

THE PRIVACY ADVISOR

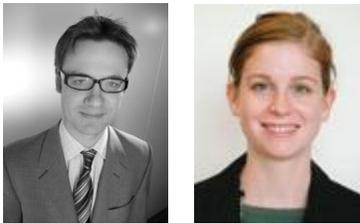
The Official Newsletter of the International Association of Privacy Professionals

iapp

Editor: Kirk J. Nahra, CIPP/US

July-August 2012 • Volume 12 • Number 6

AUSTRALIA & EU—Australian privacy law reform: A step closer to EU adequacy?



By Jan Dhont and Emily Hay

Australian privacy regime

Australia's Privacy Act 1988 governs the federal privacy regime in Australia, along with other legislation relating to telecommunications, healthcare, government data-matching and criminal records. Each state and territory in Australia also regulates its government agencies by way of separate legislation—apart from the Australian Capital Territory, which is covered by the federal laws. The Privacy Act is overseen by the Office of the Australian Information Commissioner, which is also responsible for freedom of information and information policy issues. Since 2001, the Privacy Act has also covered the private sector; however, there are exemptions for most small businesses with an annual turnover under \$3 million (AUD), which covers around 90 percent of Australian businesses. In 2012 the Australian Parliament will implement reforms to the Privacy Act that grant more powers to the information commissioner and streamline some of the public- and private-sector obligations relating to privacy.

EU adequacy

Under Article 25(6) of the EU Directive on data protection (95/46/EC), the European Commission can determine whether a third country ensures an adequate level of protection of personal data. A determination of adequacy is important because it enables the free flow of information between EU member states and third states, aiding business transactions and trade. Negotiations between the EU and Australia on adequacy led to the 2000 amendments to the Privacy Act, which extended application to the private sector. However, in March 2001 the EU's Article 29 Working Party released an opinion expressing concern about the exclusion of small businesses and employee records from the privacy regime.

Moving closer to EU requirements, 2004 amendments to the Privacy Act introduced three main provisions:

- A clear statement that National Privacy Principle 9 (transborder data flows) applies to the personal information of non-Australians as well as Australians;
- The removal of nationality and residency limitations on the Commissioner's power to investigate complaints about the correction of personal information, and

- Allowance for organizations to draft approved privacy codes which include exempt acts or practices.

Since that time, however, the drive to obtain an EU adequacy determination seems to have faded. In 2005, in a review of the private-sector provisions of the Privacy Act, the Office of the Privacy Commissioner, predecessor to the Office of the Australian Information Commissioner, reported that there was no evidence of a broad business push for adequacy and that very few stakeholders claimed trade was inhibited by the lack of adequacy determination. The Australian government has said it will continue working with the EU on adequacy, but amendments that would address EU concerns have not yet been formulated. In a 2010 country study on Australia commissioned by the EU, it was noted that the EU directive remains as an influential international standard in Australian law, but the small number of adequacy findings by the commission has caused the issue to lose currency with policymakers and the media.

2012 reforms: First stage

While they do not address all of the EU's concerns, the 2012 amendments to the Privacy Act provide more robust privacy protection and take a stronger approach to enforcement. These reforms are a partial implementation of the Australian Law Reform Commission's recommendations in a 2008 report on privacy. Due to the number of recommendations, the government decided to address them in two stages of legislation. The first stage is currently before Parliament and is expected to pass without significant amendments. Reforms would come into effect nine months after approval of the new law.

The first stage of reform introduces a number of new powers for the information commissioner, who will be able to:

- Seek civil penalties for serious or repeated interferences with privacy;
- Accept a written undertaking from an organization that they will take or refrain from a specified action. This undertaking will be enforceable in court;
- Make a determination following an investigation conducted on the commissioner's own initiative. Previously, a determination could only be made following the investigation of an individual's complaint;
- Conduct performance assessments of private-sector organizations handling personal information. Previously the Commissioner could only audit government agencies and credit reporting agencies, and
- Develop and register binding privacy codes and a credit reporting code that set out how the act's requirements will be complied with. This power may be exercised where code developers have not complied with a request to develop a code or the commissioner decides not to register the code that was submitted.

The reforms also introduce one set of Australian Privacy Principles (APPs, Schedule 1) to replace the separate public- and private-sector principles that previously applied. The APPs introduce new protections including:

- Enhanced obligations on agencies and organizations regarding an individual's access to, and correction of, their personal information;
- Requiring entities to publish more comprehensive privacy policies to promote more open and transparent management of personal information;
- Introducing a requirement for federal government agencies to accord higher protection to "sensitive" information;
- Ensuring that personal information received by an entity is still protected, even where that information was not solicited by the entity, and
- Introducing a new "Direct Marketing" principle, placing extra limitations on organizations that may use or disclose personal information to promote or sell goods or services directly to individuals.

Other changes to the Privacy Act include:

- The extension of the extraterritorial application of the act. The act and registered codes will now apply to information practices outside Australia by any government agency, and by organizations or small businesses with an Australian link (defined in Section 5B), and
- More comprehensive credit reporting, giving credit providers access to more information about credit accounts in an individual's name in order to allow them to make more robust assessments of credit worthiness. These are joined by increased responsibilities on those providers regarding notification, data quality, access and correction and complaints.

Second stage of reform

A second stage of reform will address other recommendations made by the Australian Law Reform Commission (ALRC) for amending the Privacy Act. No timetable has been set for this second stage of reform, but given that it took four years for the first stage to be brought before Parliament, expectations for a rapid process are low.

Outstanding issues include possible clarification or removal of exemptions from the act. The ALRC proposed removing exemptions for small businesses, employee records and political parties. It was also recommended to introduce mandatory data breach notifications where there is a real risk of serious harm to the individual. Currently there are only voluntary guidelines for data breaches issued by the information commissioner in April. A statutory cause of action for serious invasion of privacy will also be considered in the second phase of amendments.

If the recommendations of the ALRC are implemented, the second stage of reforms will address the major concerns of the EU regarding adequacy and may move Australia towards a positive determination in that regard.

***Jan Dhont** heads the privacy practice of Lorenz Brussels. He specializes in data protection and privacy, telecommunications, media and technology law. He may be reached at j.dhont@lorenz-law.com.*

***Emily Hay** works on the privacy team of Lorenz Brussels. She specializes in data protection and privacy, regulatory and international law. She may be reached at e.hay@lorenz-law.com.*