Roundtable to mark 30th Anniversary of the OECD Privacy Guidelines

Notes for remarks by Malcolm Crompton, Information Integrity Solutions Pty Ltd and Privacy Commissioner of Australia 1999-2004

OECD

Paris, 10 March 2010

Introduction

I have been asked to speak about an example where the OECD Guidelines were once again used as a benchmark in drawing up a privacy framework. The example is the Privacy Framework developed by the Asia Pacific Economic Cooperation forum (APEC). This Framework was drawn up by a specially convened Data Privacy Subgroup starting in 2003 and endorsed in final form by APEC Ministers in 2005.

As such, it is one of the more recent privacy frameworks that have been drawn up and certainly the most significant recent framework that spans more than one economy.

It is remarkable for an economic grouping as diverse as APEC to agree on something as potentially contentious as a Privacy Framework in such a short time. The 21 Members of APEC, after all, produce something like half the World's exports; include the World's largest economy (the USA) as well as some economies with very low levels of GDP per head; include about a third of the World's population including the World's largest population in a single economy (China); the World's two largest geographies (The Russian Federation and Canada) and a cultural diversity that reflects almost the full range available on the planet with the exception of Africa.

This achievement reflects considerable goodwill among a dedicated group of people who knew that something had to be done and could be done. The group comprised both government policy makers, privacy law enforcement officers and a range of non government interests. But one person in particular stands out: Peter Ford, an Australian official who took it upon himself to take in the full variety of views and turn around redrafts at an incredible pace (often within 24 hours) so that everybody could feel they had been heard yet ensure that the process did not lose momentum.

'The APEC way', but drawing on the OECD guidelines

It should be noted that the Data Privacy Subgroup deliberately considered the option of simply adopting the OECD Guidelines. However, it decided not to do so, even though the objective of drawing up the APEC Privacy Framework was to facilitate the growth of eCommerce in the region: an objective that is remarkably similar to the objective of the OECD Guidelines, which was to reconcile privacy and the free flow of information, particularly transborder flows of personal data.

The reasons for taking this approach were essentially twofold. As I learnt from phoning around my colleagues in the region, the most deeply felt was that officials wanted to think through the issues

'the APEC way' rather than with little insight adopt a framework that was seen as having been developed a long time ago, in a far off environment. But it was also felt that the Subgroup should take the opportunity specifically to test whether the OECD Guidelines, 25 years on, had stood the test of time.

The result: a refreshed Framework whose roots in the OECD Guidelines is obvious

When you read the APEC Framework carefully and dispassionately, it is possible to see each of the OECD Guidelines reflected in the Privacy Principles that comprise the Framework.

Again this is no accident.

The diversity of the Subgroup included members steeped in the OECD Principles who in a quiet and deliberate way made sure that the Subgroup consciously addressed each of the OECD basic Principles and decided if and how to address them in the APEC Framework. Blair Stewart, the Assistant Privacy Commissioner of New Zealand in particular took up this responsibility along with officials from Hong Kong. The shaping of the Framework reflects their input very significantly.

The major challenges facing privacy protection today and how the APEC Framework responds to them: evolution from the OECD Guidelines

Over the last few years, a surprisingly rapid consensus has emerged that the way we have gone about protecting privacy through privacy frameworks, including in the statutes, is suffering from at least two challenges.

The first of these is that the concept of individual participation has led to an over reliance on the individual to understand what is happening to personal information about them; make informed decisions that require an impossibly clear view of the future; and when they feel something has gone wrong, carry too much of the load in seeking and gaining enforcement. In the US, this has been explicitly acknowledged by the current Chairman of the Federal Trade Commission who considers that 'Notice and Choice' is a failed model. Many enforcement regimes depend excessively on ex post complaint by the aggrieved individual rather than clear ex ante governance and assurance processes. Leading thinkers and policy makers on both sides of the Atlantic and elsewhere have expressed views such as these in their own way.

The second is related to the first: far too much effort has gone into writing the perfect set of principles (leading to an incredible array of nearly-the-same frameworks that diverge sufficiently to make genuine compliance a nightmare for an organisation operating in more than just a few jurisdictions). By comparison, not enough effort has been put into effective governance and enforcement.

