THE INTERNET AND SOVEREIGNTY: WHAT ARE THE LIMITS OF GOVERNMENT CONTROL?

PATRICK FAIR AND ANNE PETTERD

Baker & McKenzie Sydney

1. Introduction

In the last 15 years the Australian economy has been transformed by the internet. The vast majority of homes now have broadband. There are more mobile phones in Australia than there are Australians. A rapidly increasing number of mobile devices support data services. Email is the most common form of written correspondence. Nearly every business has a website and the first port of call for information is Google and Wikipedia. None of these statements were true in the mid 1990s.

This ongoing transition has created many challenges for government. At the time of writing the Convergence Review\(^1\) is considering re-regulating the media to take account of the rapid growth in internet protocol (IP) based services. The Productivity Commission has recently released its final report to government\(^2\) on the structure and performance of the retail industry which focuses in large part on the impact of online retailing on the domestic industry. Our privacy laws are under review. The current ban on casino style internet gambling is under review.

As regulators examine the impact of the internet on Australian society and consider the most appropriate response, the issues are often complex and the right policy responses difficult to identify. There is a feeling that the internet has changed the game. That the power of government is being diminished. Even that the sovereignty of government is under threat.

In this paper we examine the idea that the sovereignty of government is threatened by the growth in the internet. How does this occur? How far does it go? What are the tools available for regulators to use in response? What are the implications?

We start by looking at how the internet might undermine sovereignty including the proposition that growth in the internet appears to have had a direct impact on the power of the government to regulate. We then consider the extended reach of government power. We look at the power of parliament and the powers of our courts, using the Australian Parliament and the Federal Court as case studies. We then make some observations regarding the causal factors.

We then make some observations regarding the ongoing significance of the apparent causes of the internet undermining government sovereignty and the possible impact on government regulation going forward.

We use the term ‘the internet’ to mean the public IP network that enables information and services to travel across national and international boarders.

2. How does the internet undermine sovereignty?

2.1 Introduction

There was early phase in the development of the internet where protection of the internet itself caused the government to hold back from regulatory intervention:

- In the early days of the internet the Australian government chose not to regulate the administration of commercial and not for profit country code domains for .au. Instead the government chose to support the establishment of a not-for-profit administrator considered to be more in keeping with the open spirit of the internet and better able to manage a changing environment.
In August of 2000 Senator Richard Alston, the Minister for Telecommunications at that time suggested that streaming over the internet should be regulated as broadcasting. But, after representations from industry, the Minister made a declaration to the effect that radio and television programs transmitted using the internet are not broadcasting.

Some of the more recent debate around Senator Conroy’s proposed internet content filter touched on the potential of government intervention to slow down internet services and stifle the effective operation of the medium.

Protection of the internet itself remains a factor important to the willingness of the government to regulate the online environment. However, protection is a factor for consideration along with other possible implications, rather than effectively diminishing the level of government control.

We consider that there are 3 fundamental characteristics of the expanding role of the internet in Australia that directly undermine the authority of government. They are:

(a) the internet giving citizens access to information, materials and/or services access to which has been regulated or restricted in Australia (Access);

(b) the internet facilitating communication and interactions between citizens that cannot be viewed or controlled by government (Communication); and

(c) through the distributed nature of the internet itself: the online environment has become a critical part of our society. It is distributed, open, interdependent and not easily controlled (Distributed Control).

Of course, the internet has a broader impact in ways which bring about social change and require the government to re-regulate industries and behaviours, so not all consequences of the internet fit within our categories. For example, online distribution of digital music has caused CD shops to shut down in large numbers. Increased access to electronic news services and death of the traditional classified ad has caused a decline in newspapers. These are matters caused by the internet but not impacting the sovereignty of government.

2.2 Access

The access provided by the internet impacts the sovereignty of government in two important ways:

- the government loses control of what is seen and done by Australians; and
- direct exposure to competing services and industries forces the government to moderate regulatory intervention having regard to the international context. Will Australian business be disadvantaged? Will the local rules be ignored?

The obvious example of the first category is access to interactive gambling services. Despite government regulation prohibiting the provision of interactive gambling services to Australian customers many Australians gamble online. Concern that prohibition is not working to protect problem gamblers and costing the Australian revenue tax dollars has led to a recommendation by the Productivity Commission that the legislated prohibition be replaced with a permissive harm minimisation strategy.

Another example is the increasing amount of international retail shopping done by Australians using the internet. The issue created by this phenomenon is of a different kind: it is not financially viable to collect GST on the parcels arriving in Australia and, accordingly, the market is distorted in favour of foreign retailers selling goods of a value less than AUD1000 compared to Australian retailers are required to pay the GST.

In terms of exposure to competing services and industries, the phenomenon is nothing new. The rapid expansion of international trade referred to as ‘globalisation’ can be traced back to the discovery of the New World and has been accelerating rapidly since the end of the Second World War. The internet adds a new dimension because it offers an unprecedented level of direct access to
products and services to consumers as well as to businesses. Increased access creates more acute competition between international service providers and significantly increases the need to consider how any regulatory intervention may impact the competitive advantage of local service providers.

In times when foreign service providers had trouble reaching Australian consumers, the barriers to international consumer trade shielded the local environment. The new level of access means that a law imposing Australian content rules on broadcast or subscription television services operating in Australia can work to the competitive advantage of on demand and IP TV services that operate from outside the jurisdiction. Limited rights of fair use in relation to copyright material can discourage the establishment of internet search facilities. Major search engine providers operate their major data centres from outside Australia. There are many other examples.

