MERIDIAN LAWYERS

September 2021

Commercial Insights

Do you send personal information offshore?

A recent decision of the Australian Information and Privacy Commissioner highlights the responsibilities of global corporations with Australian users under Australian privacy law, particularly where the handling of personal information of Australians is outsourced to a company based overseas, whether that be a company within the same corporate group, or an unrelated third party. It is a reminder that the Australian privacy laws have extra-territorial reach even where the company collecting the personal information has no physical presence in Australia. This decision is also a timely reminder that personal information should not be held indefinitely. Entities holding personal information are required to delete or de-identify that information once it is no longer required.

There is a complex set of corporate arrangements that make up the popular global ride sharing platform Uber, including Uber Technologies, Inc. (incorporated in the United States of America) which is the parent company of Uber B.V. (incorporated in the Netherlands). For the purpose of this article the Uber entities are collectively referred to as Uber.

The Uber platform was first introduced in Australia in 2012. In October and November 2016, Uber was subjected to an external cyberattack where Uber data stored in Amazon Web Service's cloud-based storage was accessed and downloaded. The files accessed by the bad actors had not been encrypted. At the time of the incident, the personal information of Australian Uber customers and drivers using the Uber platform was directly transferred to servers in the United States of America. The bad actors accessed and downloaded files relating to approximately 57 million individuals worldwide, including approximately 1.2 million Australian accounts. Of these Australian accounts, approximately 960,000 were rider accounts and approximately 240,000 were driver accounts.

In response to communication received from the bad actors following the data breach (among other things), Uber:

- paid the bad actors $100,000
- received written assurance from the bad actors that the hacked data had been destroyed and that they would not disseminate the data
- rotated the compromised access key, and
- began requiring two-factor authentication.

In October 2017 (approximately 11 months after the data breach) Uber engaged a forensic IT consultant firm to analyse the data in the files downloaded by the bad actors. It was identified that the bad actors had accessed various information including individuals' names, email addresses, mobile phone numbers and geolocation information. The bad actors also had access to some drivers' licence numbers. The report found that no evidence of trip history, credit card details, bank account numbers, date of birth or government related identification numbers was downloaded.

Uber didn't publicly announce the data breach until 21 November 2017. In doing so, Uber contacted drivers, but not riders who were individually impacted.

September 2021

On 30 June 2021, the Office of the Australian Information Commissioner (**OAIC**) determined that Uber had interfered with the privacy of approximately 1.2 million impacted Australians, and consequently breached the *Privacy Act 1988* (Cth). Specifically, Commissioner Falk found that Uber had breached the Australian Privacy Principles by failing to take reasonable steps to:

1. protect personal information of Australian customers and drivers from unauthorised access (in breach of APP 11.1)
2. delete or de-identify personal information that is no longer needed for a permitted purpose (in breach of APP 11.2), and
3. implement practices, procedures and systems to ensure compliance with the APPs (in breach of APP 1.2).

Uber had argued that as the server was attacked offshore, the matter was not subject to the jurisdiction of the *Privacy Act*. The determination confirms that the Australian Privacy Principles and the *Privacy Act* apply to overseas companies that have an Australian link. The Commissioner determined that while each of the Uber entities did not have a physical presence in Australia, at the time of the data breach, they were engaging in activity in Australia. In handing down the decision, Commissioner Falk stated "*Australians need assurance that they are protected by the Privacy Act when they provide personal information to a company, even if it is transferred overseas within the corporate group".*

The determination ordered Uber to:

- prepare, implement and maintain a data retention and destruction policy, information security program, and incident response plan to ensure ongoing compliance with the APPs
- appoint an independent expert to provide the OAIC with reports on these policies and their implementation, and
- make any necessary changes as recommended by the independent expert.

A link to the full determination is available here.

This article was written by Special Counsel, Hayley Bowman and Legal Assistant Meg Ryan. If you have any questions about your obligations when handling personal information or require assistance in reviewing your privacy practices and policies, please contact Hayley Bowman.

Hayley Bowman
Special Counsel
+61 3 9810 6723
hbowman@meridianlawyers.com.au