galexia

Australian and regional regulatory responses to the key challenges of consumer protection in electronic commerce (March 2008)

Chris Connolly, Galexia[1]

[1] Chris Connolly is a Director of Galexia – a specialist consulting firm working on e-commerce regulatory issues in Australia and the Asia-Pacific region. Chris spent ten years as a Visiting Fellow at the University of NSW Law Faculty, where he taught *E-Commerce Law and Practice* in the Masters Program. He is a former elected Chair of the Consumers' Federation of Australia. <www.galexia.com>

Email: consult@galexia.com **Web:** consult.galexia.com **Ph:** +612 9660 1111 **Fax:** +612 9660 7611
Post: Suite 95 Jones Bay Wharf, 26-32 Pirrama Road, Pyrmont NSW 2009, Australia

Document Control

Version

1.0

Date

6 March 2008

Source

The latest version of this article is available from
http://www.galexia.com/public/research/articles/research_articles-art51.html

Copyright

Contents

1. Introduction

It is common to note in the world of electronic commerce that traditional borders are meaningless and local laws and regulations are irrelevant. In the field of consumer protection in the online marketplace, surely some form of global regulation is required?

However, experience tells us that global regulation has been slow to emerge, and local and regional laws continue to play a key role in protecting consumers from the myriad risks they face when engaging in electronic commerce. When examined closely, these laws differ significantly from jurisdiction to jurisdiction. Each have their strengths and weaknesses, and navigating through the maze of different legal regimes and enforcement arrangements presents a challenge for consumers, and an opportunity for dishonest businesses.

In recent times a strong movement has emerged to harmonise laws, so that even in the absence of a global regime, the differences between local laws are minimised, offering a consistent standard of consumer protection and even reducing compliance costs for legitimate businesses. The harmonisation movement is itself broken down into 'hard harmonisation' and 'soft harmonisation' approaches, and true success stories are rare. However, harmonisation seems to present a more realistic option than a global regulatory regime.

This article examines the Australian and regional regulatory landscape for consumer protection in electronic commerce.

Although consumer protection in electronic commerce is a complex issue that requires an analysis of many cyberlaws, for ease of use this Article limits the analysis to the following laws:

- Consumer protection;
- Electronic contracting;
- Privacy and data protection;
- Spam; and
- Jurisdiction.

The article notes that a number of significant regional efforts in ASEAN, APEC and the Pacific Islands Forum (PIF) are underway to harmonise electronic commerce laws, and these may have some benefits for consumer protection. The article also notes several significant Australian developments in online consumer protection, but concludes that the key feature of the Australian regulation of consumer protection in electronic commerce is that it is unplanned, uncoordinated and ad hoc. The article queries whether Australia could do more to coordinate its own consumer protection measures, and would benefit from greater participation in regional harmonisation efforts.

2. Harmonisation

Many multi-national organisations have an interest in harmonisation projects, where attempts are made to align individual member country laws to remove unwanted gaps, overlaps and duplication. E-commerce harmonisation projects aim to increase legal certainty for parties engaged with more than one country.

Harmonised domestic legislation is designed to overcome the legal uncertainty in international e-commerce transactions where contracting parties are from different countries. A more certain legal environment will increase confidence in conducting electronic transactions, and in turn participation in e-commerce.

Some commentators have noted the inconsistencies that have started to appear in national and regional approaches to e-commerce law:

> A review of the electronic transaction legislation currently enacted or under consideration in many countries reveals that while there is agreement on where we ultimately want to go (facilitating e-commerce), there has been a divergence of approach regarding how to get there.
>
> Country legislation ranges from a minimalist approach that simply authorises the use of electronic signatures in very limited circumstances, to legislation that establishes a very formal and highly regulatory approach governing the manner in which electronic transactions and signatures may be used and e-businesses may operate. Moreover, many developing countries have yet to enact any legislation. The net result has been a variety of different rules (or an absence of rules) governing global electronic commerce. For those engaging in international e-commerce, the resulting environment is problematic at best.[2]

Most legal harmonisation projects are 'soft harmonisation' projects, in that there is no intention or requirement for countries to adopt the same (or even model) laws and regulatory systems. All that is undertaken is training and capacity development activities, to ensure a common (or harmonised) understanding of e-commerce legal requirements.

Examples of soft harmonisation projects include e-commerce law harmonisation projects in the following forums:

— **UNESCAP**
The United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP)[3] has 62 member countries. They are undertaking a soft harmonisation project called the *Technical Assistance Project on Harmonised Development of Legal and Regulatory Systems for E-commerce in Asia and the Pacific: Current Challenges and Capacity Building Needs*.[4]

[2] American Bar Association, *American Bar Association Recommendation 303*, 7-8 August 2006, <http://www.abanet.org/intlaw/policy/investment/unelectroniccomm0806.pdf>

[3] <http://www.unescap.org>

[4] <http://www.unescap.org/tid/projects/ecom04_conclu.pdf>

— **SAARC**
The South Asian Association for Regional Cooperation (SAARC)[5] has 8 member countries. They are undertaking a soft harmonisation project called *Harmonization of Ecommerce Laws and Regulatory Systems in South Asia*.[6]

— **Pacific Islands Forum**
The Pacific Islands Forum (PIF)[7] has 16 member countries and has a Cyberlaws strategy (part of the Pacific Plan) that includes the harmonisation of e-commerce laws as one of its goals. Overall, the strategy is based on soft harmonisation, although some specific Cyberlaws (e.g. Spam legislation) may be based on sample laws and subject to hard harmonisation.

There are some benefits to the 'soft harmonisation' approach:

1. There is considerable potential for integration and coordination with other regional capacity building activities, resulting in low costs and useful collaboration with regional neighbours.

2. Some assistance is already available, in the form of training materials and kits on e-commerce laws. For example UNCITRAL is developing training materials regarding the UN *Convention on Electronic Contracting*.

3. In theory, consistency in training should deliver reasonable consistency in outputs, including the laws, regulations and other aspects of e-commerce legal infrastructure.

However, in practice, consistency in training has not always delivered consistency in outputs. The UNCITRAL Model laws, for example, have been implemented very differently in numerous countries, despite the availability of capacity building assistance. ASEAN was also concerned that it would not necessarily have control and ownership of the development and delivery of training and materials, especially implementation guides that could help to ensure consistency.

Examples of hard harmonisation projects include e-commerce law harmonisation projects in the following forums:

— **ASEAN**
The Association of South East Asian Nations (ASEAN)[8] has 10 member countries. They are undertaking a major project known as the *Harmonisation of E-commerce Legal Infrastructure in ASEAN* project.[9] This is a hard harmonisation project based on formal Guidelines and implementation deadlines (the project is discussed in more detail below).

[5] <http://www.saarc-sec.org>

[6] *Harmonization of Ecommerce Laws and Regulatory Systems in South Asia*, Pavan Duggal, Advocate, Supreme Court Of India, Regional Expert Conference on Harmonized Development of Legal and Regulatory Systems for E-Commerce, 7-9 July 2004, Bangkok, Thailand. <http://www.unescap.org/tid/projects/ecom04_s3dug.pdf>

[7] <http://www.forumsec.org/>

[8] <http://www.aseansec.org>

[9] <http://www.galexia.com/public/projects/projects-ASEAN.html>

— **SADC**

The Southern African Development Community (SADC)[10] has 14 member countries. They are undertaking a hard harmonisation project based on a customised Model E-Commerce Law[11].

— **EU**

The European Union (EU)[12] has 27 member countries and has standardised domestic e-commerce legislation based on the EU *Directive on electronic commerce* 2000.[13] Despite this level of standardisation there is still some criticism that harmonisation has failed to achieve uniform results (especially in sanctions and enforcement) across all member countries.[14] The E-Commerce Directive is also currently under review[15].

[10] <http://www.sadc.int>

[11] <http://www.sadc.int>

[12] <http://europa.eu/>

[13] *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000*, 8 June 2000, <http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf>.

[14] <http://www.inderscience.com/storage/f102127691148315.pdf>

[15] <http://www.galexia.com/public/about/news/about_news-id98.html>

3. Australia

3.1. Consumer protection

In Australia, the issue of consumer protection for electronic commerce is dealt with through a mix of legislation and the development of industry codes of conduct. However, the value and relevance of these Codes of Conduct varies widely.

3.1.1. Trade Practices Act

In Australia, the *Trade Practices Act 1974* (Cth) (TPA) generally applies to corporations rather than individuals. It will apply to individuals who are engaging in interstate trade or commerce or aiding or abetting a breach of the Act by a corporation. The actions of individuals are otherwise covered by equivalent State or Territory trade practices legislation.[16]

If an organisation is incorporated in or carries out business within Australia it is bound by the trade practices legislation. Breach of the trade practices legislation by a corporation or individual may result in significant fines and in some cases criminal liability. The TPA defines a consumer as a purchaser of goods or services for less than A$40,000 or if the price exceeds A$40,000, where the goods or services are of a kind ordinarily acquired for personal, domestic or household use or consumption (section 4B).