2.3 Communication

The second characteristic of the internet phenomenon is perhaps the most debatable. Members of our society have always been able to communicate in private including across significant distances. The new phenomenon created by the internet is the creation of places online that are out of view and connect people who may not have connected previously.

The power of interaction between individuals over the internet to undermine sovereignty, literally, is perhaps best demonstrated by the ‘Arab spring’ where the internet has played a significant role in the downfall of Hosni Mubarak, Muammar Gadaffi and President Zine El Abidine Ben Ali. Communication was/is critical to the Arab spring because the uprisings took place in countries where the conventional media was closely controlled by the government.

In countries with a free press, clearly the enhanced ability to communicate does not have the same implications. Although, it might be said that the growth in social media including the blogosphere has diminished the ability of the government of the day to control its message. It might also be noted that Wikileaks (if it survives) is an internet phenomenon capable of substantially diminishing the independent power of government. New laws have been introduced to penalise cyber bullying and also an education program. Bullying is not new but the potential for the bully to be outside the jurisdiction recreates a new challenge for law enforcement. The current conflict between internet service providers and copyright rights holders arises from the ability of users online to infringe copyright on a significant scale in flagrant disregard for the terms of the Copyright Act 1968 (Cth).

2.4 Distributed control

Governance of the internet itself has been the subject of many papers. The distributed nature of the technology and the lack of any central point of control have the government struggling with how best it can exercise its authority in relation to what happens online.

In the physical world the defence of Australia is a matter of the protection of Australia’s borders by the army navy and air force. The ability to disrupt the economy, commit fraud or steal information is constrained by time and distance. The online environment is different. The robustness of the internet depends upon the security precautions and information sharing across the network internationally.

For some there is also an issue regarding control of ‘cyberspace’ in the sense of the virtual environments that exist online.

2.5 Summary of examples discussed in this paper

We set out in the following table some recent examples of internet related regulation and attempt to identify technological or social phenomenon that gave rise to the need for new regulation.
<table>
<thead>
<tr>
<th>Issue</th>
<th>Lack of control</th>
<th>Cause</th>
<th>Strategy being adopted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to online gambling services</td>
<td>extensive use of services despite prohibition</td>
<td>access</td>
<td>regulate local industry</td>
</tr>
<tr>
<td>Growth of online retailing</td>
<td>inability to collect GST on small packages from overseas</td>
<td>access</td>
<td></td>
</tr>
<tr>
<td>Use of e-mail services from overseas</td>
<td>no ability to intercept and webmail</td>
<td>access</td>
<td></td>
</tr>
<tr>
<td>Sharing of information with overseas businesses</td>
<td>local privacy and Spam rules do not apply</td>
<td>access</td>
<td>cooperation with international agencies in relation to spam</td>
</tr>
<tr>
<td>Regulator impost on Australian media</td>
<td>IP TV and on demand services available online do not comply</td>
<td>access</td>
<td>Under consideration</td>
</tr>
<tr>
<td>Protection of military information and software</td>
<td>risk of disclosure by electronic means</td>
<td>access</td>
<td>expansion of statutory regime and imposition of penalties beyond Australia’s borders</td>
</tr>
<tr>
<td>Protection of children online</td>
<td>lack of visibility to parents and law enforcement of online activity</td>
<td>communication</td>
<td>education, industry codes and interception</td>
</tr>
<tr>
<td>Protection against zombies online</td>
<td>attack can originate from anywhere in the world</td>
<td>distributed control</td>
<td>industry code and international cooperation</td>
</tr>
<tr>
<td>Protection of critical infrastructure</td>
<td>nature and location of critical internet infrastructure may not be planned or fully recognised. attack can be electronic or physical in nature</td>
<td>distributed control</td>
<td>Establish agency responsibility and Computer Emergency response Team (CERT) work with AusCert.</td>
</tr>
</tbody>
</table>

3. **What are the limits on the law making power of the Australian government?**

The Commonwealth Parliament has extraterritorial power to make law extending beyond Australia’s geographical boundaries. This means, the government’s power to make law regulating activities conducted over the internet extends to people inside and outside Australia. Of course, matters relating to administering and enforcing laws beyond Australia’s boundaries also need to be thought through as part of deciding whether it will be effective to regulate.

Any description of the practical reach of sovereign power must be multi-layered. We separate our review as follows:

(a) the power to make law;

(b) the way laws can be written to extend reach beyond national borders; and

(c) the principles applying to enforcement. That is, when are the courts able to act to enforce a law?
3.1 Power of the Australian Parliament to make law

Commonwealth Parliament has extraterritorial power

The Australian Constitution creates the body of rules constituting the power to make Commonwealth laws. The legislative sovereignty of the Commonwealth Parliament is specifically conferred by s 51 of the Constitution. Section 51 provides that Parliament shall have power to make laws for the ‘peace, order and good government of the Commonwealth’ in relation to specified matters.

Various powers in s 51 have been relied upon to regulate activity outside of Australia, including activity conducted over the internet. For example, the Parliament has enacted legislation that operates extraterritorially to Australia under the external affairs power. Under the external affairs power (s 51(xxix)) laws made concerning issues external to Australia include extradition, diplomacy and the ratification of international treaties.

Another Constitutional power relied upon to make laws with extraterritorial effect is s 51(v), which gives the Commonwealth Parliament the power to make laws with respect to ‘postal, telegraphic, telephonic and other like services’. The words ‘like services’ have been interpreted to include electronic communication technologies that post date the Constitution including broadcasting and the internet.\(^7\) Relevantly, using this power the Commonwealth regulates the electronic media including under the \textit{Broadcasting Services Act 1992 (Cth)} (BSA).

