Why the APEC Privacy Framework is unlikely to protect privacy

Dr Chris Pounder

The APEC Privacy Framework has been put forward as a foundation on which to build a global privacy framework. The lack of detail in the Framework makes it a shaky foundation that risks creating national privacy laws and rules that would be inconsistent with each other and far weaker than Europe's traditional approach to the subject. So argues Pinsent Masons' Dr Chris Pounder, editor of Data Protection Quarterly.

Dr Pounder's analysis follows. It is aimed at those already familiar with Europe's data protection regime. It was published on 15 October 2007 at Out-Law.com[1].

Introduction

In September 2007, Google's Global Privacy Counsel endorsed[2] the Privacy Framework published in 2004 by the Asia-Pacific Economic Community (APEC), describing it as "the most promising foundation on which to build."

"Surely, if privacy principles can be agreed upon within the 21 APEC member economies, a similar set of principles could be applied on a global scale," wrote Peter Fleischer in the search giant's Public Policy Blog.

APEC is a forum for facilitating trade and investment in the Asia-Pacific region. Its members include Australia, Canada, China, Japan, Vietnam, the Russian Federation and the US. The Framework, when implemented by APEC member states, is intended to provide a legal basis for facilitating international transfers of personal data and at the same time providing a minimum standard of privacy protection.

This analysis shows that the APEC Privacy Framework[3] (40-page / 194KB PDF) is missing a great deal of data protection detail.

In the absence of this important detail, the Framework:

- is unlikely to provide an adequate level of protection as required by the European Data Protection Directive;
- is likely to result in inconsistent implementation by APEC member states and a confused hotchpotch of national data protection laws, regulations or rules;
- is likely to be policed by a very weak regulatory regime;
- is likely to allow member states to adopt divergent policies on important privacy aspects with the result that the Framework is unlikely to provide a sound, long-term, basis for the international trade in personal data; and
- contains principles and procedures which could be implemented in a way that results in an unacceptable or minimal level of protection for personal data.

[1] http://www.out-law.com/page-8550
[2] http://googlepublicpolicy.blogspot.com/2007/09/call-for-global-privacy-standards.html
[3] http://www.ministerjusticeandcustoms.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf

Caution needs to be exercised when discussing the likely deficiencies in the APEC Privacy Framework. The Framework's principles were drafted in order to get agreements between diplomats – and diplomatic agreements tend to fudge important issues. The result is that the principles are ambiguous as to their effect and are capable of a vast number of interpretations and implementations.

It is possible that an APEC member state, for example, Australia or New Zealand, could develop rules compliant with European Directive standards. But other member states could use the Framework's flexibility to implement a minimalist approach to privacy compliance that falls very far short of what would be deemed "an adequate level of protection".

Overview of the APEC Privacy Framework

The APEC Privacy Framework comprises a set of nine principles that apply to "personal information" (equivalent to "personal data" as defined in the UK's Data Protection Act) about a living individual (equivalent to "data subject") processed by a "personal information controller" (equivalent to "data controller") and infers the existence of "data processors". To avoid confusion and because the Framework's definitions are so adjacent, the rest of the analysis uses the UK definitions wherever possible, as these are more familiar to OUT-LAW readers. Like the OECD Guidelines[4], implementation of the APEC framework is not mandatory; China for instance, has indicated that it will have nothing to do with them.

Some of the Framework's principles overlap with the thrust of the UK's data protection principles (though there are a significant differences), and the principles are enforced by a diffuse regulatory framework based around a consensus view as to what the data protection standard should be. Such standards will emerge from discussion and debate between APEC member states, no doubt with input from data protection experts. There is a requirement to establish an enforcement mechanism, but this can be very low key, and there is no requirement to establish a Privacy Commissioner, although member states can do so if they want.

The data protection principles are drafted as a number of general objectives which are capable of diverse interpretations. The principles relate to: preventing harm to data subjects; provision of a notice; limitation on collection of personal data; limit on the uses of personal information; individual choice over use and disclosure; maintaining the accuracy and integrity of personal information; security safeguards; access and correction; and accountability via a regulatory framework. These headings are unremarkable – unlike the detail that is underneath each heading.

The APEC Privacy Framework is unlikely to offer 'adequate' protection

The Data Protection Directive restricts transfers of personal data to third countries where the destination country fails to ensure an 'adequate' level of protection. So can the principles proposed by the APEC Privacy Framework be used as a basis for assessing the adequacy of protection offered by a Third Countries?

[4] http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

Although the principles dealing with security and accuracy are broadly equivalent to the Directive's provisions, other **aspects of the Framework's principles are likely to be deficient**. Indeed, it could be argued that, without further clarity or detail, the deficiencies have the potential to be so great, that the adoption of the APEC Privacy Framework as an international standard could create significant risks to personal information about private and family life, and thereby undermine international trade.