The TPA impacts on the Internet in the following areas:

— **Implies terms and warranties into certain transactions**
The TPA implies into all consumer contracts a number of non-excludable conditions and warranties including that goods are supplied with a matching description (section 70); are of merchantable quality (subsection 71(1)); are fit for purpose (subsection 71(2)); and, any warranty of services will be rendered with due care and skill (subsection 74(1)). Any term of a contract that has the effect of excluding, restricting or modifying rights or liability under these implied terms will be void.

— **Prohibits unconscionable conduct and contracts**
Generally, unconscionable conduct occurs whenever one party to a transaction is at a special disadvantage in dealing with the other party because of illness, ignorance, inexperience, impaired faculties, financial need or other circumstances affecting their ability to conserve their own interests, and the other party unconscionably takes advantage of this opportunity (*Blomley v Ryan*).[17] Whether a Court will identify conduct as unconscionable will depend on all the circumstances of the case.

[16] See for example the *Fair Trading Act 1987* (NSW) and the *Sale of Goods Act 1923* (NSW).

[17] (1956) 99 CLR 362 at 415 per Kitto J, <http://www.austlii.edu.au/au/cases/Cth/high_ct/99clr362.html>.

— **Prohibits misleading or deceptive conduct**
With regard to the Internet, it may be misleading or deceptive conduct where a consumer is or is likely to be mislead or deceived by a statement on the website or if it is unclear when you connect from one website to another. The use on websites of internal and external links, frames, meta-tags, the location and prominence of disclaimers and content generally must not be misleading or deceptive to the extent goods or services of A are passed off as those of B. Misleading and deceptive conduct is prohibited under section 52 of the TPA. A recent example of this type of investigation is the action by the Australian Competition and Consumer Commission (ACCC) against Google Australia and Trading Post for allegedly disguising paid advertising as a legitimate search result.[18]

3.1.2. Australian Guidelines on Electronic Commerce

The *Australian Guidelines for Electronic Commerce* were released by the Treasury Department in March 2006 with the aim of enhancing greater consumer confidence in e-commerce by providing guidance to businesses on how to deal with consumers when engaged in business to consumer e-commerce.[19] It replaces the e-commerce best practice model previously released by the Department in May 2000.[20]

The Guidelines contain provisions on a number of matters including:

— Fair business practices;

— Accessibility and disability access;

— Advertising and marketing;

— Engaging with minors;

— Disclosure of a business's identity and location;

— Disclosure of a contract's terms and conditions;

— The implementation of mechanisms for concluding contracts;

— Adopting privacy principles;

— Using and disclosing information about payment, security and authentication mechanisms;

— The establishment of fair and effective procedures for handling complaints and resolving disputes; and

— The law and forum for the resolution of contractual disputes.

The Guidelines have no enforcement provisions, complaints process or administrative structure. It is yet to be adopted or implemented by any industry body. In these circumstances it is best seen as a 'virtual code', which gives some useful guidance to business, but to date provides limited consumer protection.

---

[18] <http://www.accc.gov.au/content/index.phtml/itemId/792088>

[19] Australian Government, *The Australian Guidelines for Electronic Commerce*, 17 March 2006, <http://www.treasury.gov.au/documents/1083/PDF/australian_guidelines_for_electronic_commerce.pdf>.

[20] Expert Group on Electronic Commerce, *Building Consumer Sovereignty in Electronic Commerce – A Best Practice Model for Business*, Treasury Department, May 2000.

Released at the same time as the Guidelines was a *Checklist for Business-to-Consumer E-Commerce in Australia*, which seeks to enhance business awareness of key issues to be considered when dealing with consumers through e-commerce.[21] The checklist contains a list of issues that should be considered by businesses when transacting with consumers online including that the contract terms are clear and easily accessible by the consumer and appropriate steps are taken to protect the consumer. Further details on how to implement these measures are contained in the Guideline.

3.1.3. Consumer Credit Code

The Uniform Consumer Credit Code applies to credit purchases generally, and is not restricted to electronic transactions. Consumers who purchase goods or services or other things using credit are protected under the Consumer Credit Code 1996.[22]

Despite what the title suggests, the Code actually is a legislative instrument; it operates Australia wide and each State has enacted mirror legislation (for example, the *Consumer Credit (New South Wales) Act 1995* (NSW)).[23]

The Credit Code will regulate credit transactions when a consumer uses the credit for household or domestic purposes, the period for repayment exceeds 62 days and there is a charge made for the provision of credit (for example: interest). In most cases the Credit Code regulates credit cards, home loans, personal loans and also regulates associated mortgages and leases.[24]

In 2006 the Code was amended. A new section (164A) was added providing that any credit contract, mortgage or guarantee referred to in the UCCC could be made in accordance with the electronic transactions laws of the relevant jurisdiction. Through each state's *Electronic Transactions Act* (*ETA*), electronic documents have the same legal status as their traditional counterparts, and the UCCC amendments would primarily serve to confirm this in the case of credit transactions. In Western Australia, South Australia and NSW, however, regulations currently exclude the UCCC from the effects of the *ETA*, and these exclusions would cease to operate under the UCCC amendments.

Additional consumer protection measures appear in the amended legislation, including a legibility requirement (at clause 6), and the possibility (in the inserted s 164A(3)) of excluding particular classes of transactions or information, so that these could not be handled electronically.

3.1.4. EFT Code of Conduct

The Electronic Funds Transfer Code of Conduct is the main regulatory instrument in Australia for providing consumer protection in electronic payment systems.[25] The EFT Code covers any business to consumer electronic transfer of value. Business to business electronic transfers of value will be excluded where the product being used was intended primarily for business use.

---

[21] Australian Government, *Checklist for Business-to-Consumer E-Commerce in Australia,* 17 March 2006, <http://www.treasury.gov.au/documents/1086/PDF/ecommerce_factsheet.pdf>.

[22] <http://www.legislation.qld.gov.au/>

[23] <http://www.legislation.nsw.gov.au/>

[24] More information about the Code can be obtained from its website – <http://www.creditcode.gov.au>; see also the following fact sheets – <http://www.moneymanager.com.au/tools/factsheets/credit_code.html> and <http://www.oznetlaw.net.au/facts.asp?action=content&categoryid=216> (Part B).

[25] <http://www.asic.gov.au/fido/fido.nsf/byheadline/Electronic+Funds+Transfer+(EFT)+Code+of+Conduct?openDocument>

An 'electronic transfer of value' includes coverage of credit cards in some circumstances, but not where a signature is obtained. It certainly includes EFTPOS, ATM transactions, most Internet and telephone banking transactions, direct debits and direct transfers.

Stored value products, such as electronic purses and stored value smart cards, are currently included in a separate section of the Code – Part B.

Specific requirements of the Code include:

- Terms and conditions must be provided to consumers;
- Records of transactions must be available to consumers;
- Audit trails must be kept;
- Privacy provisions mirroring federal privacy legislation for the private sector must be complied with, plus some specific EFT industry privacy guidelines; and
- Complaint investigation and resolution procedures must be in place.

Of course, the most important section of the EFT Code is the section apportioning liability for unauthorised transactions. This includes coverage of:

- Access methods;
- Security and disguise of codes;
- Contribution to loss;
- Fraud and negligence;
- Lost and stolen cards or devices; and
- System or equipment malfunction.

While the EFT Code has always been voluntary, it has been a very successful and popular code with both business and consumers and has achieved a very high rate of industry coverage.

The EFT Code is currently undergoing a major review. During this review some financial institutions have sought changes to the liability for unauthorised Internet banking transactions. Two key suggested liability reforms are the subject of current debate:

- Increased liability for consumers who fail to secure their personal computers; and
- Increased liability for consumers who respond to social engineering attacks.

Although there have been some changes in the vulnerability of Internet banking since the last review of the Code (for example the growth in social engineering attacks), there is does not appear to be any justification for changing the overall liability regime in the Code. Financial institutions remain in the best position to address security issues in Internet banking and the responsibility of consumers is already fairly addressed in the Code.

Consumers will be seriously disadvantaged if they are required to accept any additional liability resulting from malicious software attacks and/or failure to adequately secure their computer.

Some financial institutions appear to support (either through submissions to the Review or in terms and conditions) an increase in consumer liability where there is malicious software on their computer. In the absence of clear direction from the EFT Code, terms and conditions are likely to be extremely harsh for consumers. For example, one bank (Westpac) has already included a Spyware Clause in their terms and conditions:

> If you knowingly use a computer that contains software, such as Spyware, that has the ability to compromise access codes and/or customer information, you will be infringing our rules for access code security referred to above and we will not be liable for *any* losses that you may suffer as a result [emphasis added].

Enforcing such a Clause would be difficult, but its presence may be a deterrent to a consumer with a legitimate EFT complaint, if for example they believe their complaint may result in an intrusive investigation into the contents of their personal computer.

It is also difficult to envisage circumstances in which account holders have displayed such a degree of carelessness in ensuring their computer meets minimum security requirements that liability should be imposed upon them for any resultant financial loss from a malicious software attack.

In addition, the task of defining acceptable 'minimum security requirements' is problematic. Internet malware is a moving target. Security risks and technical attack vectors change. It is unreasonable to expect that end-users are aware of these risks and attacks, or that they are capable of monitoring and responding to changes. Financial institutions on the other hand have specialised security resources and processes that are dedicated to addressing these risks.