Limits to the power to legislate

There are limits to the power to legislate. The Commonwealth Parliament’s power to make laws is limited by the powers conferred by the Australian Constitution. Power is also limited by the inherent jurisdictional limitation of a nation to make laws for its own governance. Governing bodies only have the capacity to make laws for their own country and that they are not, to quote Gavin Skene, ‘capable of legislating for the whole world’.\(^8\)

Principles of international law also place limits on a government’s power to legislate to control activities outside its geographical territory. In summary, extraterritorial acts may only be lawfully within a government’s jurisdiction if the following general principles (General Principles) are observed:\(^9\)

(a) there should be a substantial and bona fide connection between the subject-matter and source of the jurisdiction;
(b) the principle of non-intervention in the domestic or territorial jurisdiction of other states should be observed; and
(c) a principle based on elements of accommodation, mutuality and proportionality should be applied. Nationals resident abroad should not be constrained to violate the law of the place of residence.

3.2 How laws are written to extend beyond national borders?

Numerous laws with extraterritorial operation

A discussion about constraints on the Commonwealth government’s ability to regulate the internet should recognise that the Commonwealth Parliament has passed many laws with extraterritorial operation.

Criminal Code Division 15 — extended geographical jurisdiction categories

The Commonwealth government’s approach to legislating for extraterritorial jurisdiction in criminal matters is illustrated by the extended geographical jurisdiction categories established under Division 15 of the Criminal Code.\(^10\) These categories are identified as applying to certain statutory offences.
If, for an offence, a person’s status, conduct and/or the results of the conduct trigger the extraterritorial rules in the applicable category, a person is guilty of that offence.

The framework established by Division 15 illustrates that the Commonwealth Parliament has considered it necessary for the peace, order and good government of the Commonwealth to make certain conduct an offence under Australian law, even when committed outside Australia by a non resident or non citizen or where a result of the conduct does not occur wholly or partly in Australia. The framework also clearly shows that there is a structure available to the Commonwealth Parliament to make activity conducted over the internet an offence, even though the conduct has little connection with Australia.

The four categories can be described broadly (and somewhat inaccurately for the sake of brevity) as follows:  

**Category A**

(a) The conduct constituting the alleged offence occurs:
   
   (i) wholly or partly in Australia: or
   
   (ii) wholly outside Australia and a result of the conduct occurs wholly or partly in Australia; or
   
   (iii) wholly outside Australia and the person is an Australian citizen or a body corporate incorporated in Australia; or
   
   (b) all of the following conditions are satisfied:
      
      (i) the alleged offence is an ancillary offence;  
      
      (ii) the conduct constituting the alleged of fence occurs wholly outside Australia;
      
      (iii) the conduct constituting the primary offence relating to the ancillary offence, or a result of that conduct, occurs, or is intended by the person to occur, wholly or partly in Australia.

Defences to a Category A offence are where the alleged offender is neither an Australian citizen nor a body corporate incorporated in Australia, the conduct takes place outside Australia and there is not in force in the foreign country where the conduct constituting the alleged offence occurs a law of that foreign country, or a law of that part of that foreign country, that creates an offence that corresponds to the first-mentioned offence.

For example, for a Category A offence, the result of the conduct may occur wholly or partly in Australia but a non citizen outside Australia will have a defence.

**Category B**

This category is the same as Category A, except that the extended operation additionally applies to conduct by an Australian resident.

**Category C**

If Category C is identified as applying to an offence, the offence applies whether or not:

(a) the conduct constituting the alleged offence occurs in Australia; and

(b) a result of the conduct constituting the alleged offence occurs in Australia.

As with Categories A and B, defences to an offence within Category C are available where the alleged offender is neither an Australian citizen nor a body corporate incorporated in Australia, the conduct takes place outside Australia and there is not in force in the foreign country where the conduct constituting the alleged offence occurs a law of that foreign country, or a law of that part of that foreign country, that creates an offence that corresponds to the first-mentioned offence.
If Category D is identified as applying to an offence, the offence applies whether or not:
(a) the conduct constituting the alleged offence occurs in Australia; and
(b) a result of the conduct constituting the alleged offence occurs in Australia.

There is no defence to offences in Category D.

The following table gives examples of the types of offences within each category.\textsuperscript{15}

<table>
<thead>
<tr>
<th>Category A</th>
<th>Identity fraud offences, postal offences (such as hoaxes, threats or the mailing of dangerous articles), offences relating to use of postal or similar service for child pornography material or child abuse material offences under Part 10.6 of the Criminal Code (telecommunications services) and offences under Part 10.7 of the Criminal Code (computer offences).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category B</td>
<td>Offences related to plastic explosives, people smuggling, trafficking of persons, serious drug offences, urging violence against groups or members of groups and sexual servitude offences.</td>
</tr>
<tr>
<td>Category C</td>
<td>Unwarranted demands, various postal offences (including tampering with articles) and dishonestly obtaining delivery of articles, impersonating a government official (and other related offences) and causing a dangerous or explosive article to be carried by post.</td>
</tr>
<tr>
<td>Category D</td>
<td>Providing prohibited online gambling services to Australian customers\textsuperscript{16} or customers in designated countries,\textsuperscript{17} treason and urging violence, espionage, terrorist acts or organisations and offences related to terrorist acts, various theft and property offences, bribery offences, forgery offences, genocide and torture.</td>
</tr>
</tbody>
</table>

The operation of Division 15 remains largely untested. This may change in the near future.