There are several areas where significant deficiencies from the Directive standard can be anticipated. For example, the Framework defines a subset of personal data as being "publicly available personal information" (e.g. information published by the media or put into the public domain by the data subject) and states that these personal data are subject to minimal protection.

This is plainly different to the approach adopted in Europe: just because information is in the public domain (or has been in the public domain) does not mean that the personal data are unprotected.

On the other hand, it has to be recognised that the APEC Privacy Framework represents a **significant step forward in privacy protection** – as many Asian countries are not fully developed in their democratic structures and some Asiatic national governments contain a strong authoritarian streak. Some privacy progress in these states is better than no progress. In this context, the Privacy Framework is an important step forward. However, acknowledging that some countries are making a step forward has to be accompanied by recognition that the Framework could allow the taking of steps in the opposite direction.

The Principle of Harm

The first APEC Privacy Framework Principle states that the data protection rules should focus on the "harm" that the processing of personal data can cause and that remedies available to data subjects should be proportionate to the misuse of personal data or wrongful collection of personal data.

If the Harm Principle merely was a reference to the fact that when things go wrong, the redress available to a data subject should be proportionate to the harm caused by the processing and the severity of the breach of the principles, then one would wonder why there needs to be a Harm Principle at all.

The answer, of course, is that the Harm Principle could well intend something else. It states that "specific obligations should take account of such risk … threatened by the collection, use or disclosure of personal data".

Thus, if no harm is perceived (e.g. by Government or by data controllers), then the impact of other principles can be negated (e.g. by allowing specific exemptions or not implementing certain procedures). There is a curious side effect which illuminates the central problem to this approach: access by the data subject to his or her own personal data can be refused if there is little risk of harm to the data subject, yet the reason why the data subject might want to seek access is to find out whether the processing is causing him harm.

Those steeped in data protection history will remember that the equivalent of the "harm debate" took place in the UK some 35 years ago, well before the UK had any data protection law.

For example, the notion underpinning a "Harm Principle" was firmly rejected by the Lindop Committee in its Report on data protection in 1978 (Cmnd 7341, paras 18.24–18.27).

Lindop concluded that there was no objective standard whereby a data controller could assess harm prior to the processing of personal data because there was no way an organisation could judge whether its personal data or its processing would be sensitive or non-sensitive. This was because sensitivity was a subjective assessment that could only be accurately judged by each data subject concerned. Lindop also concluded that if the data subject assessed harm then the difference between public or private personal data, or between private and business personal data, was an irrelevance. Yet, as we shall see, the Framework makes this distinction between these types of personal data.

Lindop concluded that the only real issue was whether the data identified or related to a particular living individual and, if so, then all the data protection principles should be applied. However, having established that the principles did apply, Lindop concluded that the impact of the principles would be modified by a number of factors – for instance, whether there was foreseeable harm to the data subject, the sensitivity of the personal data, or whether the personal data were in the public domain.

This approach (that assumes the data subjects assess the potential for harm) has been adopted by most countries that have data protection law. It is the exact opposite to the Framework's approach (that suggests the principles can be dispensed with, if no harm is apparent to the data controller of the government implementing the data protection law). Of course, risk assessment tools (e.g. Privacy Impact Assessments) could be used by the data controller to reveal or quantify risks and thereby reduce harm. However, the use of such tools does not avoid the fundamental misconception underpinning a principle based on harm; it is the data subject who can accurately perceive any harm and not the data controller.

Finally, it is clear that the APEC Privacy Framework can create harm because, according to the Framework itself, "The APEC privacy framework has limited application to publicly available information" (e.g. press reports). For example, the UK policy is to protect the identity of sex offenders to ensure these individuals do not go underground and cause greater risk to children who might be abused. However, as APEC Framework permits someone to use press reports in order to compile a list of paedophiles to be posted on the internet, thus creating the risk of harm to children.

The importance of transparency

In order to make the potential for harm associated with the processing of personal data visible to the data subject, three data protection rules assume particular importance. As will be seen, the APEC Framework could further diminish these rules and thereby create a greater potential for harm to data subjects.

In general, the transparency rules require data subjects, subject to any exemption usually related to law enforcement:

- To be informed of the identity of the data controller and all the processing purposes (e.g. via a notice) so that the complete nature of the processing and the purposes of collection, disclosure and retention become visible to data subjects. The provision of notice permits data subjects to assess risk and harm, and the requirement to obtain consent for some of the processing can be seen as guaranteeing that data subjects are fully informed and are in agreement, prior to the commencement of the processing. In addition, provision of a notice can trigger a data subject making different choices at different times.
- To be given the choice as to how their personal data are to be used, disclosed or retained, and permitting data subjects to change their mind if they have made a wrong choice. The provision of choice needs to be revocable so that data subjects can minimise the potential for harm at a different time in the future.
- To be given the right of access to the personal data being processed. This is needed to permit data subjects to resolve problems that have caused harm and the right of access to personal data is a gateway right to make the cause of problems visible to data subject.