It would appear more practical and economically efficient for measures to be implemented at the financial institution end since the protection afforded would then diffuse from a central point to the entire base of consumers utilising Internet banking services. Moreover, many of the developments in security in recent years would not have occurred if the security effort was more diffuse – i.e. in the hands of consumers rather than financial institutions.

Also, the current liability regime for unauthorised transactions should not be modified so as to expand the situations in which account holders will be liable for financial losses flowing from phishing attacks. It is financial institutions who should bear the primary responsibility for implementing solutions to combat forms of online fraud including deception-based phishing attacks.

There are a host of potential solutions that are available to financial institutions to combat phishing and other attacks their customers may be subjected to online. These include:

— **1.** Two Factor Authentication Solutions; and

— **2.** Website Authentication Solutions which can be installed at either the server (financial institution) or client end.

Two-Factor authentication refers to the use of a dual-layered approach in order to verify the identity of an end-user to a server. For example, an end-user may be required to supplement a password they have memorised (something they know) with something they have (such as a hardware token that produces a random sequence of digits at pre-determined intervals) or something they are (such as a fingerprint or other biometric data).

Two-factor authentication generally represents the limits of what financial institutions in Australia are currently implementing in response to online fraud such as phishing attacks. However, the technology provides only marginally improved resistance against phishing attacks.

There is, for example, a significant possibility that the passcode displayed to a bank's customer by their hardware token can be intercepted through the use of a spoofed website designed to falsely appear to belong to the customer's financial institution. The website, if a convincing spoof, could cause the customer to provide the passcode displayed on their hardware token. The fraudulent party who created the spoofed website could then immediately use the passcode to login to the customer's account as part of a replay attack (assuming they also know the customer's password and username details). An example of this has occurred recently when account holders with Dutch bank ABN Amro had money stolen from their accounts by fraudulent parties using this very method to circumvent the bank's use of two-factor authentication.[26]

3.2. Electronic contracting

3.2.1. Australian Electronic Transactions Act(s)

In Australia, the electronic contracting issues are covered by the *Electronic Transactions Act* 1999 (Cth)[27] (ETA). The ETA states that transactions taking place under a law of the Commonwealth will not be invalid just because they are completed electronically.

The ETA is based on two principles:

— **1. Functional equivalence**
Paper documents and electronic transactions are treated equally by the law.

— **2. Technology neutrality**
The law does not discriminate between different forms of technology.

The ETA provides a legal framework for electronic contracting. The Act is technology neutral in that it enables electronic transactions to occur without prescribing the use of particular types of technology. The key sections are:

— **Section 8 – General**
A transaction is not invalid because it took place wholly or partly by means of one of more electronic communications.

— **Section 10 – Signatures**
If the signature of a person is required, that requirement may be met by use of an electronic method (subject to certain additional conditions).

— **Section 11 – Documents**
A person can produce a document in the form of an electronic communication where other laws require the production of a paper document.

— **Section 12 – Records**
If a person is required to record or retain information or documentation in writing, that requirement can be met by retaining or recording the information in electronic form.

[26] Out-Law.com, *Phishing attack evades ABN Amro's two-factor authentication*, 18 April 2007, <http://www.out-law.com//default.aspx?page=7967>.

[27] <http://scaleplus.law.gov.au/html/pasteact/3/3328/top.htm>.

In order to achieve national uniformity all States and Territories have passed Electronic Transactions Acts that complement the Commonwealth's ETA. This layer of state legislation therefore covers private sector transactions.

In order to achieve national uniformity all States and Territories have passed Electronic Transactions Acts that complement the Commonwealth's ETA. This layer of state legislation therefore covers private sector transactions. The State and Territory counter-parts are:

- Australian Capital Territory – *Electronic Transactions Act* 2001 (ACT)
- New South Wales – *Electronic Transactions Act* 2000 (NSW)
- Northern Territory – *Electronic Transactions Act* 2001 (NT)
- Queensland – *Electronic Transactions Act* 2001 (Qld)
- South Australia – *Electronic Transactions Act* 2000 (SA)
- Tasmania – *Electronic Transactions Act* 2000 (Tas)
- Victoria – *Electronic Transactions Act* 2000 (Vic)
- Western Australia – *Electronic Transactions Act* 2003 (WA)

The State and Territory ETAs are generally a mirror of the Commonwealth ETA, with occasional small differences in definitions[28], and occasional additional sections[29]. However, where the mirror breaks, indeed shatters, is in their approach to exemptions. The scope, type and location of exemptions differ markedly between jurisdictions.

3.2.2. Exemptions

The numerous exemptions to the Commonwealth ETA and the State and Territory ETAs cause significant confusion in this area of law. Having set up a series of Acts which appear, on their face, to enable an electronic communication to meet the requirements of writing, signatures, material form and record-keeping, the exemptions then strip away all or part of these provisions in a variety of scenarios.

Exemptions do serve their role, and of course some limited exemptions may be justified. Requirements for some paper based documents and real signatures may be with us for some time to come. However, it is the complexity and inconsistency of the exemptions that is most worrying for electronic commerce. It is hard to have confidence in the legal validity or enforceability of an electronic communication if there is a chance that it is subject to an obscure exemption. This situation is not helped by the difficulty faced in locating and identifying relevant exemptions.

The exemptions are incredibly inconsistent across jurisdictions – both in their application and their location. Some jurisdictions have exempted numerous pieces of legislation, while other jurisdictions have exempted virtually nothing. The exemptions are also provided in different locations across jurisdictions making the process of identifying exemptions difficult and time consuming.

Overall, these exemptions reduce legal certainty in electronic commerce, which was a key objective of both the Model Law and the ETA.

---

[28] Compare, for example, the definition of consent in the Commonwealth and Victorian ETAs.

[29] See for example the detailed and lengthy section (Part 2A) on electronic courts in the *Electronic Transactions Act* 2000 (NSW).

There are several broad types of exemptions that can be found in the ETAs:

— **General Exemptions**
Some general activities or requirements may be exempt from the relevant ETA. These exemptions do not refer to a particular legal requirement set out in a specific piece of legislation. Rather they refer to a broad category of activity. Common (although inconsistent) examples are:

  — Signing a will;

  — Signing an enduring Power of Attorney;

  — Witnessing a document;

  — Lodging a court document; or

  — Meeting the requirements of personal service of a document.

— **Exempt Legislation**
The requirements of specific, named pieces of legislation may be exempt from the relevant ETA. This type of exemption is common, although again it is inconsistent across jurisdictions. The Commonwealth have exempted or partially exempted 157 pieces of legislation. Some States and Territories have not exempted any specific legislation.

— **Applicable Provisions of Exempt Legislation**
Where legislation has been exempted, the exemption may sometimes only apply to particular requirements of the named piece of legislation. On some occasions this is very specific – such as a particular section or sub-section. On other occasions the exemption may cover a Part or a Division. This type of partial exemption is common at the Commonwealth level but is also used in several State jurisdictions.

— **Applicable Provisions of the ETA**
Where a named piece of legislation has been fully or partially exempted from the ETA, the exemption may be further limited to particular provisions of the ETA (this is also true for the general exemptions discussed above). Sometimes the exemption will be restricted to the recognition of electronic signatures, or writing, but not the other provisions of the ETA.

— **Over-riding Legislation**
In rare circumstances, another piece of legislation may contain provisions that purport to specifically override the operation of the relevant ETA. In these circumstances the legislation will specifically refer to the ETA (or an individual provision of the ETA) limiting its application to a particular set of circumstances.[30]

[30] See for example the time of receipt provisions that specifically override the ETA in the *Migration Legislation Amendment (Electronic Transactions and Methods of Notification) Act No. 58*, 2001 (Cth).

3.3. Privacy and data protection

3.3.1. Current privacy protection

Australia has the following general privacy legislation (or guidelines) in place:

Jurisdiction	Legislation / Standard	Regulator
Cth	*Privacy Act 1988* (Cth)	Federal Privacy Commissioner
ACT	*Privacy Act 1988* (Cth)	Federal Privacy Commissioner
NSW	*Privacy and Personal Information Protection Act 1998* (NSW)	NSW Privacy Commissioner
NT	*Information Act 2002* (NT)	NT Information Commissioner
Qld	*Information Standard 42*	Queensland Ombudsman
SA	Cabinet Administrative Instruction 1/89	Privacy Committee of South Australia
Tas	*Personal Information Protection Act 2004* (Tas)	Department of Justice
Vic	*Information Privacy Act 2000* (Vic)	Victorian Privacy Commissioner
WA	Not yet enacted[31]	–

The State and Territory legislation in this list generally applies to the activities of State and Territory public sector agencies.

The key legislation for privacy in e-commerce is the current Commonwealth privacy legislation – the *Privacy Act*.[32] The Act sets out the Information Privacy Principles (IPPs), which regulate the collection, use and disclosure of personal information by Australian government agencies. The Act also includes a complaints, audit and enforcement regime.

The Commonwealth legislation applies to both the Australian Government public sector, and significant parts of the private sector. However two different standards of privacy protection exist in the Commonwealth legislation:

— **Information Privacy Principles (IPPs)**
Eleven IPPs that apply to Commonwealth and ACT government agencies.

