Google $60m penalty decision illustrates heightened risk climate for data collection in Australia

AUGUST 2022

wotton kearney
A founding member of LEGALIGN GLOBAL

On 12 August 2022, Justice Thawley of the Federal Court of Australia ordered that Google LLC and Google Australia Pty Ltd (Google) pay $60m in damages for misrepresentations about the collection, use and storage of location information gathered from users of android mobile devices[1].

The Google case illustrates the high penalties and alternative means of prosecution available to Australian regulators for inadequate disclosure of data collection and handling practices. It is also evidence of the heightened regulatory and risk environment around data and management of privacy obligations generally.

The infringing conduct

The penalty ordered concludes the ACCC's prosecution of Google over the collection and use of location data.

In the 2021 Federal Court decision giving rise to the penalty[2], Google was found to have breached the Australian Consumer Law by engaging in misleading and deceptive conduct. The misleading and deceptive conduct involved the collection of android mobile phone users' location data. It was found to comprise:

- misleading users to the effect that their location data would not be collected if their 'Location History' was turned off, and
- not properly informing users that a secondary setting called 'Web & App Activity' would also collect location information unless it was turned off.

It should be noted that Google was found to have engaged in misleading and deceptive conduct even though consumers could access a privacy policy that described the full scope of collection of location data via a link.

The regulatory context

This is not the only time the ACCC has brought proceedings in the privacy and data protection space:

- **HealthEngine** – *disclosure of health information without consent (2021)*

  HealthEngine was found to have engaged in misleading and deceptive conduct regarding representations about handling personal information in the context of its disclosure of the personal information of 135,000 users to insurance brokers without consent.[3] HealthEngine was ordered to pay approximately $1.4m in fines.

- **Facebook** – *Onavo Protect VPN software (2020, ongoing)*

  The ACCC alleges that, between February 2016 and October 2017, Facebook and its subsidiaries misled Australian consumers by representing that the Onavo Protect app would keep users' data private, protected and secret, and that the data would not be used for any other purpose other than providing Onavo products. However, Onavo allegedly collected, aggregated and used significant amounts of personal activity data for Facebook's commercial benefit.

- **Google** – *separate case regarding the collection of user activity data (2020, ongoing)*

  The ACCC alleges that Google misled Australian consumers in order to obtain their consent to expand the scope of the personal information that Google could collect and combine about user activity (including for targeted advertising).

These enforcement actions reflect a similar trend seen with the ACCC's international counterparts. In the United States, for example, the Federal Trade Commission has sued companies for misleading privacy policies[4].

[1] *Australian Competition and Consumer Commission v Google LLC & Anor (No. 4)* [2022] FCA 942.
[2] *Australian Competition and Consumer Commission v Google LLC & Anor (No. 2)* [2021] FCA 367.
[3] *Australian Competition and Consumer Commission v HealthEngine Pty Ltd* [2020] FCA 1203.
[4] Examples of US Federal Trade Commission's matters available online at: https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement

Implications for organisations that collect data

It's clear that protecting consumers who use digital platforms and provide their personal information to trusted entities remains a key priority for Australian regulators.

In 2021, then ACCC Commissioner, Rod Sims, described the Federal Court's decision in the Google case as "an important step to make sure digital platforms are upfront with consumers about what is happening with their data and what they can do to protect it." He further commented that: "Companies that collect information must explain their settings clearly and transparently, so consumers are not misled."

Australian privacy law has long required organisations collecting personal information to ensure that individuals are properly informed about data collection and to seek express consent to collection of sensitive information[5]. The Google case provides another example of the ACCC taking action in what is traditionally the OAIC's domain.

