PRIVACY TOP FIVE: ISSUES AND CONCERNS IN THE FIRST SIX MONTHS OF THE APPs

*By **Alec Christie**, Partner, DLA Piper*

Today, 12 September 2014, marks six months since the Australian Privacy Principles (**APPs**) became effective. Following on from our earlier update *Privacy Top Ten: Things You Think You Know About Privacy – But Don't!*, in this *"Top 5"* we count down the top five privacy issues and client concerns we have seen in the first six months of the operation of the APPs, across all industries and Australian Government agencies.

5. INCREASED ACTIVITY OF PRIVACY COMMISSIONER AND OTHERS – NOWHERE TO HIDE!

Over the last 18 months the number of investigations (in particular, own motion investigations) reported by the Privacy Commissioner has significantly increased. In addition, the attitude of the Privacy Commissioner to investigations and reporting has toughened and the format and content of the reports have become much clearer as to what was done wrong, what should have been done and what the Privacy Commissioner now requires to be done. As a result the reports are in a press friendly style and, not surprisingly, the results of investigations are now being reported more often and more widely by the press.

Most people are aware that a breach of the Privacy Act now can lead to fines of up to A$1.7 million for corporations. But fines are not all you have to worry about!

We have seen a dramatic increase in the number of contracts which include privacy obligations (ie requiring at least one of the parties to the contract, if not both, to strictly comply with the Privacy Act in all dealings with personal information relating to that contract), often obligations in excess of those required by law/the APPs. Thus, if a party were to breach the Privacy Act, in addition to any fines under the Privacy Act that party may also face termination of their contract and/or legal action for breach of contract or for misleading or deceptive conduct, both of which may include damages.

In a recent example of this, the $33 million value contract of a service provider/subcontractor to a service provider to Defence was terminated for breaching the privacy provisions included in its contract (even through its actions were not a breach of the APPs).

4. OFFSHORE DISCLOSURE – OBLIGATIONS AND ONGOING LIABILITY!

There has been much confusion as to what constitutes an offshore disclosure (especially in the Cloud context).

Where any non employee of the Australian company accesses the personal information of that company outside of Australia (even though such information stays on the company's server in Australia), this is an offshore disclosure of the personal information. However, the transfer of personal information you hold in Australia to a server that you control in the Philippines, for example, is not an offshore disclosure of personal information. Similarly, moving personal information to an IaaS Cloud (ie where the Cloud vendor does not access/process any of your data) will not be a disclosure of personal information. Whereas many SaaS offerings, where the SaaS vendor processes/accesses your data, will involve a disclosure of personal information.

Where you disclose personal information outside of Australia (to other than your employees or to a recipient in a country with a similar law and complaints regime, eg the EU) you must take reasonable steps to ensure that the overseas recipient will comply with the APPs (other than APP 1). In addition, in such circumstances, you remain liable for any acts or omissions of the overseas recipient in respect of that personal information that would have breached the APPs if you had done that act or omission yourself in Australia.

3. "COLLECTING" PERSONAL INFORMATION FROM THIRD PARTIES – I HAVE TO DO WHAT NOW?

The APPs do not distinguish or apply different privacy obligations, as they do in the EU, for a "data controller" (eg original collector of the personal information) and a "data processor" (eg a third party processor of the personal information). If you receive personal information, whether you collect it yourself directly from the individual or via a third party, you have the same obligations under the APPs including the obligation to make the mandatory notifications and/or obtain consent (if relevant) on or prior to collection of that personal information. This obligation is not satisfied by the third party, which originally collected the personal information, complying with its obligations regarding notification and/or consent.

That is, on receiving the personal information from a third party, you must contact each individual whose personal information you have now "collected" and notify them of the mandatory matters specified in the APPs, if such is reasonable (and in most cases it will be considered reasonable to do so by the Privacy Commissioner). However, in practice, this is often impractical and so we have developed workarounds for a number of clients to meet their obligations in different ways and in a number of different circumstances.

2. SECURITY AND DATA BREACHES/CYBER ATTACKS – ARE YOU DOING ENOUGH?

APP 11.1 requires those who hold personal information to "take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss and from unauthorised access, modification or disclosure". What is less well known is that the Privacy Commissioner issued a 32 page guidance on what those 'reasonable steps' may be (see our Update on Security Obligations), which is currently being revised and updated, and that in all recent investigations compliance with APP 11.1 is being measured against the steps/measures set out in that guidance.

At least 50% of the steps/measures detailed in the guidance will come as a surprise to most businesses and, yet, failure to have implemented/addressed them will likely mean you are in breach of APP 11.1.

While failure to comply with APP 11.1 may be of some concern (re possible fines and a negative report if investigated), these steps/measures are also the de facto de minimis standard for cyber risk security. Therefore, failure to meet at least these minimum security standards will likely mean that, in the event of a cyber event/loss or theft of information, the company will be considered to have failed to implement appropriate security measures or adequately address the risks and will expose itself to potential consumer and/or shareholder actions (eg as with the recent Target case in the US).