The Notice Principle – informing the data subject

The European data protection rules require a fair processing notice to be given to the data subject before or at the time of collection of personal data from the data subject, and if the data are obtained from external sources, notice to be given to the data subject as soon as practicable. The rules also provide for a number of exclusions from providing this notice (e.g. when the data subject already is informed about the processing or when a law enforcement purpose is involved). The APEC Notice Principle provides for this option.

However, the flexibility in the drafting of the Framework's Notice Principle allows for notice to be given **after** collection of personal data from the data subject, and the Framework anticipates that the notice requirements of this Principle will be "based on a consensus among APEC member economies". This consensus could be based on commercial convenience rather than fairness to data subjects.

The Framework thus has the potential to approve consensus practices such as "telling data subjects before collection to look at a web-site for fair processing detail" and allows updates to a notice to be posted on a website, intranet sites and employee handbooks. In this way, the procedures that deliver a data subject with a notice could become **separate** from procedures that collect personal data from a data subject (e.g. when an application form is completed by data subjects at time of collection).

Additionally, the Framework's Notice Principle might not apply to "business contact information and other information that identifies an individual in his or her professional capacity in a business context". Similarly, the collection of "publicly available information" is unlikely to be subject to the Notice provisions.

This contrasts with European data protection standards that would require the provision of fair processing notices when the data controller needs to be fair (e.g. business contacts working in sensitive areas should be give a notice about the processing of their business-related personal data because they have security concerns which could influence their choices over that processing).

In general, the term "publicly available information" leaves a lot of detail to be filled in by member states. For example, it is clear that any details posted on a website by the data subject become "publicly available information". However, suppose that a data subject decided that details on the website should only be available to a closed set of friends; are these details also "publicly available"? Suppose someone else copies such data and posts them on another site – do these personal data become "publicly available"? The Framework is silent on this important detail.

The Choice Principle – control over use and disclosure

The Choice Principle permits data subjects to choose whether or not to permit certain uses and disclosures via an opt-out or opt-in. However, the Framework states that the Choice Principle might not apply for "publicly available information", to certain employment situations and for "business contact information" and permits a degree of "implied consent" in order to legitimise the choice. Additionally, the Choice Principle is silent on the circumstances where there is a change of mind (i.e. when one choice is replaced by another), or indeed whether a data subject can change his mind.

The Choice Principle also does not determine what choices should be offered, only that choice should be offered when it is "appropriate". As there is no discussion as to when it is "appropriate" to offer choice and when it is not, the impact of this Principle is very uncertain to say the least. As these factors are left to national implementation of the Framework, it can be anticipated that a hotchpotch of Choice procedures will be used.

The Framework is also silent as to whether the choice on offer to data subjects relates to the processing of personal data or to the service on offer.

For example, suppose a data subject wants a service and is faced with a statement "By signing up to this service, you consent to us doing X, Y and Z with your personal data". Obviously, one choice faced by the data subject is to decide not to take the service. However, in some cases, the choice that should be offered by a data controller is whether a data subject wants the processing options X, Y and Z to occur, and not whether or not to sign up for the data controller's service. The Framework conflates these two choice situations.

The Choice Principle is also silent as to whether the data subject can choose for personal data to be deleted. This option is important because there could be minimal risk at the time of collection of personal data with the risk only emerging at a later stage.

The classic example of this, discussed at the time of Lindop in the 1970s, was the compilation of names and addresses. In 1930 such a compilation by a Jew in Germany was relatively risk free – four years of political upheaval later, in the hands of the Gestapo, such a list was an immense danger to those on it.

This issue is very relevant to the internet as personal data on the web could well be accessible for decades ahead, for any purpose, by any person. In such circumstances, it is easy to see how "harmless" personal data processed now could easily become "harmful" data on this time scale.

A flexible Use Principle

The Use Principle could easily relax the finality principle which aims to prevent personal data being processed for another incompatible purpose.

The Use Principle of the APEC Framework states that personal data can be used "only to fulfil the purposes of collection and other compatible or related purposes". So, instead of a prohibition on the processing of personal data for an incompatible purpose (as in, for example, the Second Data Protection Principle of the UK's Data Protection Act), the APEC Framework gives permission to use personal data, without data subject consent, for "compatible or related purposes".

