

CHAPTER 7

INTERNET REGULATION

Julian Ding
First Principles Sdn Bhd
Kuala Lumpur, Malaysia

7.01 Introduction

(a) In General

This chapter discusses what the Internet and the World Wide Web are and the forms of regulation that are applied to them.

Obviously, the scope of Internet regulatory frameworks has many connections with topics such as gambling, crime, and pornography. It is too enormous a task to examine all of these subjects in this chapter.

The remaining parts of this chapter examine the regulatory frameworks applicable to:

1. Internet Protocol Address assignments;
2. Internet access;
3. Online content; and
4. Spam.

(b) What Is the Internet?

(i) In General

The Internet, in its simplest form, comprises the connection of many different computers located in many different places in the world. The connection is through the use of physical cables (i.e., wires) and, traditionally, this has been provided through the use of telecommunication cables. Now, wireless connectivity is rising and may become a substitute for wire for Internet connection.

In a sense, the Internet is the name given to the global information network which grew through cooperation among individuals rather than one which was developed by any single person or entity or country. It spans the world and connects anyone who has a computer, or access device, with a modem and an Internet access account.

Historically, the Internet grew up in the United States as part of the department of defense project (ARPA). A key element of the Internet was the development of the Transmission Control Protocol/Internet Protocol (TCP/IP) standard for communication. This breakthrough enabled the efficient use of networks to send and receive large quantities of data almost instantaneously.

Furthermore, ICANN's Strategic Priorities¹ succinctly identify three things about the Internet which makes it important, namely:

1. The Internet has been engineered with an open architecture, designed to allow new protocols and services to be readily integrated.
2. It is an aggregate of data networks that can operate over and support varied data technologies and applications.
3. [This is done by] maintaining a set of core protocols that are kept very stable. This core includes the Internet Protocol (IP), the routing system, and the domain name system.

These three elements — open architecture, capability to support varied data technologies/applications, and stable core protocol — make the Internet what it is today.

The next major breakthrough (where ordinary individuals were able to access the Internet and its content) is the development of the browser, which enabled simple “point and click” operations for anyone. This coincided with the simplification of the computers through the use of graphical user interfaces, i.e., technology started to become domesticated.

(ii) Differences between the Internet and the World Wide Web

While the terms “Internet” and the “World Wide Web” (or “Web”) are sometimes used interchangeably, there are, in fact, differences between the two. These differences are:

1. The Internet is a “massive network of networks, a networking infrastructure. It connects millions of computers together globally, forming a network in which any computer can communicate with any other computer”;²

1 Available at <http://www.icann.org/strategic-plan/strategic-plan-sec2-16nov04.pdf>, accessed on 5 February 2005.

2 Webopedia, at http://www.webopedia.com/DidYouKnow/Internet/2002/Web_vs_Internet.asp, accessed on 1 February 2005.

2. The information traveling across the Internet uses a variety of protocols, such as file transfer protocol (FTP), email (SMTP), and instant messaging;
3. Different protocols are used that enable connections to occur;
4. The Web “is a way of accessing information over the medium of the Internet. It is an information-sharing model that is built on top of the Internet. The Web uses the HTTP protocol, [which is] only one of the languages spoken over the Internet, to transmit data. Web services, which use HTTP to allow applications to communicate to exchange business logic, use the Web to share information”;³ and
5. The Web uses browsers (such as Mozilla and Internet Explorer) to access Web pages (documents built using html programming language).

Therefore, the Web is one of the ways by which information is accessed, and it is not the Internet. The Internet enables other activities, such as sending and receiving emails or accessing information contained in newsgroups or remote diagnosis of computers.

This distinction enables a proper appreciation of what should be regulated, and provides a context when one considers what Internet regulation is all about. In addition, by specifically identifying the differences between the Internet and the World Wide Web, it is hoped that the reader will appreciate that regulating the Internet and the World Wide Web are two different activities.

(iii) Meaning of Regulation

Regulation, as it is commonly understood, refers to the imposition of standards and legally enforceable controls. Licensing regulation is one example of the imposition of a legally enforceable control.