— **National Privacy Principles (NPPs)**
The *Privacy Act* was amended in 2001 to include ten NPPs that apply to parts of the private sector (those that earn more than $3 million annually and all health service providers).[33]

[31] *Information Privacy Bill 2007* (WA), <http://www.parliament.wa.gov.au/parliament/bills.nsf/B76E4F86BE5ACCADC82572AB002D2C7F/$File/Bill+193-1.pdf>.

[32] *Privacy Act 1988* (Cth), <http://www.comlaw.gov.au/>.

[33] *Privacy Amendment (Private Sector) Act 2000* (Cth), <http://www.comlaw.gov.au>.

The NPPs cover:

— **Principle 1 – Fair Collection**
Collection of personal information is only allowed if it is necessary for the function or activity of the organisation. Organisations must explain their information practices to individuals at the time when they collect their personal information.

— **Principle 2 – Use and disclosure**
Personal information should generally not be used or disclosed for the purpose other than for which it is collected without the consent of the individual concerned.

— **Principle 3 – Data quality**
Organisations must take reasonable steps to ensure that personal information collected, used or disclosed by them is accurate, complete and up to date.

— **Principle 4 – Data security**
Organisations must take reasonable steps to protect personal information they hold from unauthorised access, and must not hold data longer than needed.

— **Principle 5 – Openness**
Organisations must clearly express and make available their policies about how they collect, hold, use and disclose personal information.

— **Principle 6 – Access and correction**
Organisations must provide individuals with access to information they hold about them on request and must correct that information if it is not accurate, complete and up to date.

— **Principle 7 – Identifiers**
An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by an agency or Commonwealth provider.

— **Principle 8 – Anonymity**
Where lawful and practical, individuals must be given the option of remaining anonymous when entering into a transaction with an organisation.

— **Principle 9 – Transborder data flows**
An organisation in Australia may transfer personal information about an individual to someone who is in a foreign country only if they believe the organisation upholds similar principles of fair data handling or it is for the benefit of the individual.

— **Principle 10 – Sensitive information**
An organisation must not collect sensitive information about individuals unless the individual consents, or if the organisation is required to do so by law.

3.3.2. Potential Privacy Law Reform

Commonwealth privacy legislation is currently the subject of a review by the Australian Law Reform Commission (ALRC). The ALRC review builds on earlier work by a Senate Committee and by the Office of the Privacy Commissioner. It is likely that significant changes to the IPPs and NPPs may result from this review.

— **Office of the Privacy Commissioner (OPC) Review (2005)**[34]
The OPC Review focused on the private sector provisions of the *Privacy Act*. A final report was published in May 2005 and included several important recommendations for achieving greater consistency in Australian privacy legislation. The Government has not responded to these recommendations.

— **Australian Law Reform Commission (ALRC) Review (2006-2008)**[35]
The ALRC has been given broad terms of reference to review all aspects of Australian privacy law, including the matters raised in the earlier OPC review. This review will also cover the public sector provisions of the *Privacy Act*.

The ALRC is now due to report at the end of May 2008, and the Government's response to the report may take several months after this to prepare. The implementation of any recommendations will take longer.

3.4. Spam

The primary piece of legislation on spam in Australia is the *Spam Act 2003* (Cth).[36] The Act contains provisions regulating 'commercial electronic messages', address-harvesting software, and harvested address lists, as well as civil penalties for violations of these provisions. These provisions are concerned with spam within Australia, and are complemented by a number of international cooperation agreements. The Act is also supported by industry guidelines such as the *Australian eMarketing Code of Practice*[37] and the *Internet Industry Spam Code of Practice*.[38]

In June 2006 the *Report on the Spam Act 2003 Review*[39] was tabled in Parliament. This report was based on public submissions made between December 2005 and February 2006. The discussion is quite extensive – most, if not all, of the content of the Act receives some attention – but it was generally argued that few changes to the Act were required.

---

[34] Office of the Privacy Commissioner, *The Review of the Private Sector Provisions of the Privacy Act 1988*, March 2005, <http://www.privacy.gov.au/act/review/review2005.htm>.

[35] Australian Law Reform Commission, *Review of Privacy*, <http://www.alrc.gov.au/inquiries/current/privacy/index.htm>.

[36] *Spam Act 2003 (Cth)*, <http://www.comlaw.gov.au/>.

[37] Australian Communications and Media Authority, *Australian eMarketing Code of Practice*, ACMA, March 2005, <http://www.acma.gov.au/acmainterwr/telcomm/industry_codes/codes/australian emarketing code of practice.pdf>.

[38] Internet Industry Association, *Internet Industry Spam Code of Practice*, December 2005, <http://www.iia.net.au/files/IIA/Codes of Practice/Spam/iia spam code.pdf>.

[39] The Department of Communication, Information Technology and the Arts, *Report on the Spam Act 2003 Review*, DCITA, June 2006, <http://www.dcita.gov.au/__data/assets/pdf_file/40220/Report_on_the_Spam_Act_2003_Review-June_2006.pdf>.

3.4.1. Sending of commercial electronic messages

Subsection 16(1) of the Act prohibits (with exceptions) the sending of commercial electronic messages.

Electronic messages are defined in section 5 of the Act as messages sent using an Internet carriage service, or any other listed carriage service, to an electronic address in connection with an email account, an instant messaging account, a telephone account, or 'a similar account'. 'Message' is given a broad definition in section 4, including information encoded as text, sound, images, data, 'any other form', or a combination of forms. If the purpose, or one of the purposes, of an electronic message falls within the list of purposes in section 6, the message will be considered to be an electronic commercial message. Some examples of these purposes are:

- To offer to supply goods, services or land;
- To advertise or promote a supplier of goods, services or land;
- To offer to provide, or to advertise or promote, a business or investment opportunity;
- To assist or enable a person, through deception, to dishonestly obtain property or financial gain from another person; and
- To assist or enable a person to dishonestly obtain a gain from another person.

It is immaterial whether the goods, services, land or opportunity exist, or whether obtaining the goods, services, land or opportunity would be lawful.

Specific types of communication may be excluded from this definition by the regulations under subsection 6(7) (for example, the *Spam Regulations 2004* (Cth)[40] currently exclude fax messages). Messages sent using a standard telephone service are excluded from this definition by subsection 5(5); the *Spam Bill 2003 Explanatory Memorandum*[41] indicates that this exclusion extends to calls made using Voice Over Internet Protocol (VOIP). The exclusion applies equally to calls made using recorded or synthesised voices. The exclusion of voice calls from this section is complemented by the *Do Not Call Register Act 2006* (Cth)[42] prohibiting the making of telemarketing calls to numbers registered on the Do Not Call Register.

Subsection 17(1) requires that commercial electronic messages include clear and accurate identification of the individual or organisation that authorised the sending, and accurate contact information for the individual or organisation.

Under subsection 18(1), a person must not send a commercial electronic message unless it provides a clear and conspicuous 'unsubscribe' statement informing the recipient that they may inform the sender that they do not wish to receive further commercial electronic messages. The sender must provide a functional mechanism to allow unsubscribing (subsection 18(1)(c)(i) requires an email address to be specified in the message for this purpose, but other mechanisms may be possible).

---

[40] *Spam Regulations 2004* (Cth), <http://www.comlaw.gov.au/comlaw/Legislation/LegislativeInstrument1.nsf/0/14F2F85815E224BECA256F71004E2AF8/$file/2004B00070.pdf>.

[41] *Spam Bill 2003 Explanatory Memorandum*, <http://www.comlaw.gov.au/comlaw/Legislation/Bills1.nsf/0/0E084D5486E890FACA256F720030E3E1/$file/03150em.rtf>.

[42] *Do Not Call Register Act 2006* (Cth), <http://www.comlaw.gov.au/ComLaw/Legislation/Act1.nsf/0/1873DAF7175E5709CA2571A2001FC6DE/$file/088-2006.pdf>.

3.4.2. Harvesting

The *Spam Act* also contains restrictions on the use of electronic address-harvesting software and the results of such software. Address-harvesting software is defined as software designed or marketed for searching for and compiling electronic address from the Internet.[43]

Under subsection 20(1), a person must supply or offer to supply address-harvesting software, a right to use address-harvesting software, a harvested address list, or a right to use a harvested address list. This provision does not apply if the supplier had no reason to suspect that the customer or another person would use the software or list for sending commercial electronic messages in contravention of section 16 (see above), or if the supplier did not know and could not have ascertained with reasonable diligence that the supply or offer of supply was made to an individual physically present in Australia, or a body corporate or partnership carrying on business or activities in Australia, at the time of the supply or offer.

Subsection 21(1) prohibits the acquisition and use of address-harvesting software or harvested address lists. This prohibition does not apply if the person did not intend to use the software or list in contravention of section 16.

Subsection 22(1) prohibits the use of address-harvesting software or harvested address lists, unless the use is not in connection with sending commercial electronic messages in contravention of section 16.

These provisions apply if one or more of the supplier, acquirer, or user is an individual physically present in Australia, or a body corporate or partnership carrying on business or activities within Australia at the time of the supply or offer.

3.5. Jurisdiction

Australia's jurisdiction laws come from both the common law and the statutes of each state. Courts may exercise jurisdiction if a defendant is in their territory, or if there is a sufficient connection between the claim and the territory (such as a tort committed or a contract formed in the state). The High Court of Australia applied the existing laws to a case of Internet defamation in *Dow Jones v Gutnick*, rejecting the argument that these laws could not apply to the Internet due to its special nature.