As discussed at the recent DLA Piper and Aon "National Network Security & Privacy Symposium", cyber risk management is now squarely a Board issue and failure to plan for it/address it (including meeting the basic security standards under APP 11.1/the Commissioner's guidance) will breach the duty of care of the directors, opening the directors up to personal liability for resulting costs to the company, damages to individuals and any adverse movement in the share price (for listed entities). For more information on cyber risk and directors duties, click here.

1. DE-IDENTIFICATION/DESTRUCTION OF PERSONAL INFORMATION AFTER USE FOR THE NOTIFIED PURPOSES – THAT'S ONLY A GUIDELINE, RIGHT?

The issue of data retention is a hot topic. APP 11.2 requires you to take reasonable steps to destroy or de-identify personal information that is no longer needed for the notified purpose(s) for which it was originally collected, unless certain limited exceptions apply (including where that organisation must retain the information under an Australian statute).

Please see our Privacy Updates "Australian businesses must destroy or de-identify personal information no longer needed for the purpose(s) authorised" and "What do death, taxes and deactivated online accounts have in common?" for more information on the obligation under the Privacy Act to destroy or de-identify personal information.

In summary, you do not have the right to keep personal information forever (or use it for purposes other than which are permitted under the APPs and notified at or prior to collection). Organisations must ensure that there is a system or process in place that routinely identifies personal information that should be destroyed or anonymised.

This has caused the most concern in practice as it usually is the most expensive and disruptive change to implement, usually requiring document retention policies, internal processes and IT infrastructure to be altered to accommodate the de identification/destruction of personal information in accordance with APP 11.2.

PREDICTIONS FOR THE NEXT 12-24 MONTHS!

While not prevalent enough to secure a spot in the Top 5, yet, two areas where we are seeing increasing privacy related issues and which we predict will become bigger issues over the next 12 to 24 months are: (i) Big Data and (ii) facial recognition.

(i) Big Data: Use of Big Data analytics by Government agencies and across all industries (in particular retail) is, as its cost diminishes and the available data sets increase, growing significantly both in actual use and the number of clients that are considering the use of Big Data analytics in the next 12 months. As noted in our earlier Update, our recommendation to those considering Big Data projects is to consider privacy issues and design for privacy compliance from the beginning of the project. This will be significantly more cost effective than "reverse engineering" in privacy requirements at the end of the project (or after being investigated and told what you need to do by the Privacy Commissioner).

(ii) Facial recognition: Facial recognition, likewise, is becoming of more interest as the cost of it drops significantly and as more and more products come onto the market. While it may initially appear not to have a wide application or be of much interest to private businesses, given the prevalence of CCTV infrastructure in our cities and the drive to differentiate oneself in the market (by individualised customer service at no additional cost), we have already advised on a number of early stage/exploratory projects in this space for our clients. We expect this interest to continue to grow over the next 12 to 24 months. Watch this space!

DLA Piper has a world–wide team of over 130 privacy and data protection lawyers, ranked Number 1 Globally by Legal 500.

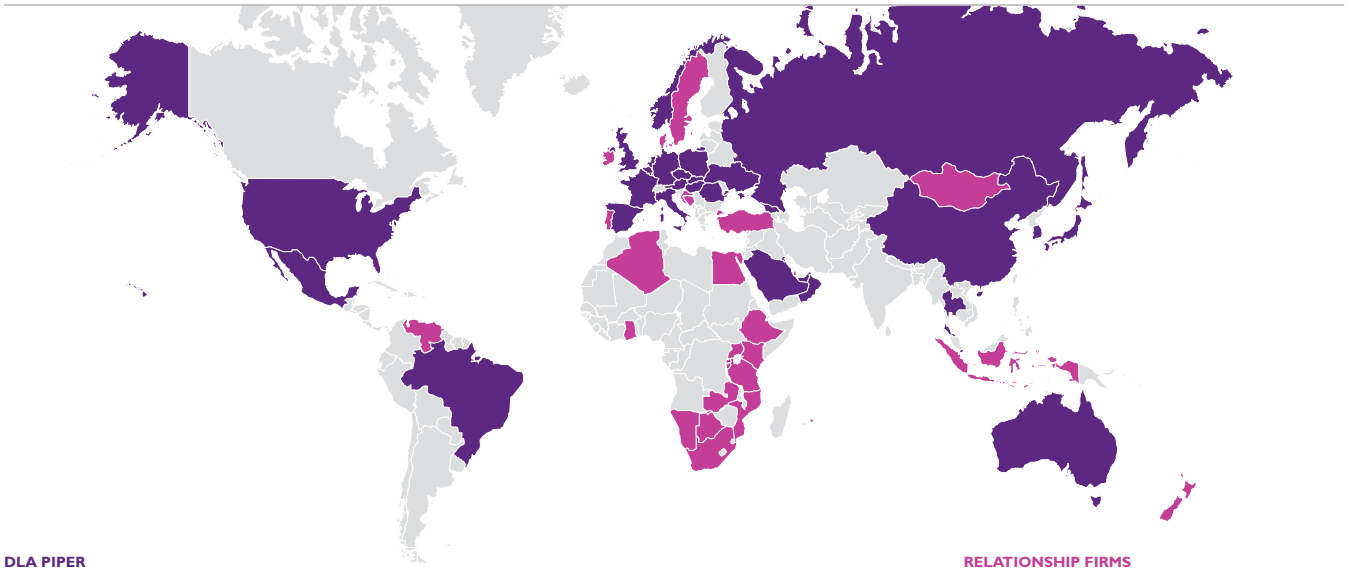
Our team members work together every day to help businesses like yours make the right decisions about how to implement privacy and data protection compliance solutions in the most practical and cost effective way.

