



■ Privacy

## IT'S PERSONAL

Tougher *Privacy Act* penalties will work hand in hand with a more rigorous approach from both the ACCC and OAIC to ensure personal data remains personal, writes Annelies Moens FAICD.

On 12 December 2019, the government responded to the Australian Competition and Consumer Commission (ACCC) final report on its Digital Platforms Inquiry. This response is in addition to the Government's initial response in March 2019 to introduce a tougher penalty regime in the *Privacy Act 1988* (Cth) to align it with penalties in the *Competition and Consumer Act 2010* (Cth).

The Office of the Australian Information Commissioner (OAIC) has also been developing a code to specifically regulate how digital platforms such as Google handle consumers' personal data.

The government supported the ACCC recommendations and some are already underway as outlined above. Some of the supported recommendations will require further review to design specific measures appropriately and ensure recommended approaches are sufficient to address consumer harms.

In the mid-year economic and fiscal outlook 2019-20, \$1.7m was allocated to the Attorney-General's Department for this *Privacy Act* review to ensure the specific measures are designed and drafted appropriately. The government has timetabled the completion of this review for 2021, while legislation implementing the increased

penalty regime will be introduced this year.

### Who is affected?

One recommendation provides for a direct right of action to enable individuals to bring actions and class actions in court to seek compensation for alleged breaches of the *Privacy Act*, in addition to lodging a complaint with the OAIC.

The recommendations will affect all entities currently regulated by the *Privacy Act*:

- Private sector businesses with an annual turnover greater than \$3m
- Private sector health service providers, regardless of annual turnover
- Credit reporting bodies
- Residential tenancy database operators
- Any organisation handling TFN data
- ACT/federal government agencies/contractors
- Offshore entities fitting the above criteria that have a link with Australia (extra-territorial application).

### Content changes to watch out for

The Final Digital Platforms Inquiry had 23 recommendations, six of which relate to privacy. The government supported changes in relation

to some fundamental concepts of the *Privacy Act*. The three key areas are:

- Clarification of the definition of personal information, specifically to ensure it covers technical data (such as device ID, IP address, location data)
- Strengthening the notice of collection of personal information requirements, in particular when personal information is not collected directly from the consumer
- Stronger consent requirements and the use of pro-consumer defaults (opt-in, not opt-out)
- Work is also underway to consider the prohibition of unfair contract terms and unfair trading practices; the latter through Consumer Affairs Australia and New Zealand.

### Governance implications – merging competition and privacy reform

The regulation of data, in particular individuals' personal information is of increasing focus to broader stakeholder groups as data collection and customisation expands, data breaches increase, consumer trust declines and more and more power is being concentrated among fewer players. The ACCC, with more resources than the OAIC, is actively targeting this area with the result that competition and privacy regulation are increasingly merging. In 2019, the ACCC launched (currently ongoing) court proceedings in relation to alleged inappropriate handling of consumers' personal information against:

**HealthEngine** – for allegedly providing contact and identification details of 135,000 patients to private health insurance brokers for a fee without adequately disclosing this to patients.

**Google** – for allegedly collecting and using location data without users' consent. When users turned off "Location History", Google was still tracking their location through "Web/App Activity". The ACCC argued it was misleading to not properly disclose to users that both settings had to be switched off, if they didn't want Google to access their location data.

► Annelies Moens FAICD is MD of Privcore.