**Defence Trade Compliance Bill 2011**

An upcoming internet relevant example of legislation which will seek to rely upon Division 15 for its operation, is the Defence Trade Compliance Bill 2011 (Bill).\textsuperscript{18} Section 8 of the Bill applies the proposed Act to activities outside Australia.

Among other things, the Bill seeks to regulate intangible transfer of controlled technology. Currently, technology listed in the *Defence Strategic Goods List* (DSGL)\textsuperscript{19} requires permission to be exported in the form of a good. The government does not have authority to control identical technology when transferred by intangible means (e.g. via email or the internet such as exporting software by electronic download).\textsuperscript{20} Regulation of intangible technology transfers is being implemented as part of Australia’s obligations as a member of the major arms and dual use export control regimes.\textsuperscript{21}

The Bill contains some ‘deemed exports’ for intangible transfers. These are to regulate for:
(a) transfer of controlled technology from within Australia to outside Australia by a foreign person to a foreign person;\textsuperscript{22}
(b) transfer of controlled technology by an Australian person supplying to a foreign person.\textsuperscript{23} This section applies regardless of the location of the Australian person or foreign person;
(c) an Australian providing controlled defence services to a foreign person that are received outside Australia;\textsuperscript{24} and
(d) a person providing controlled defence services to a foreign person that are received in Australia.\textsuperscript{25}
All the above activities to be newly regulated could occur thought intangible transfer over the internet. Unless an exception applies, it will be an offence to undertake any of the above activities without a permit. The activities are designated as Category B offences under the Criminal Code.26

A number of countries including the United States,27 the United Kingdom and Japan already regulate intangible transfers of controlled technology.

Practically, there are likely to be issues concerning how the Commonwealth government will effectively publicise, detect and enforce the new laws. Businesses are also likely to be concerned about the risk of incidental breach, particularly for email and internet communications given the ease of making these communications.

Other examples of Commonwealth legislation with relevant express extra-territorial operation

Other examples of Commonwealth legislation with relevant express extra-territorial operation include:

- **The Competition and Consumer Act 2010 (CCA):** Section 6 gives extraterritorial application to some parts of the CCA, namely by use of the Constitutional foreign trade and commerce power and the telecommunications power. Section 6 has been successfully relied upon by the Australian Competition and Consumer Commission (ACCC) to seek relief in relation to ecommerce transactions by a party located outside Australia. For example, *ACCC v Chen* (2003) 201 ALR 40 concerned an individual operating a business from the United States representing it had a false association with the Sydney Opera House. The court found that section 6 of the then *Trade Practices Act 1974 (Cth)* (TPA)28 applied to the individual’s activities, at least in so far as they affected consumers in Australia. This was because he had engaged in conduct over the internet which involved the use of telephonic services (s 6(3)) or, alternatively, which has taken place in trade or commerce between Australia and the United States (s 6(2)).29 The court found the extended application of the TPA had the effect that a person outside Australia (but subject to the jurisdiction of the Federal Court) might contravene the TPA and thereby enliven the Court’s power to grant an injunction prohibiting or requiring the performance of acts outside Australia.30

- **The Corporations Act 2001 (Corporations Act):** Section 5 of the Corporations Act extends the operation of ‘each provision of this Act … according to its tenor’ to places outside the jurisdiction specifically providing in subsection 5(7) that the act applies to natural persons whether resident or not and Australian citizens or not and to all bodies corporate and unincorporated bodies whether formed or carrying on business in Australia. This is done through requiring foreign companies to register. A foreign company may not carry on business in Australia unless registered or where a registration application is pending, and this builds on the common law requirement that a foreign company be amenable to local laws by being ‘present’ in a jurisdiction.31

  The WMD Act is stated to apply to acts and omissions done by Australian citizens, residents and companies outside Australia (as well as to things done inside Australia) (section 6(3)). The WMD Act provides the ability to regulate an intangible transfer (such as transferring technology or providing a service over the internet) if the technology or service is related to a WMD program.

4. Enforcement beyond national boarders

It is one thing to make a law purporting to bind the citizens of another country, not resident in Australia in relation to conduct taking place outside Australia. It is another to be able to enforce that law. In the context of regulating activity conducted over the internet, we see the ability to enforce and practicalities of enforcement as the major challenge (rather than the power to make laws in the first place).
4.1 Jurisdiction of the FCA

In order to illustrate the practical limitations on law enforcement, in this section we consider the circumstances in which the Federal Court of Australia (FCA) will exercise jurisdiction over a person or entity.

For the FCA to have jurisdiction over an extraterritorial or foreign matter, the FCA must be satisfied that it has the capacity to exercise authority over a defendant under the matter (personal jurisdiction). The FCA must also be satisfied that it also has subject-matter jurisdiction. This means that the issue and subject-matter under consideration must fall within the ambit of those issues suitable for consideration by the FCA.

There are differences between the FCA's personal jurisdiction in civil matters and its jurisdiction in criminal matters. In civil matters, the personal jurisdiction of the FCA requires valid service of the defendant party, or else voluntary submission of that party in order for jurisdiction to be exercised. This aspect of civil jurisdiction arises from common law. The common law requires that an originating process be served in order to gain personal jurisdiction over a matter. Statutory provisions also operate and are available under Order 10.41, explained below.

Note section 64 of the Interactive Gambling Act 2001 (Cth) (IGA) provides that where a summons or process is required to be served on a body corporate incorporated outside Australia and the body corporate does not have a registered office or a principal office in Australia and the body corporate has an agent in Australia, service of the summons or process may be effected by serving it on the agent.