Australian courts exercise jurisdiction in accordance with both the common law and the statutes of each state. The basis for jurisdiction is, in either case, a connection to the particular forum, whether by territory (at common law) or subject matter (under the statutes).

There is at present no legislation governing jurisdiction in claims concerning the Internet, however the High Court of Australia has examined the issues in *Dow Jones v Gutnick*, determining that a defamation suit could be brought against a party who publishes material on the Internet, notwithstanding that the material was uploaded in another country.

At common law, the jurisdiction of an Australian court is generally a matter of territory. In order for a court to have jurisdiction over an individual, the plaintiff must bring a suit against that individual while the individual is in the court's territory. Once a person has left the court's territory, common law jurisdiction cannot be exercised upon them, although the court may still exercise common law jurisdiction over the individual's agent. In the case of a foreign corporation, the question of whether a court may exercise jurisdiction will be answered by considering whether the corporation has a place of business in the court's territory, and the nature and duration of the business.

---

[43] Section 4, *Spam Act 2003* (Cth).

In addition to common law jurisdiction, Australian courts may exercise statutory jurisdiction. The laws governing jurisdiction are determined by individual states,[44] but are generally similar. A court is able to exercise statutory jurisdiction if the case has a sufficient connection to the court's territory (generally a state of Australia), for example, if the case relates to:

— A contract made or breached in the territory;

— A tortious act committed in the territory, or a tort occurring in the territory (where the act and the tort can occur in different places, for example in defamation), or damage suffered in the territory regardless of where the tortious act occurred; and

— Property (land) in the territory.

The statutory authority also grants jurisdiction if the person to be served (i.e. the defendant) resides in the territory, confirming common law jurisdiction.

The submission of a defendant will also allow the court to exercise its jurisdiction over that defendant. The defendant will be deemed to have submitted simply by taking part in the proceedings (unless the defendant is taking part only to the extent needed to contest jurisdiction). It can also be inferred if the defendant is party to a relevant contract containing a choice of forum clause.

Australian courts will generally recognise in a contract a clause specifying a choice of forum, however this will be subject to the court's construction of the contract, as well as considerations of public policy. Thus, a choice of forum clause specifying a country wholly unrelated to either the parties concerned or the place where the contract is carried out may be overridden.[45]

3.5.1. Forum Non Conveniens

A person once served may argue that the court should not exercise its jurisdiction on the grounds that the court is a "clearly inappropriate forum" to hear the case; this is the doctrine of "*forum non conveniens*". A court may find that it is clearly inappropriate if it would place an unfair burden on, be prejudicial to, or produce serious and unjustified trouble for a party. The application of this doctrine is a discretionary matter for the court – the court must firstly decide that it has the authority to exercise jurisdiction, and secondly decide whether another forum would be more appropriate.

"Forum shopping", whereby a litigant seeks to have a case heard before a court because of some advantage offered, rather than any real connection to the court, has received the disapproval of Australian courts. When deciding on matters of jurisdiction, especially with regard to questions of choice of forum and *forum non conveniens*, the courts have often taken a position intended to restrict forum shopping.

3.5.2. Dow Jones v Gutnick

The above law concerning jurisdiction generally has since been brought to bear on the matter of Internet jurisdiction. In *Dow Jones v Gutnick*,[46] the leading Australian case on Internet jurisdiction, the High Court of Australia ruled that, when a defamatory article is published over the Internet, the tort of defamation occurs at the place where the article is downloaded and viewed, rather than the place from which it is uploaded, or the place which houses the server on which it is stored.

---

[44] See for example schedule 6 of the *Uniform Civil Procedure Rules* 2005 (NSW) <http://www.austlii.edu.au/au/legis/nsw/consol_reg/ucpr2005305/sch6.html>.

[45] *Akai Pty Limited v The People's Insurance Company Limited* [1996] HCA 39, 23 December 1996, <http://www.austlii.edu.au/au/cases/cth/HCA/1996/39.html>

[46] *Dow Jones & Co v Gutnick* (2002) 210 CLR 575 <http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html>.

Importantly, the High Court did not view the Internet as an entirely new paradigm requiring sweeping changes to the laws of jurisdiction. Rather, the Internet was seen simply as another communication device, which could be governed by the existing laws.

3.5.3. Jurisdiction and Consumer Protection in the Trade Practices Act

Part V of the *Trade Practices Act 1974* (Cth)[47] contains a number of provisions dealing with consumer protection, in particular, Division 2 of that part includes provisions implying a number of terms into the contract, such as (for example) an implied condition that goods sold by a corporation to a consumer are of merchantable quality, and an implied condition that bulk goods will match a sample. These provisions cannot be contracted out of in contracts with consumers.

Section 67 of the *Trade Practices Act 1974* (Cth) provides that, where the proper law of a contract would be the law of Australia but for a choice of law term in the contract, the above provisions will apply notwithstanding that term.

[47] <http://www.comlaw.gov.au/>

4. International

4.1. Consumer protection

The main international developments in consumer protection for electronic commerce come in the form of scattered domestic legislation. However, the OECD has provided some leadership and general guidance on this issue.

4.1.1. OECD

The Organisation for Economic Co-operation and Development (OECD) is an international organisation of 30 member countries forming a global forum to discuss, develop and refine global and national economic and social policies. Participation and involvement in the OECD is not restricted to its member countries – its 70 non-member economies are invited to subscribe to OECD agreements, participate in OECD Committees and are given assistance in adhering to OECD standards and instruments. All of these measures help preserve the global reach of the organisation. Such non-member participation is particularly important in development of e-commerce policy, which will only be as effective as its level of international approval and compliance.

The OECD's *Guidelines for Consumer Protection in the Context of Electronic Commerce* were created to ensure that existing consumer protection principles were applied to the online marketplace.[48] The document sets out core consumer protection principles for a global approach to protecting consumer interests in electronic business-to-consumer (B2C) transactions. The Guidelines reaffirm that consumer protection mechanisms available for more traditional forms of commerce should also be made available when contracting online and also aims to protect consumers from dangers unique to the online environment. Without imposing any barriers to trade, the Guidelines are intended to assist:

- Governments in formulating and implementing online consumer policy;
- Business associations, consumer groups and self-regulatory bodies in the development and implementation of online consumer protection schemes; and
- Individual businesses and consumers who are transacting electronically by providing information and guidance on the standards of behaviour for fair business practices as well as outlining some of the basic rights of consumers transacting electronically.

The Guidelines have arguably become the leading international instrument on consumer protection in e-commerce – its recommendations have been endorsed by a number of international organisations including the Transatlantic Consumer Dialogue (TACD)[49] and the Asian-Europe Meeting (ASEM), and some of the provisions contained in the Guidelines have been incorporated in the European Union E-Commerce Directive.[50]

---

[48] Committee On Consumer Policy, *Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce*, OECD, 9 December 1999, <http://www.oecd.org/dataoecd/5/34/1824782.pdf>.

[49] <http://www.tacd.org/>

[50] Directive 2000/31/EC, <http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf>.

The OECD *Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*[51] have been created to address the growing international problem of fraudulent and deceptive practices occurring in B2C e-commerce transactions. These activities greatly undermine consumer confidence in the online environment and the integrity of global and domestic markets. Most law enforcement mechanisms were developed when such practices occurred on a mainly domestic level, and consequently are ill equipped to deal with the migration of these practices to the international arena. The increasingly international character of these practices has created a need not only for international coordination and cooperation but also to extend existing domestic regulatory frameworks that deal with online cross-border fraud and deception.

Fraudulent and deceptive commercial practices are defined in the guidelines to include practices that have caused, or have the potential to cause, harm to consumers, such as:

- Making a false misrepresentation of fact;
- Failing to deliver products or services after a consumer has been charged; and
- Charging or debiting a consumer's financial, telephone and other accounts without authorization.[52]

The Guidelines are aimed at governments and domestic consumer enforcement agencies and provide for the development of a framework for 'closer, faster and more efficient cooperation' amongst consumer enforcement agencies through:

- Effective domestic frameworks;
- Greater international cooperation;
- Notification, information sharing, assistance with investigations, and confidentiality;
- Adequate authority given to consumer protection enforcement agencies;
- Consumer redress; and
- Private-sector cooperation.

In accordance with the recommendations contained in the Guidelines, the governments of member countries have provided a list of National Contact Points[53] of consumer protection organisations to facilitate more effective cooperation in combating this growing international problem.

[51] Committee On Consumer Policy, *Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, OECD, 11 June 2003, <http://www.oecd.org/dataoecd/24/33/2956464.pdf>.

[52] Article 1.

[53] <http://www.oecd.org/document/16/0,2340,en_2649_34267_31675216_1_1_1_37441,00.html>

4.1.2. ASEAN

Coverage in ASEAN of consumer protection laws for e-commerce is minimal. It does not extend beyond a section in Malaysia's *Communications and Multimedia Act 1998*[54] providing that network service and application providers must deal reasonably with consumers and adequately address consumer complaints, a subsection in the Philippines *Electronic Commerce Act 2000*[55] which states that violations of the *Consumer Act 1991*[56] committed by using electronic transactions will be subject to the same penalties contained in that Act; and a proposed provision in the Indonesian *Bill on Electronic Information and Transactions 2006*,[57] which states that consumers have the right to receive complete information on contract requirements and product details.

