

- 30 For example, Sony has recently announced that it has accepted Microsoft's media player as its format of choice.
- 31 See Sahane Simpson, "Moving Towards Copyright Control on the Internet", *Media Arts Law Review*, Vol. 1, December 1996.
- 32 Additional Information about the SDMI can be found at <http://www.sdmi.org>.

- 33 For instance, The Copyright Law Review Committee (CLRC) Simplification Report recommends that no material form be required for copyright to subsist because of problems the concept is likely to pose with digitisation. A copy of that report is available on the Committee's website at <http://www.agps.gov.au/clrc>.

Sean Simmons is an intellectual property solicitor at Phillips Fox, Brisbane.

Sean has previously managed Brisbane bands and is a regular adviser on entertainment and media law issues at the Arts Law Centre of Queensland.

---

# An Essential Guide to Internet Censorship in Australia

*Brendan Scott, Gilbert & Tobin*

---

Brendan is Gilbert & Tobin's electronic business specialist. This paper is an update of an earlier paper "A Layman's Guide to Internet Censorship in Australia" and is current at 1 October 1999. The views expressed in this paper are not necessarily the views of Gilbert & Tobin.

## INTRODUCTION

In 1998 the Federal Liberal Party won Government in Australia by a small majority. The two major policy platforms of its campaign were the introduction of a Goods and Services Tax (GST), and the further partial sale of the incumbent telecommunications carrier, Telstra. At the time Government did not control the Senate, but would be able to secure a majority with the assistance of Senator Brian Harradine. Senator Harradine, is an independent Senator who held the balance of power in the Australian Senate until 30 June 1999. Senator Harradine is known for taking a hard line stance against the availability of pornography.

As a result of the 1998 elections, on 1 July 1999 the balance of power in the Senate was to pass from Senator Harradine to the Australian Democrats. By early March 1999 it had become clear that Australian Democrats were opposed to the Government's two main policy platforms, at least in the forms

presented by the Government. By early March 1999 it was clear that if the Government wanted to make use of Senator Harradine's vote for the passage of the GST and Telstra Sale legislation it would have to do so by 30 June.

On 19 March 1999 the Government announced that it would introduce measures to "protect" Australian citizens against "illegal or offensive" material on the Internet. On 21 April 1999 the Government introduced a Bill (the *Broadcasting Services Amendment (Online Services) Bill 1999*) which makes content hosts and service providers liable for content they carry. The Bill was referred to a Senate Select Committee controlled by the Government. The committee reported back on 11 May 1999 (a little under 3 weeks later). In that short space of time, the committee received 104 submissions in relation to the Bill, a large number of them arguing that it had serious deficiencies. The committee's report endorsed the Bill, suggesting some minor amendments to it. One member of the committee (Senator Harradine) stated that the Bill did not go far enough.

On 26 May 1999 the Bill passed the Senate. By 25 June 1999, barely days before the balance of power in the Senate would pass to the Democrats for years, the Government's legislation on both the part sale of Telstra and on the GST passed the

Senate, and, coincidentally the Online Services Bill had also passed the House of Representatives. Shortly thereafter, the Bill received the Governor-General's assent and became law, although the Act limits itself to things occurring after 1 January 2000 (to give industry participants time to put compliance procedures in place).

The Act is very complex (it's 72 pages of text are not a pleasant read) and, while this paper presents a general overview of the operation of the Act, many of its complexities have been glossed over in order to cover its main themes. You should seek specific advice from your lawyer about how it applies to you and how your risks can be minimised.

## WHAT IS THE ACT ABOUT?

The principle underlying the Act is that the holders and carriers of content should have more liability for content than the creators of that content. The Act establishes two approaches to content regulation. In both cases, the creator or owner of content is not subject to the effects of the legislation. The first approach of the Act deals with internet content hosts and internet content hosted within Australia. The second approach is for internet content hosted outside of Australia.

### **WILL IT JUST AFFECT BAD PEOPLE?**

The Act is the internet equivalent of making the owner of a self storage company liable for the material the public stores in its warehouse. It only affects people who house other people's content or move other people's content from one place to another and it affects them at up to A\$27,500 a day. It does not seek to affect the people who own or create the content.

### **HOW DOES THE ACT WORK?**

The driving force behind the Act are the "online provider rules". Failure to comply with such a rule, or failure to comply with a direction to comply with such a rule means a fine of A\$27,500 per day for companies. The fines apply for every 24 hour period of non-compliance, whether or not business is ordinarily carried on during that time. If compliance is due by a Friday and compliance does not occur until Monday multiple fines apply.

