Update.

Hot topic

PRIVATE INVESTIGATIONS

The Digital Platforms Inquiry is catalysing major enforcement changes to the Privacy Act.

By Annelies Moens FAICD

The ACCC is expected to release its final report on the Digital Platforms Inquiry on 30 June. Legislation to amend the *Privacy Act 1988* (Cth) and introduce an increased penalty regime is expected to be drafted for consultation in the second half of this year. The ACCC released its preliminary report in December 2018. There are ramifications beyond digital platforms and many of the ACCC recommendations apply to all entities regulated under the *Privacy Act*. This means: all businesses with an annual turnover of more than $3m, all federal and ACT government agencies, all private healthcare services, entities handling tax file numbers, and small businesses that are not exempt should be alert to the possible ramifications.

The ACCC recommended penalties of $10m – or three times the benefit received, or 10 per cent of annual domestic turnover – be introduced for serious or repeated interferences with the privacy of an individual. These provisions are in line with penalties under the *Competition and Consumer Act 2010* (Cth) for anti-competitive practices.

> How organisations manage personal information is a board issue, not just an IT issue or a low-level compliance issue.
>
> Annelies Moens FAICD

Historically, there has been little political appetite to adequately resource the Office of the Australian Information Commissioner (OAIC) or ensure enforcement powers are sufficient to deter harm to consumers caused by breaches of the Australian Privacy Principles (APPs).

However, as trade in personal information increases, the consequences of bad data governance practices, ubiquitous over-collection and retention of personal information, and data breaches are becoming apparent.

In its first year of operation, approximately 1000 data breaches were reported to the OAIC under the notifiable data breaches (NDB) scheme (964 between 1 April 2018-31 March 2019). The top five sectors were healthcare, finance, professional service firms, education and personal services. In March, Attorney-General Christian Porter announced increased resources to the OAIC and the tougher penalty regime.

Need to know

While the major digital platforms have a lot to contend with from a privacy perspective, every other entity regulated under the *Privacy Act* needs to consider its common privacy risks. In my experience working at the privacy regulator and consulting with clients, the top five insufficiently managed and commonly occurring privacy risks are:

1 Never deleting personal data – no destruction or retention policies in place or acted upon.
2 Over-collection of personal information.
3 Failure to effectively manage customer expectations, as most information about how personal details are handled is in privacy policies or terms and conditions that are not read or which are far removed from data collection points and contexts relevant and/or understandable to the customer.
4 Failure to use multi-factor authentication and encryption – hence insecure email and systems, and increased risk of phishing attacks.
5 Third-party arrangements with suppliers that don't adequately protect personal data, often due to failure to check supply-chain privacy risks.

Governance implications

How organisations manage personal information is a board issue, not just an IT issue or a low-level compliance issue. Privacy is both a strategic business opportunity and risk. To prepare for the expected increases in resources and enforcement powers to be given to the OAIC, directors need to ensure their organisations have determined their risk appetite and are taking steps to appropriately steward the data for which they are custodians.

Annelies Moens FAICD is managing director Privcore, co-founder International Association of Privacy Professionals in Australia and NZ.