The effectiveness of a regulation requires that there is a body (which all participants either explicitly or tacitly recognize) that is able to enforce the rules. This body is usually the nation-state, and the exercise of the authority is over those entities which are within its jurisdiction. This, however, is merely a description of regulation. There is no clear definition of regulation. One definition is:

Regulation is the process by which government induces, requires or prohibits certain actions by individuals, private institutions and sometimes public institutions, often through the efforts of specially designated regulatory agencies.⁴

3 Webopedia, at http://www.webopedia.com/DidYouKnow/Internet/2002/Web_vs_Internet.asp, accessed on 1 February 2005.

4 Gow, “Business and Government as Regulation”, in Colebatch, Prasser, and Nethercote (eds.), *Business-Government Relations: Concepts and Issues* (1997).

Another definition is:

. . . the imposition of constraints (backed by government authority) which are intended to influence the behavior of individuals or industry.⁵

Alternative forms of regulation exist, for example, as between members *inter se* of a club or association. A breach of the rules does not result in any legal enforcement by the state. Instead, their enforcement is brought about by the club's internal disciplinary process, which may result in the expulsion of the member from the club or association. The "public shame" of being expelled from the club provides sufficient incentive for individuals to comply with the rules. This is considered as a form of self-regulation.

By identifying the characteristics of regulation, a better means by which the concept of Internet Regulation can be provided or addressed. Consequently, regulation (whether as commonly understood or in the form of self-regulation) possesses these characteristics:

1. It seeks to ensure a particular behavior is developed, adhered to, or maintained;
2. There is some penalty for non-observance;
3. It applies to all participants;⁶ and
4. There is some form of enforcement to ensure compliance.

(iv) Reasons for Regulating

In General There are four theoretical perspectives why Governments regulate an activity, namely:

1. Market failure;
2. Public interest;
3. Life cycle; and
4. Private interest.⁷

Market Failure Market failure occurs when the market is unable to deal with structural problems, such as lack of competition (or monopolies), negative

5 Savage Report on the Review of Queensland Business Regulation, 1986.

6 A participant is an entity (whether as an individual person or a legal person, i.e., corporations) who is involved in the sector which is subjected to the regulation. This may be, for example, the travel agency business, which is subjected to licensing requirements (to start the business), consumer protection laws (to protect consumers), and anticompetitive or unfair trade practice laws.

7 Gow, "Business and Government as Regulation", in Colebatch, Prasser, and Nethercote (eds.), *Business-Government Relations: Concepts and Issues* (1997).

externalities (e.g., smoke-stack emissions affect quality of life of nearby residents), asymmetric information (where a consumer has insufficient information to determine whether to buy a product or not), and the provision of a public good (e.g., street lighting), thus necessitating governmental intervention through regulation.

Public Interest Public interest emphasizes the collective good rather than individual good, which may be superior and necessary. Examples of public interest are the establishment of standard weight and measures, economic management, or collective amenity.

Life Cycle The life cycle theory of regulation argues “that, while the initial regulation may have been intended to serve a particular public interest, regulation in time comes to serve a private interest”.

Private Interest The private interest theory argues that regulation is sought by private firms to accumulate the resource of the State to prevent others from entering their market space.

Other Reasons for Regulation Other commentators⁸ identify 12 reasons for regulation as set out in Table 1, below.

Table 1 — Reasons for Regulation

Rationale	Main Aims of Regulation	Example
Monopolies and natural monopolies	Counter tendency to raise prices and lower output Harness benefits of scale economies Identify areas genuinely monopolistic	Utilities
Windfall profits	Transfer benefits of windfalls from firms to consumers or taxpayers	Firm discovers unusually cheap source of supply
Externalities	Compel producer or consumer to bear full costs of production rather than pass on to third parties or society	Pollution of river by factory
Information inadequacies	Inform consumers to allow market to operate	Pharmaceuticals, food and drinks labeling