Despite the limited coverage in ASEAN of consumer protection laws for e-commerce, most jurisdictions have general consumer protection legislation in place. These, in most circumstances, will apply to goods and services sold online.

4.2. Electronic contracting

4.2.1. The UN Convention on Electronic Contracting

The United Nations Commission on International Trade Law (UNCITRAL) has finalised its Convention on electronic contracting following over three years of deliberations. The Convention has been formally titled the *Convention on the use of electronic communications in international contracts*. It is the first UN Convention addressing legal issues created by the digital environment.

The Convention seeks to enhance the legal certainty and commercial predictability of international electronic transactions by setting out a number of interpretive rules for the use of electronic communications in negotiating and forming contracts.

18 countries have now signed this UN Convention, including China, Korea, Philippines, Russia and Singapore.

The new Convention is likely to establish a default standard for electronic transactions. Even if a country does not ratify the Convention (once it is brought into force) it will still influence the terms of a transaction; particularly where the other contracting party is from a country that is a signatory to the Convention.

The Convention on electronic contracting also seeks to harmonise national law regarding how electronic contracts can be made. Harmonised domestic legislation will overcome the legal uncertainty in international business transactions where contracting parties are from different countries. A more certain legal environment will increase confidence in conducting electronic transactions, and in turn participation in e-commerce.

---

[54] *Communications and Multimedia Act 1998* (Malaysia), <http://www.mcmc.gov.my/mcmc/the_law/ViewAct.asp?lg=e&arid=900722>.

[55] *Electronic Commerce Act 2000* (Philippines), <http://www.mcmc.gov.my/mcmc/the_law/ViewAct.asp?lg=e&arid=900722>.

[56] *Consumer Act 1991* (Philippines), <http://www.dti.gov.ph/uploads/files/Forms1_File_1104836450_RA7394.pdf>.

[57] *Bill on Electronic Information and Transaction 2006* (Indonesia), <http://www.depkominfo.go.id/>.

However, the complex provisions in the Convention on scope, exclusions, party autonomy and declarations may undo some of the good intentions of the Convention, and this paper raises concerns about the management of these exclusions and declarations in practice.

The Convention contains provisions enabling the two principles at the core of any electronic transactions legislation:

— **Functional equivalence** – paper documents and electronic transactions are treated equally by the law; and

— **Technology neutrality** – the law does not discriminate between different forms of technology.

Of these two principles it is the former that is of the greatest importance, allowing the legal requirements of paper-based documents such as writing and signature to be readily translated into electronic equivalents. The interpretative nature of functional equivalence provisions allows the general application of these rules without necessitating amendment of all laws containing provisions on writing, signature or other form requirements.

The Convention refrains from including too many substantive provisions as it was felt by UNCITRAL that these were best left to national legislators to address. In any case most substantive issues would also apply to paper-based trade.

4.2.2. ASEAN

The *ASEAN E-Commerce Project* has been assisting ASEAN meet targets set in the *Roadmap for Integration of e-ASEAN Sector* (the e-ASEAN Roadmap), The Roadmap is a comprehensive list of measures to be implemented by 2010 to realise the e-ASEAN vision.

The overall goal of the *E-Commerce Project* is to assist ASEAN to integrate into one market for goods, services and investment.

During the project, *E-Commerce Project Guidelines* have been developed that build on the common objectives and principles for e-commerce legal infrastructure. These Guidelines include prescriptive information on implementation steps, and a timeline. The Guidelines were developed by Galexia in collaboration with project participants and technical experts from ASEAN Member Countries. The Guidelines have been endorsed by the ASEAN E-Commerce and ICT Trade Facilitation Working Group.

The Guidelines cover numerous e-commerce issues, and electronic contracting is one priority issue in ASEAN. All Member Countries have enacted legislation or have draft legislation in place on electronic contracting.

When selecting a model for harmonisation, ASEAN Member Countries also wanted to ensure that their legal infrastructure would be compatible with international developments. The project guidelines for electronic contracting legislation are therefore based on the *UN Convention on the Use of Electronic Communications in International Contracts 2005* (the ECC).

Whether or not a particular country signs the Convention, the text is likely to reflect minimum standards for most cross-border transactions. The text of the Convention will likely become the default standard for e-commerce law, and ASEAN Member Countries may wish to ensure that their own laws and practices are compatible with it. Becoming a party to the Convention would further support trust and certainty in cross-border contract formation and electronic transactions.

When ASEAN makes a consensus decision to take action – for example their decision to implement harmonised e-commerce laws – the next challenge is to implement this decision at the domestic level. In the area of e-commerce legal infrastructure, the diversity amongst Member Countries is most noticeable in regards to the different levels of development, as ASEAN includes both highly developed countries with mature e-commerce infrastructure (such as Singapore) and developing countries with only rudimentary e-commerce infrastructure (such as Laos).

However, a positive aspect of the *E-Commerce Project* is that it is having a direct impact on the development of domestic e-commerce legal infrastructure in ASEAN Member Countries - sooner than anticipated in the project design. This impact can be seen in the following table.

Table 1: E-Commerce Legislation in ASEAN Member Countries

Member Country	Status of E-Commerce Laws – Project Inception (January 2004)	Status of E-Commerce Laws – Current (February 2008)
Brunei	Enacted	Enacted
Cambodia	None	Draft
Indonesia	None	Draft
Laos	None	Draft
Malaysia	None	Enacted
Myanmar	Draft	Enacted
Philippines	Enacted	Enacted
Singapore	Enacted	Enacted
Thailand	Enacted	Enacted
Vietnam	None	Enacted

Source: ASEAN E-Commerce Project, Internal project materials, ASEAN Secretariat and Galexia.

4.3. Privacy and data protection

4.3.1. ASEAN

At present there are no laws enacted in ASEAN that deal with privacy and personal data protection. Three member countries have draft legislation in place, however it is uncertain in some member countries when the legislation will be enacted. Instead of implementing laws, Singapore has chosen to adopt a self-regulatory approach through the *Model Data Protection Code*.[58]

This lack of coverage is perhaps different from international developments and regulation in other nations around the world. Most developed countries, have legislation regulating the use and handling of personal information by businesses and government agencies and organisations.

ASEAN is currently considering a proposal to examine the harmonisation of privacy and data protection legal infrastructure across the ten ASEAN Member Countries.

[58] TrustSG, *Model Data Protection Code*, 2003, <http://www.trustsg.com.sg/downloads/Data_Protection_Code_v1.3.pdf>.

4.3.2. APEC

The APEC Privacy Framework promotes a consistent approach to information privacy protection across APEC member economies. The Framework includes nine privacy principles for businesses operating in APEC economies.[59]

In June 2007, the APEC E-Commerce Steering Group Data Privacy Subgroup met in Cairns to develop APEC Data Privacy Pathfinder projects with a focus on cross-border privacy rules. The Pathfinder projects were formally endorsed at the meeting of APEC Ministers in Sydney in September 2007.[60]

4.4. Spam

4.4.1. ASEAN

Singapore is the only country in ASEAN that has enacted a spam law,[61] although there is a provision in a Malaysian Act that may be of some assistance in prosecuting spammers. A spam law is currently being drafted in the Philippines and there are plans to enact laws in Thailand. There may be greater coverage of this cyberlaw in ASEAN in the future as spam becomes more of a nuisance for Internet users and lawmakers become more familiar with the legal controls needed to regulate spam. The enacted legislation in Singapore may provide lawmakers in other member countries with a convenient reference point for drafting their own dedicated spam laws.

ASEAN is currently considering a proposal to examine the harmonisation of spam laws across the ten ASEAN Member Countries.

4.4.2. Pacific Island Forum

Galexia is assisting the Department of Broadband, Communications and the Digital Economy (DBCDE) in the development of a harmonised spam legislation, enforcement and co-operation regime in the Pacific. This project, funded in part by AusAID's Pacific Governance Support Program (PGSP), is currently being applied across the island states of Niue, Samoa and Vanuatu. Australia, Tonga and the Cook Islands already have harmonised spam legislation in place, and more countries may join this group in the future.

---

[59] More information on the Framework and principles is available at: <http://www.apec.org/content/apec/apec_groups/committees/committee_on_trade/electronic_commerce.html>.

[60] Full details of the Australian meetings regarding APEC are at <http://www.ag.gov.au/apec_privacy>

[61] *Spam Control Act 2007* (Singapore), <http://statutes.agc.gov.sg/non_version/cgi-bin/cgi_legdisp.pl?actno=2007-ACT-21-N>.

4.5. Jurisdiction

4.5.1. International developments

It is widely acknowledged that in order for e-commerce to flourish both businesses and consumers need to be confident in relying on online technologies to complete a transaction. A key component in developing this confidence is creating a predictable legal environment in which electronic transactions can take place including addressing the complicated issue of jurisdiction, which is all important in disputes arising from cross-border electronic transactions.