### **ONLINE PROVIDER RULES**

The online provider rules can be broken down into the following categories:

Rules requiring an "internet content host" to comply with a take down notice (to remove content *and not host it in the future*) or with any undertaking they give to the Australian Broadcasting Authority (ABA) to "not host" specified material (these relate to content inside Australia).

Rules requiring "internet service providers" to comply with access prevention notices given by the ABA (these relate to content outside of Australia).

Rules requiring a participant in the internet industry (whether a content host or a service provider) to comply with an industry code or industry standard applicable to that participant; and

A rule requiring a participant to comply with an online provider

determination (rules made up from time to time by the ABA).

As should be evident, this is a complex scheme with many interlocking layers. In the following sections we give a broad outline of each of these categories in turn.

### **TAKE DOWN RULES**

Take down notices are notices issued by the ABA requiring an internet content host to take down prohibited content hosted by that content host within Australia and not to host that content in the future. "Internet content" is information which is accessed or available for access over the internet but excludes "ordinary electronic mail". The Act doesn't provide much guidance on what "ordinary electronic mail" is, apart to say that it doesn't include a posting to a newsgroup. As the word "access" includes "access by way of push technology" (that is, by email or by a newsgroup posting) quite a lot of material is internet content. In fact, if it is possible to send (internet) email from a computer then under the Act, all of the information on that computer that can be attached to an email can be "accessed by way of push technology" - it's internet content. In theory, the only information on such a computer which is not internet content is the "ordinary electronic mail" stored on it.

Under the Act, the ABA can investigate internet content in Australia. It may do so on its own initiative or as a result of a complaint made to it by a, presumably concerned, citizen. Where the ABA discovers that an internet content host is hosting "prohibited content" or it discovers content that is likely to be prohibited content, it must issue a take down notice to that internet content host.

"Prohibited content" is internet content which is rated X (explicit sexuality) or RC (refused classification) under the classification scheme when hosted outside of Australia and, when hosted inside Australia, also includes R rated

material (nudity) which is not subject to a restricted access system. At the moment, no system implemented to restrict access will be a restricted access system. No matter how effective a system is, it will only be "restricted access system" within the meaning of the Act when it has received the ABA's imprimatur.

When a take down notice is received, the recipient has until the following business day to take down the material. However, they must also ensure that, *at all times in the future*, they do not host that content again. The requirement to "not host in the future" will be extremely difficult to comply with, to say the least.

Take down notices also apply only to the extent the relevant content is accessible from a site specified in the notice itself. Technically, if no site is specified, no content has to be taken down. However, the Act doesn't set out what an "internet site" is.

### **ACCESS PREVENTION RULES AND INDUSTRY CODES**

The legislation's approach to content outside Australia is broadly similar to that for content inside Australia in that the ABA issues a notice to a service provider after receiving and investigating a complaint. The basic effect of the notice issued by the ABA is to require the service provider to take reasonable steps to prevent access to specified content, or, if a code or standard is in place, to prevent access to that content in accordance with the code or standard. As for content within Australia, the requirement to restrict access is only limited to the site specified in the notice.

The legislation requires an industry code to be drawn up for internet content hosts and for internet service providers. In the event that a code is unsatisfactory, or is not drawn up quickly enough, the ABA may create an industry standard. Once a code or a standard is in place covering a section of the internet community, then all participants in that section of the community are bound by the relevant standard or code. If the ABA

declares a standard, then failure to comply with it is a breach of the Act, and subject to a fine.

It is the intention of the legislation that, if a code or standard is in place and it deals with a number of specific things, then a person should comply with the code or standard in restricting access. However, if the code does not cover the specific things set out in the legislation, the ABA may send an access prevention notice to the service provider, which requires them to take reasonable steps to prevent access to the content. In determining whether the steps are reasonable, regard must be had to the technical and commercial feasibility of taking the steps. It is not clear whether the same test of reasonableness will be applied across the industry. That is, does a one person operation have to comply to the same standard as an organisation the size of Telstra (the current market incumbent)?