8 Baldwin and Cave, *Understanding Regulation: Theory, Strategy, and Practice* (1999), at pp. 9–17.

Continuity and availability of service	Ensure socially desired (or protect minimal) level of “essential” service	Transport service to remote region
Anticompetitive and behavior predatory pricing	Prevent anticompetitive behavior	Below-cost pricing in transport
Public goods and moral hazard	Share costs where benefits of activity are shared but free-rider problems exist	Defense and security services. Health services
Unequal bargaining power	Protect vulnerable interests where market fails to do so	Health and safety at work
Scarcity and rationing	Public interest allocation of scarce commodities	Petrol shortages
Distribution justice and social policy	Distribute according to public interest Prevent undesirable behavior or results	Victim protection
Rationalization and coordination	Secure efficient production where transaction costs prevent market from obtaining network gains or efficiencies of scale Standardization	Disparate production in agriculture and fisheries
Planning	Protect interests of future generations Coordinate altruistic intentions	Environment

Table: *Regions for Regulating* [source: Baldwin and Cave (1999)]

(v) *Why Regulate the Internet?*

Telecommunications is regarded as an essential service in most countries in the world. Until the 1980s, this service was provided by the government (or the public sector) rather than the private sector (with the exception of the United States). The 1980s saw the rise of privatization, led by the United Kingdom, which pursued privatization as a means of introducing economic efficiencies into an otherwise inefficient enterprise.

Once privatization occurred, governments soon realized that it was necessary to introduce regulation to ensure that the former state-owned enterprise did not behave improperly and to ensure that new entrants were allowed to participate. This created the licensing structure by which governments could enable a competitive market to emerge.

For access to the Internet to occur, it is necessary that a user subscribe to an entity which provides Internet access, known as an Internet Service Provider or Internet Access Provider (ISP or IAP, respectively). Assuming that users have

telephone connections to their home or office, the ISP or IAP will usually be an entity licensed or permitted by the government of the country in which the users reside to offer Internet access, email, or newsgroups as a service to them.

It is highly unlikely that a user will subscribe to an ISP or IAP located in another country because of the prohibitive cost of making an international call over a long period of time, just to get access to the Internet, although it is possible.

The technology that has enabled the Internet is fundamentally a “disruptive technology” (i.e., it changes the way things were done in a dramatic form). Examples of disruptive technology are the printing press and television.

Previously, one needed different devices to watch television (television set), communicate verbally (telephone), or process data (computer). Today, all of these activities can be performed by a single device, the personal computer connected to the Internet.

Government concerns relating to the Internet are based on issues dealing with:

1. National security;
2. Protection of minors;
3. Protection of human dignity;
4. Economic security;
5. Protection of information;
6. Protection of privacy;
7. Protection of reputation; and
8. Protection of intellectual property.⁹

Furthermore, it has been pointed out that today cyberspace (i.e., the Internet and the Web) is, in fact, subject to various forms of regulation.¹⁰ There are:

. . . four things that regulate cyberspace [namely]: laws (by government sanction and force), social norms (by expectation, encouragement, or embarrassment), markets (by price and availability), and architecture (what the technology permits, favors, dissuades, or prohibits).¹¹

9 Peng, “How Countries Are Regulating Internet Content”, at http://cad.ntu-kpi.kiev.ua/events/inet97/B1/B1_3.htm, accessed on 5 February 2005.

10 Lessig, “The Laws of Cyberspace”, cited in Reagle, “Why the Internet is Good”, at <http://cyber.law.harvard.edu/people/reagle/regulation-19990326.html> accessed on 30 November 2004.

11 Lessig, “The Laws of Cyberspace”, cited in Reagle, “Why the Internet is Good”, at <http://cyber.law.harvard.edu/people/reagle/regulation-19990326.html>, accessed on 30 November 2004.