International law in the field of cross-border jurisdiction for e-commerce is still developing and is quite immature. A consistent approach to dealing with jurisdiction issues arising from online commerce has not yet emerged. Some conclusions that can be drawn on the state of online jurisdiction at an international level are:

- The breakdown of negotiations on the proposed Hague Convention on International Jurisdiction and Foreign Judgments in Civil and Commercial Matters and the subsequent settling on a Convention on Choice of Court Agreements indicates that international consensus on jurisdiction and choice of law rules is unlikely to occur for a long time;
- Considering the divergent approaches adopted in domestic law to resolving jurisdiction and choice of law rules, a consistent international approach can only be reached through international agreement or a treaty. In light of the recent failure of the Hague Judgments Convention it will be a while before efforts at producing an international jurisdiction convention are renewed;
- Where a plaintiff obtains a judgment in their favour they may face difficulty in enforcing that judgment in a foreign jurisdiction (such as jurisdictions where the defendant has their assets) if the judgment is in conflict with the public policy of that jurisdiction. See, for example, *UEJF and LICRA v Yahoo! Inc (2006)*.
- Superior courts in some countries are reluctant to develop new and separate rules for the Internet, finding that traditional legal principles can be easily adapted to address legal issues raised by the Internet. With this in mind the place of publication for material published online and offline is the place where the material is accessible and comprehended. For the Internet, this is where the information is downloaded and read. See, for example, *Dow Jones v Gutnick (2002);* and
- In America it is widely accepted that the test for determining whether a court can exercise personal jurisdiction over a defendant whose contacts with a forum occur solely via the Internet is based on a "sliding scale" test on the interactivity of the website (see *Zippo Manufacturing Co v Zippo Dot Com Inc (1996).* The Zippo test is supported by a vast body of case law interpreting how and when the test should be applied. However, the value of the Zippo test as an international authority is somewhat limited as it does not appear to be applied outside the United States. The test also does not address problems experienced by parties in enforcing foreign judgments.

Self-management and mitigation of jurisdictional issues in cross-border commerce remains one of the most effective ways to avoid the problems associated with the uncertain state of international law. Choice of forum clauses are the most obvious example of these. Guidance on the use of these clauses can be gleaned from the Hague *Convention on Choice of Court Agreements 2005.*

4.5.2. Hague Conference on Private International Law

The Hague Conference on Private International Law is an international body dedicated to developing unified rules of private international law and has created many conventions directed at this goal[62]. In 1992 the Conference began work on a convention on jurisdiction and the recognition and enforcement of foreign judgments. However, the development of this Convention was abandoned in 2002 after it was clear that international consensus could not be reached. If a convention on international jurisdiction was formed it would have been a momentous development in private international law, greatly unifying the exercise of jurisdiction by national courts and paving the way for greater legal certainty in enforcing cross-border transactions. Instead the Hague Conference adopted in June 2005 a Convention on Choice of Court Agreements. It is too soon to determine the impact of this Convention, however it is not likely to be significant if it is not widely adopted by states.

The Failed Convention – the Proposed Convention on International Jurisdiction and Foreign Judgments in Civil and Commercial Matters

Negotiations for the proposed Hague Convention on International Jurisdiction and Foreign Judgments in Civil and Commercial Matters began in 1992 following a request from the United States. The impetus for the Convention was noted by the Hague Conference in 2002:

> There is little doubt that one of the factors which has recently attracted so many new Member States to the Organisation is their interest in this project [the proposed Convention on International Jurisdiction and Foreign Judgments in Civil and Commercial Matters]. The ongoing globalisation of trade and commerce, and the exponential growth of the use of the Internet and e-commerce continue to add to the need for a global framework for jurisdiction and the recognition and enforcement of judgments.[63]

In October 1999 the Conference prepared a preliminary draft convention, which was further revised in June 2001. The proposed Convention would apply to most civil and commercial transactions including consumer transactions, however it was not to apply to arbitration proceedings. Some of the matters addressed in the draft Convention included:

- Whether a defendant may be sued in a court where they are habitually resident;
- Provisions on the making of exclusive choice of court agreements;
- With regard to contracts, the proposed Convention provided that the plaintiff may bring an action in the state where the defendant conducted or directed frequent or significant activity if it was reasonable to do so;
- For consumer contracts, the consumer may generally bring proceedings in the state where the consumer is habitually resident if the contract was concerned with activity the other party conducts in that state or directs at that state; and
- Judgments based on an exercise of jurisdiction under the Convention or consistent with the Convention shall be recognised and enforced subject to some conditions specified in the proposed Convention. One of the grounds for not recognising a foreign judgment includes where it is manifestly contrary to public policy.

---

[62] <http://www.hcch.net>

[63] Permanent Bureau, *Some Reflections on the Present State of Negotiations on the Judgments Project in the Context of the Future Work Programme of the Conference*, Hague Conference on Private International Law, February 2002, <http://www.hcch.net/index_en.php?act=publications.details&pid=3500&dtid=35>, p5.

As deliberations progressed, it became clear that international agreement on the form of the Convention would not be reached and the proposed Convention was abandoned. The disagreement primarily arose from the United States who found that they could not sign the Convention which too closely reflected the provisions of the EU *Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters 1968* and was not adequately tailored to the international context or the method used in other countries to determine jurisdiction and recognition and enforcement issues.[64]

The narrower Convention on choice of court agreements was instead negotiated and was adopted by the Hague Conference in June 2005. The failure to reach international consensus on jurisdiction and recognition and enforcement of foreign judgment issues does not bode well for the future of international Internet law. The failed negotiations indicate that it will be some time before international consensus can be reached. In the meantime the fate of cross-border litigation is in a state of limbo: each country will apply its own domestic law to resolve jurisdiction issues, which will make international consensus even more difficult to achieve as countries are given time to develop and refine their own principles for dealing with cross-border jurisdiction.

The failure to negotiate a Convention on jurisdiction and enforcement of foreign judgments is perhaps unsurprising considering the limited impact of the 1971 *Hague Convention on the Recognition and Enforcement of Foreign Judgments in Civil and Commercial Matters*.[65] The Convention aims to establish a common framework on principles for the mutual recognition and enforcement of judicial decisions in member states. This Convention is also plagued with its own problems. The Convention is only in force in Cyprus, Kuwait, the Netherlands and Portugal. Its application in private international law is inhibited by its limited adoption by states. It does not create rights in favour of contracting states but acts as a guideline for bilateral enforcement agreements between contracting states by providing conditions in which foreign judgments should be recognised. The Convention does not specify the circumstances in which the courts of a contracting state can exercise jurisdiction over a foreign defendant. This obviously is a significant limitation on its application to cross border jurisdiction issues.

Convention on Choice of Court Agreements 2005

On 30 June 2005, the Hague Conference finalised its Convention on choice of court agreements.[66] The Convention sets out rules for parties wishing to enter into an international choice of court agreement that indicates the court which is to have exclusive jurisdiction over the parties in the event of a dispute.

The Convention aims to promote international trade and investment through enhanced judicial cooperation and increased uniformity and certainty on the legal rules surrounding jurisdiction and the recognition of foreign judgments where the parties have entered into a choice of court agreement. The Convention is in essence a compromise following the failure to reach sufficient international consensus to form a Convention on international jurisdiction and foreign judgments in civil and commercial matters.

As yet the *Convention on Choice of Court Agreements* has not been signed by any country or regional economic integration organisation, and is not yet in force.[67] It is expected that that the Hague Conference will publish a draft report on the Convention and member states will consider ratifying the Convention after this report is released and they have had time to consider ratification issues.

---

[64] See Jeffrey Kovar's (Assistant Legal Adviser, Unites States Secretary of State) letter to Alasdair Wallace (Head of International and Common Law Services Division, Lord Chancellor's Department, United Kingdom) on the negotiations on the Hague Draft Convention, 10 September 2000, <http://www.cptech.org/ecom/jurisdiction/kovarletter.html>.

[65] <http://www.hcch.net/index_en.php?act=conventions.text&cid=78>

[66] *Convention on Choice of Court Agreements 2005* <http://www.hcch.net/index_en.php?act=conventions.text&cid=98>.

[67] Article 29 gives regional economic integration organisations made up of sovereign states have the power to sign the convention, at which point has the same rights and obligations as a contracting state.

The Hague Conference on Private International Law has not been able to procure international consensus on jurisdiction and recognition and enforcement of foreign judgment issues. States, for the moment, are left to their own devices to develop rules to regulate these issues. However the problem with the continuation of the status quo is that states will continue to develop their own principles and methods for resolving jurisdiction issues and as the inconsistencies grow and become more entrenched in domestic law bridging the gap through international agreement and consensus will become harder.

The Hague Convention on Choice of Court Agreements is a compromise among states when considering a broader convention on jurisdiction could not be reached. While it aims to afford parties with greater legal certainty in cross-border contracts by entering into exclusive choice of court agreements, it only applies where the states of the contracting parties have adopted the Convention.

5. Australian Resources

Argy and Martin, *The effective formation of contracts by electronic means,* Issue 46, Computers and Law Journal, December 2001, <http://www.nswscl.org.au/journal/46/Argy.html>.

Attorney General's Department, *APEC Privacy Framework*, May 2006.

Attorney General's Department, *Privacy Protection in Australia*, May 2006.

Attorney General's Department, *Review of Australia's Privacy Laws*, May 2006.