Some of the things that a code or standard is intended to deal with are:

- (a) procedures directed towards the achievement of the objective of ensuring that online accounts are not provided to children without the consent of a parent or responsible adult;
- (b) giving parents and responsible adults information about how to supervise and control children's access to Internet content;
- (c) procedures to be followed in order to assist parents and responsible adults to supervise and control children's access to Internet content;
- (d) procedures to be followed in order to inform producers of Internet content about their legal responsibilities in relation to that content;
- (e) telling customers about their rights to make complaints under the scheme;
- (f) procedures to be followed in order to assist customers to make complaints under the scheme;
- (g) procedures to be followed in order to deal with complaints about unsolicited electronic mail that promotes or advertises one or more:
  - i) Internet sites; or
  - ii) distinct parts of Internet sites;
  - iii) that enable, or purport to enable, end-users to access information that is likely to cause offence to a reasonable adult;
- (h) action to be taken to assist in the development and implementation of Internet content filtering technologies (including labelling technologies);
- (i) giving customers information about the availability, use and appropriate application of Internet content filtering software;
- (j) procedures directed towards the achievement of the objective of ensuring that customers have the option of subscribing to a filtered Internet carriage service;
- (k) procedures directed towards the achievement of the objective of ensuring that, in the event that a participant in the relevant section of the Internet industry becomes aware that an Internet content host is hosting prohibited content in Australia, the host is told about the prohibited content.

All of these obligations can be backed up by the \$27,500/day fine. For example, failure to give parents information about how to supervise and control children's access to internet content can be an offence and subject to a \$27,500 fine for each day (and possibly also for each set of parents) that the person fails to comply with the procedures relating to giving that information. Similarly if a content host fails to inform producers of internet content about their legal responsibilities in relation to that content, they can also be committing an offence.

The Act makes provision for "designated alternative access prevention arrangements". The purpose behind these amendments was to excuse a content host or service provider from complying with access prevention notices if they had an appropriate access prevention arrangement in place. The provisions in the Act refer to not being required to take steps in relation to particular end users where those users have their access subject to a restricted access arrangement. However, if even only one end user hasn't signed up for one of these arrangements the service provider must still keep in place the infrastructure necessary to restrict that user's access.

### **ONLINE PROVIDER DETERMINATION**

Finally, the ABA may make written determinations setting out rules that apply to internet service providers and internet content hosts. These determinations have the force of law of themselves and any failure to comply with an online provider determination will be an offence. An online provider rule might be used by the ABA to augment an industry code, for example.

### **HOSTING**

The word "host" is not defined in the legislation. It would be reasonable to assume that "to host" will require some element of permanence. That is, that "hosting" content in transit via a server for the purpose of enabling that transit is unlikely to be hosting within the meaning of the legislation. The creation of a cache however, will be another matter. It is reasonable to suspect that service providers which host content for third parties will be content hosts within the meaning of the legislation. Where the dividing line will ultimately be drawn is very difficult to tell. For example, will providing a room to house a third party's server and maintaining that server be "hosting"?

## INTERNET SERVICE PROVIDER

The Act defines "internet service provider" very broadly. Effectively any person who provides a carriage service through which a non-employee third person accesses the internet is an internet service provider for the purposes of the legislation. The definition of "internet service provider" in the Act also omits to restrict its meaning to persons providing services partially or wholly within Australia. While it is unlikely that this was Parliament's intent (or that it would be read in this way), there is some scope for arguing that it applies to non Australian service providers, especially given that the corresponding definition of "internet content host" makes a specific reference to hosting within Australia. If this is the case, any access by an Australian to foreign content will make at least one foreign carrier an internet service provider for the purposes of the Act.

Strictly interpreted the definition of "internet service provider" means that, for example, if a given internet circuit is made up of a number of hops, each provided by a separate reseller, each and every reseller will be an internet service provider for the purposes of the Act. In fact, taken to its extreme the parents who purchase an internet access service and the resupply it to their children are also likely to be internet service providers for the purposes of the legislation.

The practical effect of this means that most people who take or provide any form of carriage service within Australia will find it very difficult to escape the operation of the Act, even though it may have no sensible application to them. For example, if a person provides a trunk route between two cities within Australia - but provide carriage only, with no routing or switching functions that person would not normally be considered to be an internet service provider within the ordinary meaning of the term. However, if only one person of the hundreds of

thousands to which use of part of that trunk line is ultimately resold accesses the internet over it, the owner of the trunk will be an internet service provider on a strict reading of the Act. Given that the Act also sets out a scheme which permits ISPs to receive an ABA notification by substituted service (that is, the ISP will be bound if they ought to have known about the notice, even if they did not actually know about the notice) puts carriage service providers in a difficult position. Theoretically they may be liable for a breach of a notice where they weren't aware of the notice, and, indeed, if they were aware of the notice, may not have been aware that they were the covered by it or have any real means of determining whether they were.