Examples are:

1. Architectural structure of Internet Protocol Addresses — No one would consider using an Internet Address (i.e., an Internet Protocol Address used on the Internet as opposed to a private network) outside the standard structure, (i.e., the numeric range of 0 to 255), because of the possible impact to the stability of the core protocol. Consequently, it is necessary for there to be a proper, fair, and efficient management and administration system for allocating Internet Protocol Addresses. This is undertaken through various non-governmental bodies.
2. Market regulation — This is where rules that are set in a market environment apply to participants in that market. Examples of such market regulation are the online market places, business-to-business supply markets, and online auctions.
3. Social norms — This is perhaps the most widespread. It exists in all online communities, newsgroups, or other forms of membership-based organizations. Each group or community is subjected to certain norms or standards of behavior to which all adhere. The standards are made known at the outset, and individuals who continue to subscribe are deemed to have acceded to them. Breach of the norms does not result in penal sanctions but, in most cases, continued membership is prevented.
4. Laws — Legislation, by its very nature, requires the use of the state's coercive power to bring about a particular behavior. It is usual that laws are applied to such areas as the licensing of Internet access or the control of online content. The difficulty is with the enforcement of the laws, especially if the individual concern is beyond the geographical jurisdiction of the state.

(vi) *Scope of Internet Regulation*

The scope of Internet regulation falls within four categories, namely:

1. “Scarce resource” and public goods, i.e., bandwidth allocation and the quality of communal spaces;
2. Efficiency, i.e., anti-fraud regulation;
3. Interoperability, i.e., open standards, open source, and protocol and name registration; and
4. Behavior, i.e., prohibition of obscene speech.¹²

This categorization is a useful starting point, but it is by no means exhaustive or comprehensive. Governments are at various stages of evolution and are of

12 Reagle, “Why the Internet is Good”, at <http://cyber.law.harvard.edu/people/reagle/regulation-19990326.html>, accessed on 30 November 2004.

different types. Some are democratically elected, while others are totalitarian regimes; yet, others are absolute monarchies. The Internet now enables knowledge to be shared by many individuals at a fraction of the costs. The concern of governments is that such access to knowledge may affect their political power and position. This concern is what drives these governments to sometimes ban or prevent access to the Internet totally. This is not regulation but outlawing, and is not considered in this chapter.

(c) Issues Affecting Regulation of the Internet

(i) *In General*

The rules and laws that govern human behavior have traditionally been limited by the geographical boundaries of the state. With the Internet, these geographical boundaries, to a great extent, have disappeared. Accordingly, there is uncertainty as to how to regulate the Internet.

It is necessary to distinguish between rules affecting the Internet and rules affecting the activity which uses the Internet. An example of the former would be the control of Internet access by a country, whereas an example of the latter would be the sale of books online by a commercial outlet. The sale of books is subject to existing laws on operating a business, content censorship or control, and taxation which are applicable to the vendor based on the geographical nexus of the vendor to the state.

These laws apply regardless of the fact that the activity occurs in cyberspace. The issue surrounding the activity and which is a problem for governments is one of enforcement. It is difficult to enforce the rules prohibiting sale of certain types of content if the vendors are physically outside the country seeking such enforcement.

In the first instance, in 2000, La Ligue successfully sued Yahoo! Inc. in France and obtained an order that imposed a daily fine of US \$13,000 if Yahoo! did not block access to the Nazi content on its portal. Subsequently, La Ligue sought to enforce the French court's order in the United States and, there, the court of first instance ruled that Yahoo! was not subject to the French court order in the United States. This decision was appealed and the United States 9th Circuit Court decided that Yahoo! was so subject. Thereafter, Yahoo! filed a suit to seek a rehearing of the United States 9th Circuit Court's decision.¹³ The United States Court of Appeals decided in 2005 that the original United States court order against Yahoo! in 2004 must be subjected to a rehearing because the issue of free speech and the right of a foreign state to impose a financial penalty were at play.

13 *Yahoo! Inc. v. La Ligue Contre le Racisme et L'antisemitisme and Another*, United States Court of Appeals for the 9th Circuit [Appeal Number 1-17424].

The *Yahoo!* case typifies the complexity of the issues affecting the Internet and content available thereat. Material which is considered acceptable in one country, but is available using the Internet or the Web, becomes unacceptable in another country. In such a situation, how should such material be treated? Is it illegal in the recipient country and, if so, can the “provider” be subjected to legal fines enforceable against it in its home country. The outcome of the rehearing would be of significant interest as it may provide some guidance on how the United States would treat the provision of content which is inappropriate by other countries laws by its companies.

