;

(c) a declaration that the person or entity must perform any reasonable act or course of conduct to redress any loss or damage suffered by one or more of those individuals;

(d) a declaration that one or more of those individuals are entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice;

(e) a declaration that it would be inappropriate for any further action to be taken in the matter.

APP entity

6 Interpretation

In this Act, unless the contrary intention appears:

…

APP entity means an agency or organisation.

Interferences with privacy

13 Interferences with privacy

APP entities

(1) An act or practice of an APP entity is an *interference with the privacy of an individual* if:

(a) the act or practice breaches an Australian Privacy Principle in relation to personal information about the individual; or

(b) the act or practice breaches a registered APP code that binds the entity in relation to personal information about the individual.

…

APP compliance

15 APP entities must comply with Australian Privacy Principles

An APP entity must not do an act, or engage in a practice, that breaches an Australian Privacy Principle.

Extra-territoriality

5B Extra-territorial operation of Act

…

Organisations and small business operators

(1A) This Act, a registered APP code and the registered CR code extend to an act done, or practice engaged in, outside Australia and the external Territories by an organisation, or small business operator, that has an Australian link.

Note: The act or practice overseas will not breach an Australian Privacy Principle or a registered APP code if the act or practice is required by an applicable foreign law (see sections 6A and 6B).

Australian link

(2) An organisation or small business operator has an ***Australian link*** if the organisation or operator is:

(a) an Australian citizen; or

(b) a person whose continued presence in Australia is not subject to a limitation as to time imposed by law; or

(c) a partnership formed in Australia or an external Territory; or

(d) a trust created in Australia or an external Territory; or

(e) a body corporate incorporated in Australia or an external Territory; or

(f) an unincorporated association that has its central management and control in Australia or an external Territory.

(3) An organisation or small business operator also has an ***Australian link*** if all of the following apply:

(a) the organisation or operator is not described in subsection (2);

(b) the organisation or operator carries on business in Australia or an external Territory;

(c) the personal information was collected or held by the organisation or operator in Australia or an external Territory, either before or at the time of the act or practice.

…

Personal information

6 Interpretation

In this Act, unless the contrary intention appears:

…personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

APP 1

1 Australian Privacy Principle 1—open and transparent management of personal information

…

Compliance with the Australian Privacy Principles etc.

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

(a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

…

APP 11

11 Australian Privacy Principle 11—security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If:

(a) an APP entity holds personal information about an individual; and

(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

(c) the information is not contained in a Commonwealth record; and

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.