Attorney General's Department, *Summary of Privacy Commissioner and Senate Committee Reports,* May 2006.

Attorney General's Department, *Summary of the Electronic Funds Transfer Code of Conduct*, May 2006.

Australian Communication and Media Authority, *Australian eMarketing Code of Practice,* March 2005, <http://www.acma.gov.au/acmainterwr/telcomm/industry_codes/codes/australian emarketing code of practice.pdf>.

Australian Government, *Checklist for Business-to-Consumer E-Commerce in Australia,* 17 March 2006, <http://www.treasury.gov.au/documents/1086/PDF/ecommerce_factsheet.pdf>.

Australian Government, Expert Group on Electronic Commerce, *Review of Building Consumer Sovereignty in Electronic Commerce: A best practice model for business Discussion Paper,* November 2003, <http://www.ecommerce.treasury.gov.au/bpmreview/content/_download/BPM_Review.pdf>.

Australian Government, *The Australian Guidelines for Electronic Commerce*, 17 March 2006, <http://www.treasury.gov.au/documents/1083/PDF/australian_guidelines_for_electronic_commerce.pdf>.

Australian Law Reform Commission, *Review of the Privacy Act, Terms of Reference,* 30 January 2006, <http://www.alrc.gov.au/inquiries/current/privacy/terms.htm>.

Bhyat and Minister for Immigration and Multicultural and Indigenous Affairs [2003] AATA 1051, <http://www.austlii.edu.au/au/cases/cth/aat/2003/1051.html>.

Connolly C and Ravindra P, *Fantastic Beasts and Where to Find Them – A Guide to Exemptions in the Electronic Transactions Act (ETA) in Australia,* September 2004, <http://www.galexia.com/public/research/articles/research_articles-art30.html>.

Consumer Credit (New South Wales) Act 1995, <http://www.legislation.nsw.gov.au/>.

DCITA, *Report on the Spam Act 2003 Review*, June 2006, <http://www.dcita.gov.au/__data/assets/pdf_file/40220/Report_on_the_Spam_Act_2003_Review-June_2006.pdf>.

DCITA, *Spam Act 2003 Review – Issues Paper*, 2006, <http://www.dcita.gov.au/__data/assets/pdf_file/34418/Spam_Review_Issues_Paper.pdf>.

Electronic Funds Transfer Code of Conduct, <http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/eft_code.pdf/$file/eft_code.pdf>.

Electronic Transactions Act 1999 (Cth), <http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/0258AF6450DC213ECA2570450023A032/$file/ElectronicTrans1999.pdf>.

Fair Trading Act 1987 (NSW), <http://www.legislation.nsw.gov.au/>.

Ford & Anor v La Forrest & Ors [2001] QSC 261 <http://www.austlii.edu.au//cgi-bin/disp.pl/au/cases/qld/QSC/2001/261.html>.

Internet Industry Association, *Internet Industry Spam Code Of Practice – A Code For Internet And Email Service Providers*, v1.0 December 2005, <http://www.iia.net.au/files/IIA/Codes of Practice/Spam/iia spam code.pdf>.

KPMG Consulting, *NCP Review of the Consumer Credit Code Final Report*, December 2000, <http://www.creditcode.gov.au/content/downloads/final.pdf>.

Malcolm J, *Australia's Stand on Spam*, Presentation delivered at AUUG 2004 – Who Are You? The Conference for Unix, Linux and Open Source Professionals, 1 September 2004, <http://new.auug.org.au/resources/proceedings/auug2004/papers/malcolm.pdf>.

NOIE, *Final report of the NOIE review of the spam problem and how it can be countered,* April 2003, <http://www.security.iia.net.au/downloads/spamreport.pdf>.

NOIE, *Spam Act 2003: A practical guide for businesses*, February 2004, <http://www.acma.gov.au/acmainterwr/consumer_info/frequently_asked_questions/spam_business_practical_guide.pdf>.

Office of the Attorney General for Western Australia, *Privacy Legislation for Western Australia Discussion Paper*, May 2003, <http://www.ministers.wa.gov.au/mcginty/docs/features/McGinty_privacy_legislation.pdf>.

Office of the Federal Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, March 2005, <http://www.privacy.gov.au/act/review/revreport.pdf>.

Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector*, 9 November 2001, <http://www.privacy.gov.au/publications/hg_01.html>.

Office of the Federal Privacy Commissioner, *Guidelines to the Information Privacy Principles*, <http://www.privacy.gov.au/act/guidelines/index.html – 3.4>.

Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles*, September 2001, <http://www.privacy.gov.au/publications/nppgl_01.pdf>.

Office of the Federal Privacy Commissioner, *Spam Act 2003 Review,* February 2006, <http://www.privacy.gov.au/publications/spamreviewsub.pdf>.

Privacy Act 1988 (Cth), <http://www.comlaw.gov.au>.

Sale of Goods Act 1923 (NSW), <http://www.legislation.nsw.gov.au/>.

Sneddon M, *Legal Liability and E-Transactions: A scoping study for the National Electronic Authentication Council*, August 2000, <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN014676.pdf>.

Spam Act 2003 (Cth), <http://www.comlaw.gov.au/>.

Spam Regulations 2004 (Cth), <http://www.comlaw.gov.au/>.

Szaeg & Ors v Minister for Immigration [2003] FMCA 258, <http://www.austlii.edu.au/au/cases/cth/FMCA/2003/258.html>.

The Consumer Credit Code Website, *What's New,* accessed: 5 March 2008, <http://www.creditcode.gov.au/display.asp?file=/content/whatsnew.htm>.

The Senate, Legal and Constitutional References Committee, *The real Big Brother: Inquiry into the Privacy Act 1988*, June 2005, <http://www.aph.gov.au/Senate/committee/legcon_ctte/privacy/report/report.pdf>.

Trade Practices Act 1974 (Cth), <http://www.comlaw.gov.au/>.

Tubin G, *The Sky Is Falling: The Need for Stronger Consumer Online Banking Authentication*, TowerGroup, April 2005, <http://www.bnet.com/>.

UN *Convention on the use of electronic communications in international contracts* (2005), <http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html>.

Uniform Consumer Credit Code, <http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/C/ConsumCredCode.pdf>.

6. International Resources

Allende LA. and Miglino MA., Internet Business Law Services, *Internet Law – International Electronic Contracting: The UN Contribution*, 6 March 2007, <http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1610>.

ASEAN Secretariat, *e-ASEAN Framework Agreement*, 29 November 2004, <http://www.aseansec.org/6267.htm>.

ASEAN Secretariat, *e-ASEAN Reference Framework For Electronic Commerce Legal Infrastructure*, 2001, <http://www.aseansec.org/EAWG_01.pdf>

ASEAN Secretariat, *Roadmap for Integration of e-ASEAN Sector*, 29 November 2004, <http://www.aseansec.org/16689.htm>.

Chong KW and Suling JC, Singapore Academy of Law, *United Nations Convention on the Use of Electronic Communications in International Contracts – A New Global Standard*, 2006, <http://www.sal.org.sg/Pdf/2006-18-SAcLJ-116%20ChongChao.pdf>

Connolly C and Ravindra P, *First UN Convention on E-Commerce Finalised*, Computer Law and Security Report, 2005, <http://www.galexia.com/public/research/articles/research_articles-art35.html>.

Federal Financial Institutions Examination Council, *Authentication in an Internet Banking Environment*, 2005, <http://www.ffiec.gov/pdf/authentication_guidance.pdf>.

Hong Kong Government, *Launch of Two-factor Authentication for Internet Banking*, 30 May 2005, <http://www.info.gov.hk/hkma/eng/press/2005/20050530e3.htm>.

Infocomm Development Authority (IDA) and Attorney-General's Chambers (AGC), *Joint ISA-AGC Review of Electronic Transactions Act Stage III: Remaining Issues,* 22 June 2005*,* <http://www.agc.gov.sg/publications/docs/ETA_StageIII_Remaining_Issues_2005.pdf>

Luddy WJ. and Schroth PW., Academy of Legal Studies in Business, *The New UNCITRAL E-Commerce Convention in the Mosaic of Developing Global Legal Infrastructure*, 8-12 August 2006, <http://www.alsb.org/proceedings/copyright/UNCITRAL_William_Luddy_Peter_Schroth.pdf>

Monetary Authority of Singapore, *Technology Risk Management Guidelines for Financial Institutions*, 11 November 2002, <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN011549.pdf>.

Pavan Duggal, Advocate, Supreme Court Of India, *Harmonization of Ecommerce Laws and Regulatory Systems in South Asia*, Regional Expert Conference on Harmonized Development of Legal and Regulatory Systems for E-Commerce, 7-9 July 2004, Bangkok, Thailand. <http://www.unescap.org/tid/projects/ecom04_s3dug.pdf>

Polanski P, *Convention of E-Contracting: The Rise of International Law of Electronic Commerce Law*, 19th Bled eConference, 5-7 June 2006, <http://domino.fov.uni-mb.si/proceedings.nsf/0/48ecfcae60f83bf6c12571800036bae9/$FILE/49_Polanski.pdf>

UNCTAD, *Information Economy Report 2007*, United Nations Publication, New York and Geneva, <http://www.unctad.org/ecommerce>)