What these evidence is the importance of the concept of national sovereignty. With national sovereignty, a nation-state is able to pass laws within its territory and deal with its citizens and businesses. Consequently, the recognition of national sovereignty by other nation-states has led to the conventions and norms for the dealings between them. Effectively, such dealings are undertaken on the basis of peers, as opposed to primary and secondary relationships.

From this concept, the evolution and creation of international institutions has been enabled. One must look at the preamble to the United Nations Charter,¹⁴ which brought the United Nations into existence and which states:

We the Peoples of the United Nations Determined:

to save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind, and

to reaffirm faith in fundamental human rights, in the dignity and worth of the human person, in the equal rights of men and women and of nations large and small, and

to establish conditions under which justice and respect for the obligations arising from treaties and other sources of international law can be maintained, and

to promote social progress and better standards of life in larger freedom,

And for These Ends:

to practice tolerance and live together in peace with one another as good neighbors, and

to unite our strength to maintain international peace and security, and

to ensure, by the acceptance of principles and the institution of methods that armed force shall not be used, save in the common interest, and

to employ international machinery for the promotion of the economic and social advancement of all peoples,

14 United Nations Charter, at <http://www.un.org/aboutun/charter/index.html>, accessed on 12 February 2005.

Have Resolved to Combine Our Efforts to Accomplish These Aims:

Accordingly, our respective Governments, through representatives assembled in the city of San Francisco, who have exhibited their full powers found to be in good and due form, have agreed to the present Charter of the United Nations and do hereby establish an international organization to be known as the United Nations.

The preamble clearly identifies that it is the people, through their respective governments, that have agreed to establish the United Nations. The choice of the words is material because it establishes that:

1. The governments represent their people;
2. Each government is sovereign; and
3. Each government is equal.

Without such recognition of national sovereignty and the peer-status of each government and country, the basis for setting up the United Nations would not exist. Furthermore, the arena of public international law, the prohibition of the enforcement of penal and revenue statutes or laws of one country in another country, and the need for the existence of extradition treaties before extradition proceedings in one country can be commenced all reinforce the principle of national sovereignty.

This legal legacy by which the world functions today finds difficulty in providing solutions to the borderless world of the Web. In such a situation, how does one exercise control of or regulate the Web?

There are, in fact some, simple solutions. Contractual arrangements made via the Web are no different than contractual arrangements made via telex or facsimile. Laws have evolved to recognize such contractual arrangements¹⁵ and, accordingly, such evolution will occur to recognize contracts made via the Web simply because it is necessary to recognize such transactions which business people undertake.

The contrary would be unthinkable as it would cause immense commercial difficulty. Lord Wilberforce, in *Brinkibon v. Stahag Stahl und Stahlwarenhandelsgesellschaft mbH* (1983),¹⁶ said that the approach to be taken to resolve these issues is by reference to the intention of the parties, by sound business practices and in some cases by a judgment where the risk should lie, indicating that courts do take a pragmatic approach to resolving some of these issues.

15 *Entores Ltd. v. Miles Far East Corporation* [1955] 2 Q.B. 327; [1955]2 All E.R. 493; *Brinkibon v. Stahag Stahl und Stahlwarenhandelsgesellschaft mbH* [1983] 2 A.C. 34; [1982] 1 All E.R. 293.

16 *Brinkibon v. Stahag Stahl und Stahlwarenhandelsgesellschaft mbH* [1982] 1 All E.R. 293 (per Lord Wilberforce, at p. 296d-e).

While national sovereignty has been the basis for the evolution of the political and legal institutions today, it is necessary for governments to determine what exactly they want to regulate when it comes to the Internet and the Web. The lack of identification of where the problems are or the areas that need regulation has resulted in the perception that the Internet is beyond regulation.