## THE GOOD POINTS OF THE ACT

Part 9 of the Act has relatively broad exemptions from liability under State and Territory content regulation laws. In particular State and Territory laws have no effect to the extent that they;

- (a) subject an internet content host to civil or criminal liability for hosting content where the host was not aware of the nature of the content;
- (b) requires an internet content host to monitor, make enquiries about or keep records of internet content hosted by that host;
- (c) subject or could have the effect of subjecting a service provider to liability in relation to content carried when they were not aware of the nature of that content; or
- (d) requires a service provider to monitor, make enquiries about or keep records of content carried by the provider.

This does not mean that content hosts will be immune from Commonwealth laws which have any of these effects (in particular the Act). The Minister may make determinations which have the effect of removing the immunity from specified laws.

## LIABILITY FOR COMPLIANCE

The Act has specific exemptions from civil liability for complying with the provisions of the Act, either as a content host or service provider.

## MISCONCEPTIONS ABOUT THE ACT

Perhaps the most dangerous misconception about the Act is that it is a "toothless tiger" in that, though it may be in place, it won't be enforced. This reaction has been fuelled in part by the perceived harshness of the Act in the internet industry - if it is so bad, the thinking goes, it mustn't be intended to be enforced. Under the Act, the ABA has a limited discretion to fail to investigate complaints (primarily if they are vexatious). Similarly, if the ABA believes that prohibited content is available there are very limited circumstances in which it is not required to issue a relevant notice. In the majority of cases the ABA must issue the notice. In effect, the legislation practically mandates the enforcement of its own provisions.

The second misconception is that completely "turning off" a hosted site once a notice is received in relation to content hosted on that site will be a remedy available to a content host. The exemption from civil liability provided by the Act is effectively limited to what is required by the Act. If the Act only requires taking down specified content (for example), then the content host could be sued for anything done which goes further than what is required by the Act. A similar argument can be made in respect of access to overseas sites. An end user may have a claim for breach of contract in the event that a service provider restricts access in a manner not required by the Act.

Another misconception is that private networks are not subject to the application of the Act. In the course of campaigning in favour of the legislation the Government was confronted by arguments about the applicability of this legislation to "private" information contained on

computers. In response it indicated that information contained in private networks was unlikely to be the subject of a complaint because access to the information is restricted and, if a complaint was made, the ABA was unlikely to be able to successfully investigate the complaint. While both of these things are true, the legislation itself does not draw any distinction between different types of host. The legislation can be read equally as applying to private information as it does to public information.

### **PROBLEMS WITH THE ACT**

A number of arguments as to the technical feasibility of the measures prescribed by the Act have been made by commentators. However, the fundamental problem with the Act is that it is wrong in principle. The Act makes the wrong people liable for content - it is carrier liability legislation. Carrier liability introduces significant compliance costs at the wrong point in the distribution chain, leading to significant market distortions. If the Act applied to end users and content producers it may still offend principles of free speech, but at least it would make the right people shoulder the liability.

Putting this into a real world context better shows the problems - an analogy might be that the Post Office should be liable for restricting access to inappropriate content sent through the post. First, the Post Office would have a strong incentive to inspect all articles passing through the post. To do so it would need to acquire and maintain expertise irrelevant to its core function (the delivery of mail), incur compliance costs in effecting the content review, replicate the content review function (it should already have been undertaken by the sender of the content), and would detrimentally impact on its ability to perform that function efficiently. Needless to say, costs would rise and performance would drop. Businesses which used the Post Office would in turn become less efficient.

What this analogy does not bring out is the underlying economy of the

internet. Fundamental to that economy is a system of payments for data received. Under that system service providers wishing to access content not housed on their network must pay another service provider for access to that content. Those payments are set by reference to the haulage cost involved to present the data at the network boundary between the two service providers. "Close" content - content within Australia - costs less to deliver than "distant" content - that is, content overseas. The Act's purpose is to force a portion of Australian content offshore, increasing the costs to acquire that content. Further, from an end user's perspective the source of content is largely, if not entirely, irrelevant. The information superhighway completely transcends national borders. So, forcing content offshore does not limit access to the content. All it does is increase the cost of access and make it payable to a foreign carrier.