Service in a civil matter can take place either inside or outside of Australia under Order 10.41 of the FCA Rules 2011, which allows for jurisdiction to extend to service of a defendant outside of Australia in certain specified circumstances. These circumstances include where a proceeding is based on a cause of action arising in Australia including breach of contract, proceedings related to contract, tort, or contravention of an Act committed in Australia, and allows for service of a foreign company carrying on business in Australia (to achieve outcomes including injunctions etc). However, Order 10.14 applies to civil matters only and does not extend to criminal matters.

Broadly, Australian criminal law applies to both foreign individuals and corporations in respect of offences committed in Australia. To establish jurisdiction in the FCA, the FCA must — following an indictment or similar approach to the court — issue either a summons or a warrant for arrest on the defendant; a summons being non-coercive in nature and the warrant being compulsory in nature.

4.2 Extradition

Where the defendant is not physically located in Australia, a summons or warrant will not be effective, and the FCA will be unable to claim jurisdiction over the defendant. In this case, an extradition order will need to be sought. One way this can be achieved is through the Extradition Act 1988 (Cth), which applies in cases where a person has committed an offence punishable by twelve months or more imprisonment, and can be found to be located in a foreign State with whom Australia has an extradition treaty. Under the Act, an individual cannot be extradited where to do so would offend the ‘double criminality’ principle; meaning that the State where the individual is currently located does not have to extradite the individual where that State does not recognise the criminality of the offence. Therefore, where certain acts do not constitute crimes in the State where the defendant is residing, it is unlikely that an extradition order would be successful.

The Commonwealth also retains the power to require a State to surrender a fugitive in the absence of a treaty, through means of diplomatic comity. In this sense, the relationship between States can make or break the success of an extradition request, and this can impact upon the ability for the FCA to exert personal jurisdiction over foreign individuals who have broken Australian law.
4.3 Enforcement of foreign judgments in Australia

In Australia the enforcement of foreign judgements is governed by the *Foreign Judgements Act 1991* (Cth), which covers both judgements enforced in Australia (made in external jurisdictions) and the enforcement of Australian judgements overseas. The procedure for enforcing an Australian judgment in a foreign jurisdiction varies between countries and depends largely on whether or not Australia has a reciprocal enforcement arrangement with the country where the judgement is to be enforced.

Some common prerequisites to effectively getting an Australian judgement enforced overseas include ensuring that the application to the foreign court includes a certified copy of the Australian judgement, an affidavit identifying the defendant and stating the sum payable in the currency of the foreign country. In countries such as the United States where no reciprocal enforcement arrangements exist, the process is difficult and often involves commencing a new law suit for the debt arising from the judgement.

4.4 Treaties and multilateral cooperative arrangements

In addition to extradition treaties, traditional ways of overcoming the limits of State sovereignty also include the implementation of treaties to create strategic cross-border alliances. This approach recognises the limitations of traditional sovereign authority, and attempts to bypass this through strategic reliance on international neighbours and allies. Examples of relevant treaties ratified by Australia include the Universal Copyright Convention, ASEAN Australia–New Zealand Free Trade Agreement and the Australia–United States Free Trade Agreement. These laws have each determined the form and content of Australian law.

The major arms and dual use export control regimes (mentioned above in relation to best practice export controls) illustrates difficulties in implementing consistent regulatory regimes across member countries. The member countries collectively develop lists of goods to be controlled for export and best practice guidelines on export. However, the member countries each apply a number of different approaches in implementing their obligations. This can make it difficult for organisations seeking to manage and apply consistent export control approaches globally. For example:

(a) at any one time, member countries will be applying different versions of the list;
(b) as noted above, some but not all member countries, regulate intangible transfers such as transfers of controlled technology over the internet; and
(c) the member countries each apply their own interpretation approach to whether an item is controlled under the list. What is controlled in one country may be uncontrolled in another.

4.5 Direct prohibitions

The Federal government has the power by legislative control over telecommunications services to create an internet filter to block access to foreign websites. In fact, as discussed below in relation to Schedules 5 and 7 of the *Broadcasting Services Act 1992* (Cth) (BSA), provision for the blocking of online content has already been legislated. Blocking is the ultimate form of direct action that the Australian government could take to maintain (perhaps expand) sovereign power. As has been witnessed during the debate over content filtering, this is not a politically attractive option (e.g. the benefits of filtering out child pornographic images have been debated against concerns about whether the filters are effective and also concerns about lack of transparency in development of the lists). However, as the internet becomes more critical to every part of the economy and the issues of control discussed in this paper become more important, increasing direct control by government remains a possibility.

The *Interactive Gambling Act 2001* (Cth) (IGA) is aimed at minimising problem gambling among Australians. The IGA prohibits providing online gambling services to Australians. The prohibition
applies to all interactive gambling service providers, whether based in Australia or offshore, and whether Australian or foreign-owned.

However, the IGA does not prohibit Australian customers accessing and using prohibited interactive gambling services. In practice, Australian customers have been easily accessing online gambling services from operators outside Australia. This raises the concern that Australian customers are accessing services from overseas operators who may not be subject to sufficient regulatory oversight to address problem gambling and other concerns.

The IGA is currently under review. The IGA has been identified as effective in preventing companies in Australia from selling online gaming services to Australians. However, the IGA has not prevented Australians from accessing interactive gaming services outside Australia. In particular, it has been noted that:

- The global nature of the internet means that online gambling services can be based in any country and made accessible to Australians. In practice, there have been few allegations of Australian-based companies offering prohibited online gambling services to Australians. Most allegations of companies offering prohibited services to Australians concern overseas-based companies. While the IGA applies to providers in other countries, there is limited practical scope for Australian law enforcement agencies to pursue, with any prospect of success, foreign-based providers.