Of these developments, the OECD has already recognised the second and put increased focus on understanding the state of play with privacy law enforcement, especially cross border cooperation, and facilitating improvement. This work started with the "Report on the Cross-Border Enforcement of Privacy Laws" in 2006 and subsequently led to work including the "OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy".

We may well see the OECD address both of the challenges as it reviews the Guidelines over the next year or so.

APEC has had a very clear focus on addressing the enforcement and assurance challenge. It has gone about it in a number of ways. It started with the construction of the Privacy Framework itself, which it has then backed up by a very strong focus on implementing the Framework.

This approach is based on two especially important principles APEC Privacy Framework, one new and one not so new but until recently given very little emphasis.

The first of these two principles is Information Privacy Principle I in the APEC Framework: Preventing Harm. This is the new Principle. It started life as a very controversial concept but has since not only been accepted but also adopted by privacy regulators elsewhere.

Principle I in short emphasises that the regulatory effort should focus on the most harmful. It does not imply that less harmful privacy impacts should be ignored.

As such, it is simply a statement of common sense. Privacy law enforcement bodies, like all other organisations but especially regulators are heavily resource constrained and so need to be strategic in the application of those resources that are at their disposal.

Applied well, Principle I can lead to dramatic improvement in compliance with any set of privacy principles.

The second of the two principles is Information Privacy Principle IX, the Accountability principle. It is very recognisable from the corresponding basic Principle in the OECD Guidelines. It is worthwhile quoting both in full. APEC Information Privacy Principle IX states that:

> "A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles."

The OECD equivalent is in Paragraph 14 of the Guidelines. It provides that:

> "A data controller should be accountable for complying with measures which give effect to the principles stated above".

This is elaborated in the Detailed Comments on Paragraph 14 in the Guidelines which state that:

> "it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation merely because the processing of data is carried out on his behalf by another party, such as a service bureau".

Along with wording in Part B of the APEC Privacy Framework that exhort economies to work on cross border cooperation, APEC Information Privacy Principle IX has been the basis of a concerted effort in a so-called APEC Pathfinder project to develop a complete process for ensuring the safety of personal information when it moves across borders.

While this is a work in progress, it has already resulted in the only cooperative arrangement for the enforcement of a privacy framework outside the unique treaty arrangements of the European Union. The APEC Cooperation Arrangement for Cross-Border Privacy Enforcement has been finalised and was endorsed by APEC Ministers at the end of 2009.

Other far sighted elements in the Pathfinder include ways of bringing non-government accountability agents into the framework to provide a first line of assurance and enforcement in the handling of personal information. This has huge potential to allow the scarce resources of government funded accountability agents, including privacy commissioners and consumer affairs regulators, to focus on the most difficult and harmful in much the same way as has been in place for decades for the governance of financial information.

Concluding remarks

The work by APEC has been a very significant and recent effort. It has put the OECD Guidelines of 30 years ago to the test in a particularly diverse and challenging environment.

The verdict is clear from the APEC experience: the OECD Guidelines have stood the test of time remarkably well. The most significant changes from one framework to the other appear to be changes in emphasis rather than any requirement for radical change.

The biggest difference has been the renewed focus on effective governance and enforcement.

However, I would suggest that both frameworks are already facing further challenge.

The first derives from one of the challenges identified earlier: how to ease the decision making and enforcement burden on the individual. Will we find a way to 'automate' the management of personal information so that most individuals feel comfortable with the approaches being taken by the organisations around them, only needing to exercise their rights of individual participation on an exceptions basis? Will this flow from the 'privacy by default' and 'privacy by design' concepts that have been discussed recently?

The second is the only true breakthrough in developing privacy frameworks (as opposed to addressing governance and enforcement) since the OECD Guidelines were first promulgated: data breach notification. The impact of this new concept has really only been realised since the APEC Privacy Framework was adopted. The custodians of both Frameworks will need to consider whether to incorporate data breach notification. The custodians of other significant privacy frameworks, have already begun to do so including the Privacy Act in Australia and the EU Directive.

I congratulate the OECD and the authors of the Guidelines for their foresight so many years ago.