So what is meant by a "related purpose"? Clearly a "related purpose" has to be different to a "compatible purpose" because there would be no need to use the phrase "compatible or related purposes" in the Framework's text. One plausible reason for the inclusion of the words "related purpose" is that the Framework attempts to narrow the scope of an "incompatible purpose" to those purposes that cannot be "related to" the purpose of collection. In this way, one can expect many commercial purposes will automatically become "compatible" purposes and legitimised without the need to obtain consent of the data subject.

There is no principle requiring a data retention policy

In general, the Framework contains no obligation to delete personal data whose retention is no longer justified and the absence of any obligation for data controllers to adopt retention criteria is a curious omission.

Individuals can gain deletion on a case-by-case basis via the Access Principle (e.g. show that personal data are so out of date that they should be deleted) – but this is applied on an individual basis and cannot be a substitute for a general principle that would require data controllers to devise general retention policies that apply to the personal data they process.

It could be that the Framework considers that it is obvious that if a data controller has no further use for the personal data, then the data will be destroyed. But years of data protection experience in Europe shows that most data controllers can always argue that because their personal data assets might be used, the data should be retained. That is why, when left to their own devices, many data controllers determine overtly long periods for personal data retention.

The access and rectification Principle

Access to all the personal data processed by a data controller is subject to exemptions not found in the UK's data protection law or the Directive.

For example, access and rectification can be refused if "the burden or expense of doing so would be unreasonable or disproportionate to the risks to individual privacy" or in order to "protect confidential commercial information" or if release would "compromise security".

There is also a general exemption if release of personal data to the data subject would violate another law. Finally, access can be refused if "the information privacy of persons other than the individual would be violated" (my emphasis). The use of 'persons' rather

than 'individuals' in this context means that the exemption from the right of access can extend to any personal data a company or corporation considers 'private'.

A warning from history

Many observers, including some European Data Protection Commissioners, have commented that the Data Protection Directive is too prescriptive and inflexible. However, one of the reasons for this prescription arose because Member States of the European Union had different interpretations of Council of Europe Convention No. 108, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[5]

This divergence in turn arose because Convention No. 108 was drafted in general terms (but is far more detailed than the APEC Privacy Framework) with the result that European states took different views of the specific nature of the Convention's data protection obligations.

The result was that Europe's Member States went 'off on a frolic of their own' with respect to the implementation of Convention No. 108. The consequence was a detailed specification of common data protection standards and a Directive that needed to identify precisely where harmonisation was needed.

Because the APEC Framework is far more general, there is a risk that history will repeat itself – i.e. there will be diverse implementations by APEC member states. Thus if the APEC Framework is to become a global standard (and avoid the problems that afflicted the implementation of Convention No. 108), it follows that **there needs to be far more clarity as to how the Framework is to be implemented**.

The missing detail as to the data protection and privacy requirements that have been outlined above should be specified prior to implementation by an APEC member state of its data protection regime.

If this clarity or detail fails to materialise, then the APEC Privacy Framework might still become a global standard. However, it will be a standard that is at risk of describing a global privacy fig leaf, and one which has, in the long term, the potential to undermine the international transfer of personal data between APEC's economies, if data subjects lose trust in the protection it affords.

Some speculation on privacy politics – US-style

The elephant in the room is the US. If, as with the Notice Principe, the correct data protection procedures are to be "based on a consensus among APEC member economies", one wonders when reaching this consensus, whether each country's opinion will carry equal weight? Will the USA and Vietnam be equals?

Also, when it comes to privacy protection, it is intriguing to note that the USA and China could have the same political interests albeit for different reasons: one will want to minimise the burdens on business, the other will not want privacy protection for its

[5] http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm

citizens. If this convergence of interests arises, one can easily see APEC's privacy politics being dominated by a Faustian agreement between these two strange bedfellows.

The backdrop to the APEC Privacy Framework should also recognise that there is an emerging privacy debate in the US.

Given that the wording of the principles of the APEC Privacy Framework has a passing resemblance to the privacy principles of Safe Harbor, or in the OECD Guidelines, or the principles promoted by the USA's Federal Trade Commission, it is clear that the APEC Principles (or something like them) could become the favoured way any future US Administration might choose to counter any idea that the Data Protection Directive (or something like it) should become the international standard of data protection. Any US Administration, after all, will want corporate America to lead its charge into a global information economy using flexible privacy rules that are to its liking.

If Google, Microsoft, Yahoo! and other key players in US business said to their politicians in one collective voice: "we can live with the APEC standards" then one suspects that some Presidential hopefuls would willingly accept the deal. One reason for this is that in the post 9/11 era, most politicians in the US are aware that something needs to be done about privacy but don't want to be accused by their opponents of putting privacy ahead of homeland security. APEC's Privacy Framework could become the embodiment of that 'something to do about privacy'.

Comments: chris.pounder@pinsentmasons.com