- As noted above, the IGA has extraterritorial application by extending to ‘acts, omissions, matters and things outside Australia’. The IGA makes it a criminal offence with a Category D designation under Division 15 of the Criminal Code to intentionally provide an interactive gambling service to customers physically present in Australia. The IGA attempts to encourage preventative action by a foreign service provider by saying that the following matters will be taken into account when determining whether the offender intended to breach the section:
  
  (a) whether prospective customers were informed that Australian law prohibits the provision of the service to customers who are physically present in Australia;
  
  (b) whether customers were required to enter into contracts that were subject to an express condition that the customer was not to use the service if the customer was physically present in Australia;
  
  (c) whether the person required customers to provide personal details and, if so, whether those details suggested that the customer was not physically present in Australia; and
  
  (d) whether the person has network data that indicates that customers were physically present outside Australia:
    
    (i) when the relevant customer account was opened; and
    
    (ii) throughout the period when the service was provided to the customer.

The IGA provides that, where the Australian Media and Communications Authority (ACMA) is satisfied that internet content hosted outside Australia is prohibited internet gambling content, ACMA may notify the content to the Australian Federal Police (AFP) or another suitable body inside or outside Australia, subject to the creation of an enforcement scheme (that has not been created), notify ISPs or give each ISP known to ACMA a standard access-prevention notice requiring the content to be blocked. In fact the power to issue an access prevention notice is circumscribed by later provisions that permit ISPs to rely on providing a voluntary internet filter as a substitute measure.

As already noted, despite the IGA’s quite comprehensive prohibition on Australian and overseas operators providing online gambling services to Australian customers, the IGA has been largely ineffective in reducing online gambling. Australian customers can easily access overseas services. The Productivity Commission estimates that Australians gamble approximately $790 million per annum (based on figures for 2008/2009) on online gambling games of the kind banned by the
The Productivity Commission also estimates that 4% of the adult population or around 700,000 Australians have online betting accounts with such services. From July 2010 to June 2011, the ACMA completed 48 investigations into alleged breaches of the IGA. Of these, 38 involved overseas-hosted prohibited internet gambling content and the URLs were notified to the AFP, while seven involved overseas-hosted content that was found not to be in breach the IGA and were not referred on. Three investigations were terminated due to insufficient information. During the same period, the ACMA referred one Australian hosted site to the AFP for action.

There are also a range of regulatory approaches across countries taken towards online gambling. The lack of a uniform approach among countries towards regulating such internet activity makes it a challenge to assess how best to regulate online gambling in Australia.

The limitations with the IGA pose some questions. Should the government prohibit offering online gambling services when unregulated services provided by operators outside Australia can be easily accessed? Alternatively, can the government better protect Australian customers by trying a different approach? For example, to allow online gambling in Australia on a regulated basis so as to encourage Australian customers to use Australian providers operating within the regulatory regime.

4.6 Indirect or secondary restrictions

Perhaps to recognise both the legal and practical limits of direct regulation, the Commonwealth Parliament has also adopted secondary restrictions designed to inhibit the impact of conduct outside the jurisdiction on Australia.

The BSA specifically regulates the internet. Schedule 5 of the BSA takes a ‘border control’ approach to stopping harmful overseas content from entering Australia. Under Schedule 5, an internet service provider (ISP) is required to block access from Australia to prohibited internet content hosted outside of Australia once certain notification requirements have been met. A similar mechanism exists in Schedule 7 of the BSA for foreign content the subject of a complaint that has been classified RC. In taking a secondary approach to regulation, it might be said Schedule 5 of the BSA operates as a form of ‘border control’. However, the direct blocking mechanism is not, in fact in use, a ‘recognised alternative access-prevention arrangement’ is in place via an industry code of practice whereby the offensive content is notified to the providers of ‘family friendly’ filter software so that the sites are include in the content blocked by those using the filters.

The Privacy Act 1988 (Privacy Act) contains in Schedule 3, National Privacy Principle (NPP) 9 which restricts the transfer of personal information from Australian shores subject to a number of conditions. These include ‘that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles’. A common means of satisfying this requirement is to put in place a data transfer agreement that requires a party outside Australia to abide by the privacy laws that bind the Australian entity. In this way, NPP 9 uses civil law to extend the operation of the Privacy Act outside Australia.

The Spam Act 2003 (Cth) (Spam Act) extends to ‘acts, omissions, matters and things outside Australia’ and creates an offence for sending an unauthorised commercial electronic message with an Australian link. The Spam Act contains only civil penalty provisions and does not, therefore, have express operation in accordance with the Criminal Code. However, the Spam Act makes provision for an international treaty dealing with Spam. Section 45 provides that regulations may make provision for and in relation to giving effect to an international that deals with commercial electronic messages and/or address harvesting software.
4.7 Permitting harmful conduct within a regulated regime

As mentioned above the Productivity Commission in its report on the IGA concluded that regulated access to licensed providers (both in Australia and overseas), subject to a strong regime of consumer protection, could play a role in reducing harm to online gamblers and provide better outcomes for consumers by encouraging competition.