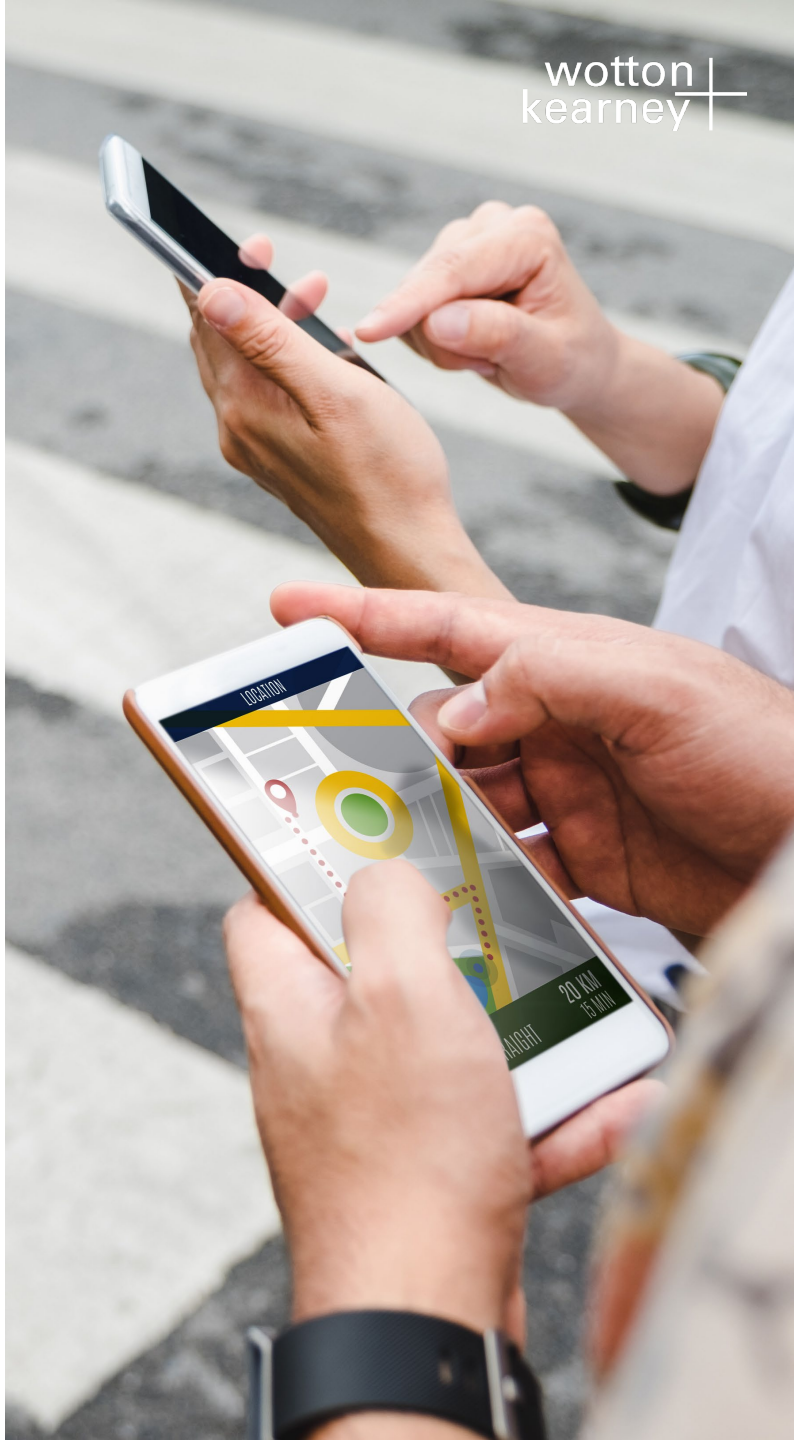
The magnitude of the penalty, together with other penalties in the cyber and data space (as we discuss in our update on the RI advice penalty in this bulletin) starkly demonstrates that organisations face a willing coalition of regulators and a high price for getting privacy or data collection wrong. While the alternative avenues for prosecution are not new, the current environment is one of significantly heightened regulatory and legal risk.

In this environment, Google-like regulatory attention and consequences can be avoided if organisations:

- fully (and consistently) describe matters like collection of personal information and use, storage and disclosure of data
- seek express consent where sensitive information is involved, and
- are upfront about data collection, use and consent, rather than relying on layers of 'click through' information, like a link to their privacy policy

Insurers can mitigate risk by ensuring that insureds have adequate privacy policies in place, as well as robust data collection, handling and compliance processes.

The Google penalty is a call to action on privacy and data obligations. If you are leaving it to your customers to work out what you are doing with their data instead of being upfront with them, the magnitude of the penalty may mean some uncomfortable conversations with your board and shareholders.



[5] See, in particular, APP 1, APP 3 and APP 5, Schedule 1, *Privacy Act* 1988 (Cth).