This has three consequences. The first consequence is that everyone must pay more for access to any content. If a significant proportion of data in Australia is moved overseas, Australians must pay to import that data in the first place. Further, where before that data could be stored in Australia to satisfy later requests (that is, it could be cached or mirrored), now the data must be imported each time a content seeker requests it, multiplying the cost of providing the data. Billing mechanisms in the internet are relatively immature. Current technology is unable to premium bill content subsets - all content is charged at a flat rate. As such, there is no way to assign the increase in cost to those end users which are forcing the cost increase with the result that all end users must pay for use by the few.

The second consequence is that by forcing content offshore, the position of the current market incumbent, Telstra, is strengthened. Telstra currently offers a bundled rate for data provided over the internet. That is, using Telstra's network it costs the same to acquire 1 MB of data from a

computer in the next building as it does from a building on the other side of the world. Other operators, including Cable & Wireless Optus, have for some time offered an unbundled internet access rate in which Australian domestically sourced content is charged at a lesser rate than foreign sourced content. This arrangement encourages the development and housing of content within Australia and promotes competition and efficiency in the Australian internet market. However, if a significant proportion of Australian content is suddenly transformed into foreign content, the ability to differentiate unbundled products is greatly reduced. If the availability of unbundled rates declines, so does the competitive advantages of local content providers - as they are unable to take advantage of lower cost distribution.

The third consequence is to do with provisioning of international capacity and lead times. Again, this works to the benefit of the market incumbent. Unless a carrier owns physical infrastructure - that is, undersea cabling - to foreign countries, in particular the United States, it must purchase the international capacity from a carrier that does. While such purchases are commonplace, they usually involve the need for specific capacity forecasting anything up to 12 months in advance, and capacity usage commitments for a similar period. This means that the transition period during which the Act will be put into effect will place capacity lead time risk on a number of internet providers. They will need to make advance provisioning for the expected increase in traffic flows. If they overestimate this provisioning, they will be paying for unutilised capacity, if they underestimate, their end users will experience lag during peak periods.

Ironically, the processes set out in the Act all contain a common single point of failure - the conduct of an investigation by the ABA. Those service providers which are on a network isolated from the ABA are unlikely, as a practical matter, to be

investigated by the ABA and, consequently, are unlikely to be the subject of any of the notices contemplated by the Act. At the very least we are likely to see the development of a "content underground" of network islands which permit access to known friends and deny that access to outsiders - in a sense, an internet ghetto-isation. While these "ghettos" probably already exist, if they increase they will provide a haven for serious criminal elements - for example pushers of truly abhorrent material, rather than "mere pornography".

As a final point, it is also not at all clear what relationship internet content bears to broadcasting services, or the *Broadcasting Services Act 1992* to which it has been added as an amendment. The divergence of characteristics between broadcast media and the internet are manifold and significant:

### **BROADCAST MEDIA CONTENT/INTERNET CONTENT**

- content selected and provided by content provider vs content selected and acquired by content seeker
- content "pushed out" vs content "pulled in"
- "minimum to play" includes significant infrastructure - only the big end of town can compete vs "minimum to play" is negligible, size of player of low relevance
- physical limitations on the location of infrastructure vs no limitations on the location of infrastructure
- physical limitations on the mobility of infrastructure vs no limitations on the mobility of infrastructure
- competition confined to specific geography and therefore quantifiable competitors vs no geographical barriers to competition
- significant barriers to entry in the provision of content (eg video production etc) vs minimal or no barriers to entry in the provision of content (users are forgiving of "unprofessional" content)
- communications costs are borne by content provider (establishing and maintaining a transmitter) vs communications costs are borne by content seeker (interconnection charges).

It is almost as if broadcasting and internet are antonymous. Given the extreme divergence of characteristics, one might argue that the more experience a body has with broadcast regulation, the less qualified it is to deal with the internet. Further, the justification for regulation of broadcasting is that an exclusive licence over public property (the broadcast spectrum) is being given to a broadcaster for the purpose of conducting a business. There is no comparable analogy in the internet space. There is no readily identifiable public property that is being appropriated to someone's exclusive use.

In summary:

1. the Act is fundamentally wrong in principle. Shooting the messenger is not the solution;
2. compliance with the scheme will be both uncertain and involve significant compliance costs which will be passed on to all internet users
3. the Act will introduce significant distortions into the market. These distortions are likely to favour the market incumbent;
4. failure to comply with the scheme is attended by disproportionate penalties;
5. all internet businesses within Australia and all businesses relying on them will be adversely impacted. Internet related businesses within

Australia will be placed at a competitive disadvantage as against our regional neighbours;

6. some of the provisions of the Act indicate a disturbing lack of understanding of the medium being regulated; and
7. anecdotal evidence suggests that the access to prohibited content in Australia will be only marginally impacted if at all.