Schedule 7 of the BSA contains a regulated access approach. Online content rated less than MA 15+ does not need to be classified. Online content rated MA 15+ or more that is hosted by a commercial content service provider in Australia must be classified by a certified classifier and made available only behind compliant age warning notices. If the content is not hosted in Australia, ACMA may review it and have it classified in response to a complaint but their only enforcement response is to add the address of the offensive content to the list of sites to be blocked by participating industry content filters. This regime is interesting because it appears to be designed around the practical limitations on the government’s power to take action against internet content posted overseas. The content is tolerated until it has complained about. Only then is it added to the list of sites that will be blocked by content filters. This regime stands in stark contrast to the traditional operation of the film and literature classification board with films and magazines were required to be classified and were prohibited from publication until unless the regulator was satisfied that the content was within acceptable limits.

5. Out of reach: observations on the limits on the exercise of sovereign power by the Australian government

It is demonstrated both by the theoretical reach of parliamentary authority and by the extended operation of existing legislation, that Australian law may purport to regulate almost any conduct taking place almost anywhere provided a relevant head of power can be identified, the law can be said to be for the peace, order and good government of Australia and the General Principles are observed.

In circumstances where there is a perceived harm suffered in Australia but the act giving rise to the harm took place outside the country, the challenge for legislators in almost every case is not whether the Parliament may make a law banning the relevant conduct, but rather whether there is a way of controlling the conduct by regulation that operates within the jurisdiction or, alternatively, whether an law with extraterritorial force be enforced.

The key factors that are relevant to whether or not a law can be enforced are:

- is the responsible entity or person present in the jurisdiction or likely to visit?
- is the offending act of breach of the law in the country where it took place?
- did the action take place in the country that is prepared to allow Australia to enforce its law?
- will the country where the act took place extradite the offending person?
- will a country where the act took place enforce an Australian judgement against the party who committed the offending act?

There are also other threshold questions. For example, whether it is possible to identify who committed the offending act or where the act took place. Additionally, there is the practical question of whether the contravention was sufficiently serious to justify the costs of attempting international enforcement.

The answers to these questions clearly depend on a number of factors. First among them is the nature of the offending conduct. Certain criminal acts are the subject of international law enforcement treaties and contraventions are pursued by international law enforcement agencies. The
recovery of civil debts may be enforced in countries that are signatories to enforcement of foreign judgements legislation.

However, in looking for some general observations, there appear to be two significant areas that are clearly beyond the reach of local law enforcement:

- where the business or service is legal in the jurisdiction where it is being provided but illegal in Australia; and
- where the business or service originates from a country that does not co-operate with international law enforcement agencies and/or has weak institutions and little-effective law enforcement.

From the perspective of social regulation, the first of these is the most significant. Examples of how the ability to regulate services that are legal in other jurisdictions has directly undermined the ability of the Australian government to enforce rules in relation to Australians include:

- Where Australian websites and social media are used by people outside Australia who are based in jurisdictions with privacy laws and online marketing law different from those in Australia. Marketing messages that comply with Australia’s Spam laws and behavioural tracking (taking place in this cause with Australian guidelines) can be illegal under the law in place in many European countries.

- Where Australian customers use casino style gambling services offered from jurisdictions where they are legal. Note that it is legal for Australian businesses to provide interactive gambling services outside Australia.

- Where digital media such as interactive games, software, music and movies are purchased by Australians from international websites that do not have a presence in Australia. The classifications and age warnings that are displayed by the sites do not comply with Australian law but are not illegal in the place of origin.

From the perspective of protecting Australia’s IT infrastructure and also in terms of the risk to Australians from fraud and exploitation online, the second area is also very significant.

6. Moderating factor: the global business

It does not reflect reality to simply assume that all businesses operating from outside Australia, but providing services to Australians, will comply with the law of the place where they are operating and disregard Australian law. This has not been our experience, particularly in relation to large international service providers.

In our experience, major global online brands regularly take advice regarding the local regulatory environment of each of the jurisdictions in which they operate and where possible, take steps to accommodate local laws by adopting local languages, submitting to local consumer protection laws and otherwise complying with regulatory requirements.

Good citizenship of this kind is considered necessary to maintain a positive brand image and to avoid more direct regulatory intervention by local authorities.

It is an important point that compliance by many international on-line services is voluntary rather than mandatory. This shift from a mandatory compliance with the law to voluntary compliance represents a significant shift in the source and nature of the power of government. Situations can arise where detailed country specific requirements are too complex and difficult to implement as part of a global system. Governments often negotiate with stake holders regarding the detail of regulation particularly in terms of what is practical and what is economic, however it is a relatively new phenomenon for the government to be negotiating in a situation where it has no direct legislative power to impose its decision on the party wishes to regulate.
7. Conclusions

The government has available and has used a range of mechanisms to control activity online including:

(a) directly prohibiting a person whether inside or outside of Australia from engaging in the harmful conduct. This may be effective in stopping providers in Australia providing those services, but potentially ineffective against overseas providers if they are not subject to enforcement action. For example, if customers in Australia can still easily obtain the services from overseas, the prohibition may seem wasted effort;

(b) secondary or indirect prohibitions. This approach places the prohibition on a person within the government’s reach (i.e. in the jurisdiction) but who is not the originator of the perceived harmful conduct. The practicality and effectiveness of imposing such a burden on a person who has not caused the harmful conduct always needs to be carefully considered;

(c) permitting the harmful conduct within a regulated regime. This approach allows potentially harmful conduct but with certain controls and safeguards in place;

(d) perhaps one of the most interesting mechanisms tried is the provision in the interactive gambling act to prohibit Australian businesses from providing interactive gambling services to the citizens of jurisdictions that also prohibit their businesses from providing interactive gambling services to Australians. Unfortunately no other countries took advantage of this mechanism;