7.02 Applicable Regulatory Frameworks

(a) In General

It is appropriate now to explore the structure of regulatory frameworks used by various countries affecting four areas, namely:

1. Regulating Internet Protocol Addresses;
2. Regulating Internet access;
3. Regulating online content; and
4. Regulating spam.¹⁷

(b) Regulating Internet Protocol Addresses

(i) In General

In order for the Internet to function, there are certain pre-requisites as summarized below:

1. There is a need for every device that is connected to the Internet to have a unique and particular number, i.e., the Internet Protocol Address;
2. There must be a mechanism by which software can resolve these Internet Protocol Addresses, a process which is now undertaken by root servers located in three major areas in the world; and
3. There must be a system by which human recognizable names are managed (referred to as domain names) to which the Internet Protocol Address resolution must occur.

The Domain Name System relies on each domain name being assigned a unique identifier or number. *Webopedia* defines Internet Protocol Addressing as follows:

An identifier for a computer or device on a TCP/Internet Protocol network. Networks using the TCP/Internet Protocol route messages based on the Internet Protocol Address of the destination. The format of an Internet Protocol Address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For

¹⁷ Other areas, such as privacy, the issue of domain names and trade marks (and cybersquatting), e-contracting, and digital signatures are dealt with elsewhere in this publication.

example, 1.160.10.240 could be an Internet Protocol Address. Within an isolated network, you can assign Internet Protocol Addresses at random as long as each one is unique. However, connecting a private network to the Internet requires using registered Internet Protocol Addresses (called Internet Addresses) to avoid duplicates. The four numbers in an Internet Protocol Address are used in different ways to identify a particular network and a host on that network. Four regional Internet registries — ARIN, RIPE NCC, LACNIC, and APNIC — assign Internet Addresses from the following three classes:

Class A — supports 16-million hosts on each of 126 networks

Class B — supports 65,000 hosts on each of 16,000 networks

Class C — supports 254 hosts on each of 2-million networks

The number of unassigned Internet Addresses is running out, so a new classless scheme called CIDR is gradually replacing the system based on classes A, B, and C and is tied to adoption of IPv6.¹⁸

(ii) *Who Assigns Internet Protocol Numbers?*

Internet Protocol Numbers are required to be unique and are today assigned by non-governmental groups. These include IANA,¹⁹ which has overall responsibility for assigning Internet Protocol Addresses to Regional Internet Registries (RIRs); each RIR, in turn, allocates Internet Protocol Addresses to local Internet registries or large end-users within their respective geographical jurisdictions. There are currently four RIRs, namely:

1. APNIC is a company incorporated under the laws of Australia,²⁰ and its official corporate name is APNIC Pty. Ltd. Its function according to APNIC's brochure is to ensure the fair distribution and responsible management of Internet Protocol Addresses and the related numeric resources which are required for stable and reliable operation of the Internet globally,²¹ but not the domain name system. The countries that fall within APNIC's jurisdiction are Afghanistan, American Samoa, Australia, Bangladesh, Bhutan, British Indian Ocean Territory, Brunei Darussalam, Cambodia, China, Christmas Island, Cocos Keeling Islands, Comoros, Cook Islands, East Timor, Fiji, French Polynesia, French

18 *Webopedia*, at http://www.webopedia.com/TERM/I/Internet_Protocol_address.html, accessed on 4 August 2004.

19 IANA stands for Internet Assigned Numbers Authority, at <http://www.iana.org>.

20 The memorandum of association of APNIC Pty. Ltd. is at <http://www.apnic.org/docs/corpdocs/MoAhtm>, and the articles of association of APNIC Pty. Ltd. are at <http://www.apnic.org/docs/corpdocs/AoAhtm>, accessed on 30 November 2004.

21 APNIC, at <http://www.apnic.org/info/brochure/apnicbroc.pdf>, accessed on 28 December 2004.

Southern Territories, Guam, Hong Kong, India, Indonesia, Japan, Kiribati, North Korea, South Korea, Laos, Macau, Madagascar, Malaysia, Maldives, Marshall Islands, Mauritius, Mayotte, Micronesia, Mongolia, Myanmar, Nauru, Nepal, New Caledonia, New Zealand, Niue, Norfolk Island, Northern Mariana Islands, Pakistan, Palau, Papua New Guinea, Philippines, Pitcairn, Reunion, Samoa, Seychelles, Singapore, Solomon Islands, Sri Lanka, Taiwan, Thailand, Tokelau, Tonga, Tuvalu, Vanuatu, Vietnam, Wallis and the Fortuna Islands.