Addendum: On 30 September 1999, the Australian Senate (the Upper House of the Australian Parliament) passed the following motion:

That the Senate—

- (a) notes the range of recent criticism and developments surrounding the Government's *Broadcasting Services Amendment (Online Services) Act 1999* (the Act);
- (b) recognises that:
  - i) the Act will not achieve the Government's stated objectives,
  - ii) the Act will impact adversely on the emergent Australian e-commerce and Internet industries, which are strong employers of young Australians,
  - iii) the Act will discourage investment in information technology projects in Australia and will force Australian business offshore, and
  - iv) the most appropriate arrangement for the regulation of Internet content is the education of users, including parents and teachers, about appropriate use of the Internet, the empowerment of end-users, and the application of appropriate end-user filtering devices where required; and

- (c) calls on the Government:
- i) to immediately address the concerns raised by industry and the community about the unworkability of the Government's approach, and the Act in general,
  - ii) to urgently revisit aspects of the Act, prior to its commencement on 1 January 2000, and
  - iii) to table a report on the effectiveness and consequences of the Act in
- the Senate at 6-month intervals from the date of implementation of the regulatory regime.
- The text of the Act is available from <http://scaleplus.law.gov.au/html/comact/10/6005/rtf/No90of1999.rtf>.
- 

## And Now to Regulate Internet Gaming —A Gamble in Itself

*John Lambrick, RMIT University, Melbourne*

---

### INTRODUCTION

Enthusiasm for online gaming appears to be gaining significant momentum in Australia, and it is estimated that last year 86,000 Australians used the Internet to bet on sports and casino games<sup>1</sup>. This is hardly surprising given that gambling, and now Internet use, are firmly engrained in Australian popular culture. It also comes as no surprise that Australian legislatures have rushed headlong into regulating Internet gaming activity.

With the exception of New South Wales and Western Australia, the remaining Australian states have passed or have indicated an intention to pass legislation to regulate online gaming. The Northern Territory has also enacted such legislation. For the purposes of this article, I propose to make comparisons between the Queensland Interactive Gambling (Player Protection) Act 1998 and the Victorian Interactive Gaming (Player Protection) Act 1999.

### WILL THE LEGISLATION SUCCEED?

Whether or not the legislation will succeed depends upon the purpose of the legislation. If the purpose of the legislation is to regulate Internet gaming activity in Australia, then it will be a dismal failure. Unfortunately, many politicians and

lawyers have still not come to grips with the fact that it is impossible to effectively regulate Internet activity through legislation. If, on the other hand, the purpose of the legislation is to facilitate Internet gaming and to give players a greater opportunity to gamble online with a solvent body and with a reasonable likelihood that any winnings will be paid, then I suggest that the legislation has some prospects of success.

### THE JURISDICTION ISSUE

Legislation which attempts to regulate Internet activity must recognise the jurisdictional limitations involved in doing so. The legal issues relating to jurisdiction and the Internet have been extensively and well argued elsewhere<sup>2</sup>, and it is the writer's opinion that for a government to effectively regulate any activity, the following are necessary criteria:

- The government must have jurisdiction to regulate the activity. Jurisdiction is geographically determined, and ultimately the jurisdiction of a government depends upon its recognition by other governments. Therefore, attempts to assert jurisdiction need to be credible. A government will only have jurisdiction over persons and things which have some nexus

or relationship with the relevant state or country administered by that government. Thus, for example, the Victorian state government would not be recognised by other governments as having jurisdiction to legislate with respect to kiwi breeding in New Zealand.

- The government must also be in a position to exercise power over or control breaches of the activity which the government seeks to regulate. Law-making requires some mechanism for law-enforcement which in turn depends on the ability to exercise physical control over law violators<sup>3</sup>.

Attempts to create effective regulation of the Internet fail on both counts. The Internet is so geography-averse that in any instance it may be impossible to determine an Internet user's physical location or the location in which Internet activity occurred. For example, I may register an address in the "com.au" domain, but I do not need to have my operations based in Australia to enable me to do so. Furthermore, there is nothing to stop me transferring my host computer and my Internet address (or either of them) to any other location in the world. Persons dealing with me would have no idea that such transfers had taken place.