(e) the government also has the controversial power to require blocking of foreign websites. The possibility of this option is a source of leverage for the government when dealing with service providers based outside Australia. However the political fallout from adopting what might be regarded as an undemocratic approach to regulation generally keeps this option off the table; and

(f) creating and implementing treaties to make laws consistent across borders and multi-national cooperative arrangements. These are limited in effectiveness by the number of participating countries and the extent to which the laws are implemented consistently;

However, it is clear that the growth of the internet has had a direct impact on the sovereignty of the Australian government. Most significantly:

- access to online services originating from outside jurisdiction that operate within the laws of their home country cannot be directly regulated by Australian law;
- the direct availability of online services from offshore also has a direct impact on the economic viability of Australian services, creating pressure for the Australian government to avoid rules and restrictions which put local businesses at a disadvantage;
- the increased power of Australians to communicate with one another directly online has not had an impact of the same magnitude as the impact in the closed societies of the Arab world. However it seems arguable that online access to source materials, direct access to ministerial statements, original source documents and the largely unregulated commentary from the blogosphere has diminished the ability of government control its message;
- it is also clear that the social media is creating new challenges in the area of protection of children; and
- the nature of the internet as a distributed system with the dependencies and connections that go beyond the jurisdiction of the Australian government also creates particular challenges.

In our view, some of these changes represent a permanent shift. In particular, increased exposure of Australian businesses to international competitors will be an important factor in determining the business regulation going forward. When creating rules in relation to a wide range of matters including access to online content, privacy, licence fees and reporting requirements the Australian
government will need to consider not only the impact on the comparative advantage of Australian businesses but also whether international service providers operating in Australia will choose to comply.

Issues related to the distributed nature of the internet require a new approach to regulation. Co-operative schemes such as the Internet Industry Association iCode\textsuperscript{56} demonstrate a distributed approach to governance which may be the paradigm for regulating in cyberspace.

1 The Convergence Review is described by the Department of Broadband, Communications and the Digital Economy as ‘an independent review established by the Australian Government to examine the policy and regulatory frameworks that apply to the converged media and communications landscape in Australia’. See http://www.dbcde.gov.au/digital_economy/convergence_review.


6 The Imperial Statute of Westminster 1931 implemented in Australia by the Statute of Westminster Adoption Act 1942 (Cth) declared that the Commonwealth parliament has full power to make laws having extraterritorial operation. Jones v Commonwealth (1965) 112 CLR 206; Interactive Gambling Act 2001 (Cth).


8 XYZ v Commonwealth (2006) 227 ALR 495 per Gleeson CJ at 498 referring to Professor Brownlie’s summary of the effect of international law as contained in I Brownlie, Principles of Public International Law, 6\textsuperscript{th} ed, Oxford University Press, New York 2003, p. 309.

9 Contains in the Schedule to the Criminal Code Act 1995 (Cth).

10 For the purposes of summarising the categories, ‘Australia’ includes on board an Australian aircraft or an Australian ship.

11 For example, an ancillary offence includes attempting to commit an offence or aiding and abetting, incitement or conspiracy to commit a primary offence. See Criminal Code Act 1995 (Cth) Part 2.4, Division 11.

12 A primary offence is an offence against a law of the Commonwealth that is not an ancillary offence.

13 The treatment of defences for primary and ancillary offences is slightly different.

14 The majority of the listed offences are contained in the Criminal Code. However, the categories are also designated as applying in other legislation containing Commonwealth offences.

15 IGA s 15(5).

16 IGA s 15A(5).

17 The exposure draft for the Bill was released on 15 July 2011 followed by a consultation period that closed on 26 August 2011. See http://www.defence.gov.au/strategy/deco/usec/treaty.htm. The Bill was introduced into the House of Representatives on 2 November 2011.

18 The current version at the time of writing is the Defence and Strategic Goods List Amendment 2011 (effective 14 October 2011). There is an ability to regulate an intangible transfer if the technology is related to a weapon of mass destruction (WMD) program under the Weapons of Mass Destruction (Prevention and Proliferation) Act 1995 (Cth) or if covered as a sanction implemented domestically under the Charter of the United Nations Act 1945 (Cth).

19 Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Goods and Technologies; Australia Group; Nuclear Suppliers Group; and Missile Technology Control Regime.

20 Section 10(1)(b)(i).

21 Under the Export Administration Regulations and other regulatory regimes. The predecessor to the Competition and Consumer Act 2010.

22 ACCC v Chen (2003) 201 ALR 40 at 47 per Sackville J.
Section 601CD Corporations Act; Re Kalis Groote Eylandt Fisheries Pty Ltd (rec and mgr apptd) (1977) 2 ACLR 574.

Flaherty v Girgis (1987) 162 CLR 574.


Crimes Act 1914 (Cth) s 4B(1).

Extradition Act 1988 (Cth).


There are currently 40 member countries.


Call for submissions Discussion Paper released on 24 August 2011 by the Department of Broadband, Communications and the Digital Economy, page 12.

Interactive Gambling Act 2001 (Cth) s 14.

Interactive Gambling Act 2001 (Cth) s 15

Interactive Gambling Act 2001 (Cth) s 24.


Some of these are outlined in Call for submissions Discussion Paper released on 24 August 2011 by the Department of Broadband, Communications and the Digital Economy.

Schedule 5 of the BSA imposes certain obligations on internet service providers in relation to dealing with prohibited content hosted outside Australia.

Spam Act s 14.

‘Australian link’ is defined in s 7 of the Spam Act.