2. ARIN, or the American Registry for Internet Numbers, Ltd., is a company incorporated under the Virginia Non-Stock Corporation Act and is domiciled in the State of Virginia, United States.²² ARIN is responsible for such countries as the Bahamas, Barbados, Canada, the Cayman Islands, Mexico, South Africa, and the United States.²³
3. LACNIC, or the Latin America and Caribbean Internet Addresses Registry, is a non-governmental, not-for-profit organization established under the laws of Uruguay. Its functions are to “administer Internet Protocol Addresses space, Autonomous System Numbers (ASN), reverse resolution and other resources of the Latin American and Caribbean region (LAC)”.²⁴
4. RIPE NCC (*Resaux Internet Protocol Europens Network Coordination Centre*)²⁵ is a non-profit association registered in Amsterdam, The Netherlands.²⁶ The RIPE NCC is responsible for countries in Europe, the Middle East, Central Asia, and Africa located north of the equator. RIPE NCC performs many functions and services, including managing, distributing, and registering public Internet Number Resources (i.e., Internet Protocol Addresses) within its region.

At the time of writing, a proposed new RIR for Africa, called AfriNIC,²⁷ received provisional recognition from ICANN²⁸ and is on the way to becoming

22 A copy of the articles of incorporation of ARIN is at http://www.arin.net/library/corp_docs/artic_incorp.pdf, accessed on 30 November 2004.

23 A complete list of countries within ARIN's jurisdiction is at http://www.arin.net/library/Internet_info/ARINcountries.htm.

24 Information about LACNIC is at <http://lacnic.net/en/sobre-lacnic/estatuto/> and at <http://lacnic.net/en/sobre-lacnic/>, accessed on 30 November 2004.

25 General information about RIPE NCC is at <http://www.ripe.net/>.

26 A copy of the articles of association of RIPE NCC is at <http://www.ripe.net/ripe/docs/articles-association.html>, accessed on 28 December 2004.

27 Details about AfriNIC are at <http://www.afrinic.net/>.

28 AfriNIC received provisional recognition on 11 October 2004 from ICANN. A copy of the letter is at <http://www.afrinic.net/documents/icann/Letter%20%20AfriNIC1.pdf>.

the fifth RIR. AfriNIC is a company limited by guarantee, and it is incorporated under the Mauritius Companies Act 2001. It will have jurisdiction over those “African organizations that presently obtain Internet Protocol Address space from RIPE or ARIN”.²⁹

The RIRs are not controlled by any government, but are companies incorporated or societies organized under the laws of a selected country for convenience. Each RIR operates on a membership basis, and anyone can become a member of it. This is quite different from the way the International Telecommunications Union (ITU) is organized, where countries (represented by their governments) are members and these countries then allow their privatized telecommunications providers to attend.

Another entity that has overall responsibility for the Internet and the World Wide Web is ICANN, or the Internet Corporation of Assigned Names and Numbers.

ICANN is a corporation which is organized under the State of California Nonprofit Public Benefit Corporation Law for charitable and public purposes.³⁰ This makes ICANN a United States-domiciled company. Furthermore, ICANN is to ensure that the Domain Name System (DNS) works, as ICANN is responsible for managing and coordinating the DNS to ensure that every address is unique and that all users of the Internet can find all valid addresses. It does this by overseeing the distribution of unique Internet Protocol Addresses and domain names. It also ensures that each domain name maps to the correct Internet Protocol Address.³¹

According to the ICANN web site,³² ICANN also is responsible:

... for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions. These services were originally performed under United States Government contract by the Internet Assigned Numbers Authority (IANA) and other entities. ICANN now performs the IANA function.

InterNIC is not a legal entity but a brand name owned by the United States Department of Commerce and managed by ICANN.³³

29 AfriNIC's background information at <http://www.afrinic.net/about.htm>, accessed on 30 November 2004.

30 Articles of incorporation of ICANN, article 3, at <http://www.icann.org/general/articles.htm>, accessed on 30 November 2004.

