BUDDLEFINDLAY

25 years young – the Privacy Act gets a face lift

Alastair Hercus, Hamish Kynaston, Peter Chemis, Sherridan Cook, Susan Rowe, Susie Kilty, Tony Dellow, Alastair Sherriff, Amy de Joux, Holly Hedley, Jessica White, Mere King, Natasha Wilson, Nicola Cuervo

29 March 2018

The Privacy Act 1993 became law at a time when the internet was in its infancy, and the way in which agencies gathered, stored, and shared information was very different than it is now.

There have been calls, including from the Privacy Commissioner, to modernise the Privacy Act to reflect the significant changes to technology and the way that agencies deal with personal information (and how much information they hold), and to keep pace with privacy developments around the world. The 2011 Law Commission Review of the Privacy Act 1993 contained 136 recommendations for change, including that a new Privacy Act be enacted.

The new Privacy Bill would repeal and replace the existing Act, although it largely retains the structure of the existing Act, and includes the 12 information privacy principles (IPPs) that set out agencies' key obligations when dealing with personal information. The Bill also includes new provisions designed to strengthen (and clarify) the current privacy framework, as summarised below, which will have an impact on all agencies that hold or otherwise deal with personal information.

Mandatory reporting of data breaches and compliance notices

The Bill introduces a mandatory requirement for agencies to report privacy breaches (unauthorised access to, disclosure, alteration, loss, or destruction of personal information, or an action that prevents an agency from accessing information) to the Privacy Commissioner and affected individuals if the breach has caused or risks causing harm. Harm is defined in the Act, and includes situations where an individual has suffered loss, where their rights and interests may or have been affected, or where they have suffered significant humiliation, loss of dignity, or injury to feelings.

Notification must occur as soon as practicable after an agency becomes aware of a breach, and if it is not reasonably practicable to notify affected individuals, the agency must instead give public notice of the breach. The requirement to report a breach is subject to some exceptions, for example, to protect trade secrets, security, or vulnerable individuals. It is an offence to fail to notify the Commissioner, with a maximum penalty of $10,000 (clause 122). The Regulatory Impact Statement on the Bill records that Cabinet considered that this provides "an effective incentive to ensure breaches are notified to the Commissioner, thus allowing the Commissioner to become aware of, and begin to address, emerging or systemic privacy issues".

Under the new Bill, the Commissioner will also be able to issue compliance notices that require an agency to do something, or stop doing something, in order to comply with its obligations under the Act (clause 124). The Human Rights Review Tribunal will be able to enforce compliance notices and hear appeals (clause 130).

Strengthening cross-border information flow protections

Currently under the Act an agency that stores information overseas does not avoid its obligations under the Act (see section 10). The Bill imposes further requirements relating to the disclosure of information overseas by amending IPP11 (disclosure of information) to say that an agency must not disclose personal information to an overseas person unless:

- The person is an agent of the agency or the information is disclosed for the purpose of safe custody or for processing information on behalf of the disclosing agency (clause 8)
- The individuals concerned have authorised the disclosure
- The overseas person is in a country that is specified in regulations to have privacy laws comparable to New Zealand's
- The agency believes on reasonable grounds that the safeguards that apply to the information are comparable to those in the Act.

It is becoming more common for New Zealand entities to store personal information with overseas-based cloud services. However, the requirements relating to storage in countries with comparable privacy laws, or with safeguards comparable to the Act, do not apply when the disclosure is to a person acting as agent or for safe custody or processing – rather, the agency making the disclosure remains responsible for the information under the Act. That would describe many cloud service arrangements with overseas providers, so the practical effect of the change to IPP11 in those cases may be limited.

Other changes of interest

The Bill gives the Commissioner a new power to direct that an agency provide an individual with access to their personal information (clause 96). While the Act requires agencies to provide access to information when requested, if an agency refuses or incorrectly fails to provide access, the Commission can currently only refer the matter to the Human Rights Review Tribunal. This change will provide the Commissioner with more authority in those situations.

The Bill adds two new grounds for refusing access to an individual's personal information, being if there is a significant likelihood of serious harassment of an individual if access is granted, or if giving access would disclose personal information of a victim (or alleged victim) of crime (clause 52(1)(a)).

The Commissioner is given expanded information-gathering powers when investigating complaints about an interference of privacy, including being able to require any person to provide information and specify a time limit for providing information (clause 92).

IPP4 is amended to require an agency to consider the age of an individual when deciding whether the means of collection of personal information is fair and not unreasonably intrusive.

Part 10 of the Privacy Act sets out information matching programmes authorised by other statutes. While Part 10 is retained as subpart 4 of Part 7 of the Bill, the Bill makes it clear that those provisions are historical, and apply only to information matching programmes authorised under the current Privacy Act before its repeal. This resolves uncertainty about the scope and application of those provisions.

Changes not proposed in the Bill

The Privacy Commissioner has welcomed the new Bill, and is supportive of the additional powers it gives to his office. However, the Bill does not implement a number of recommendations that the Commissioner made to the Government in 2016. These included a new power to impose fines for serious privacy breaches (up to $1m for organisations and $100,000 for individuals), protection for individuals against re-identification of information, the introduction of data portability as a consumer right, and reform of the outdated public register privacy principles.

Given recent developments in relation to Facebook and big data overseas, and the Commissioner's recent comments that "... without real and meaningful consequences, cowboys will ignore their obligations", we expect that the Commissioner is likely to advocate for further changes to be made to the Bill as it goes through the Parliamentary process.

Auckland

PwC Tower
188 Quay Street
Auckland 1010

PO Box 1433
Auckland 1140
New Zealand

P: +64 9 358 2555
F: +64 9 358 2055

Wellington

Aon Centre
1 Willis Street
Wellington 6011

PO Box 2694
Wellington 6140
New Zealand

P: +64 4 499 4242
F: +64 4 499 4141

Christchurch

83 Victoria Street
Christchurch 8013

PO Box 322
Christchurch 8140
New Zealand

P: +64 3 379 1747
F: +64 3 379 5659