Please click here to download our Global Data Protection Laws of the World, covering the data protection laws of 70 different countries.

MORE INFORMATION

For more information on privacy in Asia and Australia, please do not hesitate to contact Alec or any of our dedicated privacy team:

Alec Christie
Partner, Sydney
T +61 2 9286 8237
alec.christie@dlapiper.com



DLA PIPER

AUSTRALIA
Brisbane
Canberra
Melbourne
Perth
Sydney

AUSTRIA
Vienna

BAHRAIN
Manama

BELGIUM
Antwerp
Brussels

BRAZIL
São Paulo

CHINA
Beijing
Hong Kong
Shanghai

CZECH REPUBLIC
Prague

FRANCE
Paris

GEORGIA
Tbilisi

GERMANY
Berlin
Cologne
Frankfurt
Hamburg
Munich

HUNGARY
Budapest

ITALY
Milan
Rome

JAPAN
Tokyo

KUWAIT
Kuwait City

LUXEMBOURG
Luxembourg

MEXICO
Mexico City

NETHERLANDS
Amsterdam

NORWAY
Oslo

OMAN
Muscat

POLAND
Warsaw

QATAR
Doha

ROMANIA
Bucharest

RUSSIA
Moscow
St. Petersburg

SAUDI ARABIA
Riyadh

SINGAPORE
Singapore

SLOVAK REPUBLIC
Bratislava

SOUTH KOREA
Seoul

SPAIN
Madrid

THAILAND
Bangkok

TURKEY
Istanbul

UKRAINE
Kyiv

UNITED ARAB EMIRATES
Abu Dhabi
Dubai

UNITED KINGDOM
Birmingham
Edinburgh
Leeds
Liverpool
London
Manchester
Sheffield

UNITED STATES
Albany
Atlanta
Atlantic City
Austin
Baltimore
Boston
Chicago
Dallas
Houston
Los Angeles
La Jolla
Miami
Minneapolis
New York
Northern Virginia
Philadelphia
Phoenix
Raleigh
Sacramento
San Diego
San Francisco
Seattle
Short Hills
Silicon Valley
Tampa
Washington, DC
Wilmington

RELATIONSHIP FIRMS

ALGERIA
Algiers

BOSNIA-HERZEGOVINA
Sarajevo

BOTSWANA
Gaborone

BURUNDI
Bujumbura

CROATIA
Zagreb

DENMARK
Copenhagen

EGYPT
Cairo

ETHIOPIA
Addis Ababa

GHANA
Accra

INDONESIA
Jakarta

IRELAND
Dublin

KENYA
Nairobi

MAURITIUS
Port Louis

MONGOLIA
Ulaanbaatar

MOZAMBIQUE
Maputo

NAMIBIA
Windhoek

NEW ZEALAND
Auckland
Wellington

PORTUGAL
Lisbon

RWANDA
Kigali

SOUTH AFRICA
Cape Town
Johannesburg

SWEDEN
Stockholm

TANZANIA
Dar es Salaam
Mwanza

TURKEY
Ankara

UGANDA
Kampala

VENEZUELA
Caracas

ZAMBIA
Lusaka

CONTACT YOUR NEAREST DLA PIPER OFFICE

BRISBANE

Level 29
Waterfront Place
1 Eagle Street
Brisbane QLD 4000
T +61 7 3246 4000
F +61 7 3229 4077
brisbane@dlapiper.com

CANBERRA

Level 3
55 Wentworth Avenue
Kingston ACT 2604
T +61 2 6201 8787
F +61 2 6230 7848
canberra@dlapiper.com

MELBOURNE

Level 21
140 William Street
Melbourne VIC 3000
T +61 3 9274 5000
F +61 3 9274 5111
melbourne@dlapiper.com

PERTH

Level 31, Central Park
152 – 158
St Georges Terrace
Perth WA 6000
T +61 8 6467 6000
F +61 8 6467 6001
perth@dlapiper.com

SYDNEY

Level 22
No. 1 Martin Place
Sydney NSW 2000
T +61 2 9286 8000
F +61 2 9286 4144
sydney@dlapiper.com