APEC PRIVACY FRAMEWORK
JUNE 2005
DOMESTIC IMPLEMENTATION

Peter Ford

Introduction

The completion of the APEC Privacy Framework is a significant achievement of which the ECSG is justly proud. Its implementation will be a more difficult task but one that is well within the capabilities of all economies. Its domestic implementation by APEC economies in a reasonably consistent manner, while allowing for the particular circumstances of each economy, is also a goal that is well worth the effort.

The changed landscape

Two major changes from the environment of the last century are recognised, or are implicit, in the language of the Framework. The first is the necessity for the free flow of information over electronic networks if the benefits of electronic commerce are to be fully realised. The second is the very different security environment for all economies following the events of September 11, 2001 and subsequent incidents.

Principle 1 – **Preventing Harm** - departs from previous statements of privacy principles in that it immediately focuses attention on the underlying objective of protecting personal privacy. While it might be argued that this objective is already obvious, its express inclusion here underlines the need to ask, in applying the principles: 'what is the harm that is to be avoided?'

The Preamble to the Framework notes that it was developed in recognition of the importance of, among other things:

- 'recognizing the free flow of information as being essential for both developed and developing market economies to sustain economic and social growth;'

Further elaboration is provided in paragraph 29 of the Framework.

We live in the fastest growing and most diverse region in the world. Electronic commerce is playing a large part in this growth and has the potential to play an even larger part in the future. The diversity of the region is recognised in the Framework itself. In particular, paragraph 12 of the commentary notes that it is not essential for electronic commerce that all laws and practices within APEC be identical in all respects. It then states that the principles take into account social, cultural and other differences among economies and 'focus on those aspects of privacy protection that are of the most importance to international commerce.

The particular focus of the Framework is electronic commerce. There have been many surveys showing that consumers are concerned about their online privacy and the security of electronic systems. It has been argued that the widespread distrust of existing privacy intrusive practices inhibits the growth of electronic commerce[1]. Although participation in electronic commerce has grown significantly in recent years, an effective program to address privacy concerns would open the way for strong growth in participation rates. Moreover, the competitive advantage that can be obtained through enlightened privacy policies is increasingly being recognized by leading global companies, at least in the financial services sector.[2] Within APEC economies, awareness of privacy issues is already at a high level and is growing rapidly.[3]

Business practices have changed substantially over the last decade to adjust to technological developments and are continuing to evolve. Privacy policy occupies a central place in the growth of electronic commerce and is given considerable attention in business practices.

Addressing concerns of all stakeholders

Almost everyone has a stake in privacy policy. Obviously, consumers are concerned to protect their personal information and business must be sensitive to the concerns of its customers. Governments have broad responsibilities for the social and legal environment in which commerce takes place, for encouraging electronic commerce and for safeguarding security, including law enforcement, within their societies.

The events of September 11, 2001 brought about profound changes in security policies in all societies, not just that of the United States, which was, of course, the immediate target. Counter-terrorism arrangements now occupy a much more central place in government and there is a much higher premium on measures to identify emerging threats so as to prevent their realisation and a much broader scope to security measures themselves.[4] The implications for privacy policy are that it is not enough to consider only the scope of particular exemptions for law enforcement and security agencies to privacy principles. It is now more important than ever before to consider the impact and scope of security and law enforcement arrangements on privacy protection. Privacy advocates may, of course, legitimately seek to influence public opinion to minimise the incursion of such arrangements on privacy law but should understand that government decisions may be influenced by many other

---

1 Recent studies include:
"Attitudes and Behaviors of Online Consumers: A Study of five Cities", M. Rivera Sánchez (National University of Singapore), online at: http://26konferencja.giodo.gov.pl/data/resources/RiveraSanchez_pres.pdf;
"Research into privacy attitudes in Australia" commissioned by the Federal Privacy Commissioner of Australia in 2004 and 2001, online at: www.privacy.gov.au/business/research/index.html;
"A crisis of confidence: rebuilding the bonds of trust", the Yankelovich Trust study by Yankelovich Partners, www.yankelovich.com, and available online at: www.compad.com.au/cms/prinfluences/workstation/upFiles/955316.State_of_Consumer_Trust_Report_-_Final_for_Distribution.pdf

2 "Global Security Survey 2004", p.14. conducted by Deloitte and published in May 2004; online at: www.deloitte.com/dtt/research/0,1015,sid%253D3489%2526cid%253D48978,00.html

3 ibid.

4 See, for example, 'Security Changes', The Economist, March 19, 2005, Special Report pp. 29 – 34.

considerations. Accountability arrangements are also likely to be quite separate from the general arrangements governing accountability for privacy protection.

Those with policy responsibilities for the implementation of the Framework may find it advantageous to develop effective consultative arrangements with the security and law enforcement agencies in their economies.

For these reasons, privacy policy cannot be considered in isolation but needs to take account of a range of twenty-first century problems such as identity fraud. It also needs to address the use of electronic technology to commit traditional crimes in novel ways.[5] Government responses to problems of this kind frequently take the form of legislation addressing the specific issues. Invariably, such legislation also impacts on privacy protection and privacy advocates can often contribute substantially to the formulation of solutions to these problems.

Achieving the benefits

As purchasers of the new products and services made possible through electronic commerce, consumers derive great benefits from the global flow of information. Innovative products and services are more widely available and the disadvantages for some economies of remoteness from major markets and supply centres may be eliminated or at least reduced.

