Session 3: Case studies on e-commerce regulation
"Privacy and consumer protection"

Ms Hilary McGeachy
Department of Foreign Affairs and Trade, Australia

As you'll be aware, information privacy and the internet have become rather topical in the last week or so. And as it happens, I'll be talking about Australia's regulatory experiences around privacy and consumer protection. We have undertaken a number of regulatory reforms in recent years to address some of the challenges created by the rapid expansion of electronic commerce. Even as I was preparing this presentation, Australia's Attorney General, the Hon Mark Dreyfus QC MP, announced an inquiry into certain aspects of privacy in the digital age. I'll talk about that a little more a later on. So this presentation is even more topical than we had envisaged.

The key point I will be making is that many of the policy issues that arise in regulating electronic commerce also arise in regular commerce. To this end, Australia takes a technology neutral approach to regulation - that is, the same principles, and regulatory rights and obligations, apply to commerce which takes place in a 'bricks and mortar' setting as it does for those transactions which take place via electronic means. However, there are some new challenges created by electronic commerce, to which public policy needs to adapt.

Australia's experience of electronic commerce is shaped by a number of factors. The Australian Government recognises the synergies between high speed broadband and cloud computing, and their potential to drive productivity and innovation across the digital economy. Last month the Australian Government released a National Cloud Computing Strategy. I've asked the Secretariat to provide a link to on the workshop webpage for those who would like to read a little more about it.

Despite the explosion of electronic commerce, we have found in Australia that Australian consumers and small businesses can be reluctant to make use of goods and services provided online. This includes cloud computing services. Some of this reluctance can be attributed to frustrations created by infrastructure limitations – that is, access to high speed internet. This is being addressed by the rollout of a National Broadband Scheme.

Another factor in the comparatively slow uptake of electronic commerce is public concern about privacy protections for personal information, and uncertainty about consumer protection for online transactions. Just today the Australian consumer protection watchdog, the ACCC, announced that over the last 12 months AUD93 million was reported stolen in internet scams. That does not include the unreported losses.

But this reluctance is not limited to commercial transactions. It also includes electronic services provided by the Australian Government. For example, the government has had to work hard to encourage Australians to make use of a new Electronic Health Record initiative, despite the obvious benefits an electronic health record brings to patients.

And so to our privacy laws. Australia's privacy regime has recently undergone a substantial overhaul. The new national privacy law, which will come into effect in March next year, is a modernised privacy framework. It applies to both public and private sector entities. It operates on a series of thirteen principles, known as the 'Australian Privacy Principles'. These thirteen principles are grouped into five categories which reflect the 'life cycle' of entities gathering, holding, using and disclosing information.

For the purposes of today's discussion, I want to focus on the principle which deals with the cross-border transfer of information. The Australia Law Reform Commission's privacy inquiry spent considerable time examining how to shape a new principle to deal with cross-border transfers of personal information. Cross-border transfers have, and continue to be, a source of considerable community concern. At the same time, the inquiry recognised that the previous approach, which prohibited cross-border transfer, subject to some exceptions, was no longer adequate. Developed in the 1980s, this approach no longer reflected the ease of, or the need for, information to flow across borders. It was an inhibitor to the modern reality of electronic commerce.

The new principle takes an 'accountability' approach to cross-border disclosure of information. Those of you familiar with APEC privacy guidelines will recognise this concept. The benefit of this approach is that it does not prevent information from being transferred. Instead, it requires government agencies and organisations to remain responsible - accountable - for the personal information that they transfer. In other words, it is a focus on the protections applied to information, not the location of that information.

The principle operates like this: before an entity discloses personal information to an overseas recipient, they must take reasonable steps to ensure the overseas recipient does not breach any of the Australian Privacy Principles (eg, collection, security, accuracy). In most cases, entities will make contractual arrangements with overseas recipients about how personal information is handled. The overseas recipient must deal with the information in a way that complies with privacy principles. However, even when an entity makes those contractual arrangements, it remains accountable for what happens to personal information that it sends overseas. The existence of a contract does not remove the accountability requirement.

There are limited circumstances in which we have applied a more liberal approach to accountability – that is, when the domestic entity is no longer held accountable for the information its has transferred. An enforceable privacy protection scheme is one such circumstance. If the overseas recipient is subject to a law or binding scheme, *and* the scheme provides privacy protections in substantially the same way as the Australian Privacy Principles, *and* there are mechanisms available to an individual to enforce that protection. In that circumstance, the responsibility for protecting personal information passes to the overseas recipient.

It is not essential that the overseas jurisdiction have an identical privacy structure to Australia in order for there to be accessible enforcement options. It should be possible for a range of dispute resolution or complaint handling models to satisfy this requirement. Informed consent is another circumstance in which the entity is released from their accountability.

We believe these privacy principles strike the necessary balance between protecting the privacy and integrity of personal information, and the promotion of technological innovation and the economic opportunities associated with cross-border data transfer.

I'll now turn to the main elements of Australia's consumer protection framework. Consumer confidence is another reason why Australians have been somewhat reluctant to embrace electronic commerce. The aim of the consumer protection framework is to provide a set of basic rights and responsibilities which allow consumers to engage confidently in the marketplace, and support them in making their own purchasing decisions. As I said at the start of this presentation, Australia's consumer law is technology neutral, and applies to online transactions

as well as physical transactions. However, there are some consumer protection issues that arise in the online environment.

In principle, consumers are entitled to the same consumer protection when they buy something online as when they buy it by any other means. However, consumers buying internationally may not enjoy the consumer protection that is provided in Australian law. Even if they are buying from a country that has strong consumer protection provisions in law, it can be hard to call on that protection from a distance.

Australia engages with a range of partner economies and forums on consumer policy and enforcement matters. We also work to improve dialogue with international counterparts to enhance information sharing. These forums include the OECD, APEC and the International Consumer Protection and Enforcement Network (ICPEN). Another way of increasing international cooperation on both consumer protection and privacy is by including these issues in trade agreements that deal with electronic commerce.

The last two weeks have thrown some of these issues into the public arena in a very stark way, including in Australia. As I mentioned at the start of this presentation, on 12 June, the Australian Attorney General announced an inquiry into the 'protection of privacy in the digital era'. This inquiry is a continuation of Australia's privacy reform process, but was also prompted by strong public concerns about the rapid growth in information technology capabilities. The inquiry will consider whether to create a right to sue for breach of privacy – a question that will need to be balanced against complex issues including the freedom of communication. The result of this inquiry is due in June 2014. I mention this inquiry as the most recent example of the public policy challenges that electronic commerce will continue to create.

The Australian Government does not see privacy and consumer protection operating in contest with electronic commerce. Rather, in our experience, it is these public policy settings which encourage the further development of electronic commerce, and cloud computing in particular. It is essential that consumers and small businesses are able make use of new technologies and services, if they truly are to be a position to benefit from the economic opportunities created by trade which occurs by electronic means. The Australian Government will need to remain alert to the need to adjust regulatory settings in order to maintain that balance. As in all services trade, having the right regulatory settings in place in the market is an important part of electronic commerce.