To realise these benefits, however, it is necessary to identify and remove unnecessary obstacles to the further development of electronic commerce. This is a constant process and not one that can be achieved in a single step. Some of the difficulties that have been identified to date are:

- difficulties facing consumers when their privacy is infringed by an organisation located in another jurisdiction;
- difficulties for companies in having to seek approval from different agencies in a number of economies for the same proposal for information flows; and
- difficulties for companies in having to observe different privacy regimes.

The traditional approach taken by lawyers to the international movement of personal information is to analyse the law of each jurisdiction through which the information passes and ask whether it applies to the particular circumstances under review. Some commentators argue that companies should survey the law of all the jurisdictions in which they operate, or plan to operate, and adopt the highest standard in relation to each privacy issue.[6]

---

[5] Examples abound but a fairly typical case is that of Philip Cuming in the US who pleaded guilty to identity theft over the period of his employment from mid-1999 to mid-2000 by Teledata Communications Inc. Cuming obtained client passwords and codes that enabled him over a three year period to download and on-sell credit reports of more than 30,000 people, causing losses of more than US$50 million. See Privacy Law Bulletin, (LexisNexis Butterworths Australia) Vol. 1, No. 4, Sep. 2004 p.66.

[6] For example, in dealing with the growth of international calling centres, Katherine Sainty and Andrew Ailwood suggest: 'In general, multinational organisations need to consider adopting privacy policies, procedures and guidelines that satisfy a "minimum highest standard of data protection on each issue".' Moreover, companies might choose to express such policies in binding corporate rules.

The need to examine the law of a multitude of jurisdictions may disadvantage not only business but also consumers in the smaller jurisdictions. This is because there may be substantial costs associated with the conduct of such surveys. Consequently, the requirement to carry them out may act as a disincentive to extending a multinational company's operations to a particular economy and an obstacle to the further development of commerce in that economy.[7]

Implementation of the Framework will result in a far less cumbersome means of assuring privacy protection.

Compatibility

The principles set out in the Framework deal with those elements of privacy policy on which there is a need for some consistency throughout the region. At the same time, they recognise the diversity among APEC economies and the different ways in which each economy may choose to address particular issues and periods within which they may choose to act. All that is sought by the principles is that degree of compatibility that will encourage the further development of electronic commerce in the region.[8]

The main options are legislation, self-regulation and some combination of the two. Several precedents are available from those economies that have implemented these or other privacy principles. If legislation is developed, to be consistent with the APEC Privacy Framework, it should embody the privacy principles that are set out in Part III of the Framework. It will be necessary to spell out the operation of those principles in some detail but the facing page commentary in Part III should prove of assistance.

Legislation generally requires some elaboration of the language of principles with specification of exceptions and detailed definitions to suit the circumstances of the society in which the legislation is enacted as well as enforcement mechanisms.

Self-regulation can take a variety of forms but an obvious one is the adoption of industry, or company, codes of practice. Such codes can specify in detail practices and procedures to take account of the particular circumstances that apply to the industry or company. They may, therefore, be more flexible and may more easily be modified than legislation but may lack the credible enforceability that is desirable as far as consumers are concerned.[9]

See 'Implications of Transborder data flow for global business', Privacy Law Bulletin, (LexisNexis Butterworths Australia) Vol. 1, No. 7, Dec. 2004/ Jan. 2005 p.101 at p.106.

[7] See paragraph 30 of the Framework which provides that all member economies should, consistent with the Framework and any existing domestic privacy laws, 'take all reasonable and appropriate steps to identify and remove unnecessary barriers to information flows and avoid the creation of any such barriers.'

[8] See paragraph 32 of the Framework which recognises that the means of giving effect to the Principles may differ among economies and even from Principle to Principle but that 'the overall goal should be to develop compatibility of approaches in privacy protections in the APEC region that is respectful of requirements of individual economies.'

[9] Useful reference material on the various forms of self regulation and self regulation good practice are online at: www.consumersonline.gov.au/content/SelfRegulation/Default.asp

A combination of legislation and self-regulation may offer the best of both worlds by guaranteeing a certain basic level of protection for the consumer while, at the same time, allowing industries or companies to modify general rules to suit their particular circumstances. One way of doing this is to legislate basic principles but allow for their displacement by codes of practice which meet certain criteria. If this option is followed, it is necessary to consider a number of questions including:

- whether to encourage the establishment of private sector enforcement agencies;

- whether codes should be able to set a lower standard in some areas provided they match the legislation in an overall way; and

- processes and criteria for approval of codes.

Flexibility

Having regard to the diversity of APEC economies, the Framework recognises that there needs to be flexibility in the ways in which the principles may be implemented. (Elaboration is provided in paragraphs 12 and 32 of the Framework.) Even apart from this consideration, flexibility in implementation arrangements was always recognised by the ECSG as a principal objective in the formulation of the Framework. Against this background, it is now time to consider how best to achieve a desirable level of consistency in implementation without constructing any bureaucratic obstacles to further economic development.

Conclusion

The changed landscape, the need to address the concerns of all stakeholders, the objective of achieving the benefits of electronic commerce and the need to achieve a measure of compatibility throughout the APEC region are all significant problems but ones on which guidance is obtainable from the Framework itself. All of these issues will be addressed in greater detail in subsequent sessions.