31 See <http://www.icann.org/faq/#WhatisICANN>, accessed on 4 August 2004.

32 ICANN, at <http://www.icann.org/general/>, accessed on 30 November 2004.

33 See <http://www.internic.org/index.html>.

Therefore, IANA will allocate Internet Protocol Addresses from the pools of unallocated addresses to the RIRs according to their established needs. When an RIR requires more Internet Protocol Addresses for allocation or assignment within its region, a request is made and IANA makes an additional allocation to the RIR.³⁴ It should be noted that the functions of IANA are being transferred to ICANN.

APNIC, however, recognizes national Internet registries and defines them as:

. . . [a] National Internet Registry (NIR) primarily allocates address space to its members or constituents, which are generally LIRs organized at a national level. NIRs are expected to apply their policies and procedures fairly and equitably to all members of their constituency. The policies in this document apply to NIRs; however, this document does not describe the entire roles and responsibilities of NIRs with respect to their formal relationship with APNIC. Such roles and responsibilities may be described in other documents and agreements, subject to APNIC Document review procedures.³⁵

Taiwan, China, Vietnam, Indonesia, Japan, and Korea operate National Internet Registries. They receive bulk allocation of Internet Protocol Addresses from APNIC and are able to allocate individual Internet Protocol Addresses to users within their countries. The role played by these NIRs is to provide a degree of control over the allocation of Internet Protocol Addresses within their countries, as opposed to allow a non-governmental organization to do so. For example, in Vietnam, it is VNNIC that allocates Internet Protocol Addresses to those who require it in Vietnam whereas, in Thailand, APNIC allocates Internet Protocol Addresses. The rationale for governments taking over Internet Protocol Address allocations is to exercise some form of sovereignty over their use.

Malaysia has introduced regulatory provisions making the Malaysian Communications and Multimedia Commission the entity with overall responsibility for assigning Internet Protocol Addresses in Malaysia. However, this statutory duty has yet to be enforced whereby the Malaysian Communications and Multimedia Commission becomes Malaysia's National Internet Registry.

(iii) Process to Obtain Internet Protocol Addresses

According to IANA:

[Internet Protocol] Addresses are assigned in a delegated manner. Users are assigned Internet Protocol Addresses by Internet Service Providers

34 See <http://www.iana.org/ipaddress/ip-addresses.htm>, accessed on 4 August 2004.

35 See <http://www.apnic.net/docs/policy/add-manage-policy.html#4.1.2>, accessed on 30 January 2005.

(ISPs). ISPs obtain allocations of Internet Protocol Addresses from a local Internet registry (LIR) or national Internet registry (NIR), or from their appropriate Regional Internet Registry (RIR).

According to RFC 2050, entitled “Internet Registry Internet Protocol Allocation Guidelines”,³⁶ Internet Addresses (or Internet Protocol Addresses) are distributed with intent of meeting the following goals:

Conservation: Fair distribution of globally unique Internet Address space according to the operational needs of the end-users and Internet Service Providers operating networks using this address space. Prevention of stockpiling to maximize the lifetime of the Internet Address space.

Routability: Distribution of globally unique Internet Addresses in a hierarchical manner, permitting the routing scalability of the addresses. This scalability is necessary to ensure proper operation of Internet routing, although it must be stressed that routability is in no way guaranteed with the allocation or assignment of Internet Protocol Addresses.

Registration: Provision of a public registry documenting address space allocation and assignment. This is necessary to ensure uniqueness and to provide information for Internet trouble shooting at all levels.

The guidelines do caution as to the possible conflict between conservation and routability and suggest that, in the final analysis, it is sound judgment which is to be relied on. To achieve these goals, an Internet registry with a hierarchical structure is created, whereby IANA has authority over all number spaces used on the Internet. IANA, in turn, allocates Internet Addresses to Regional Internet Registries, and RIRs, in turn, assign Internet Addresses to local Internet registries, ISPs, or large users (as defined in RFC 2050 *ante*).

Allocation of Internet Addresses entitles the “allocatee” to assign the Internet Numbers to users below it (remembering that the Internet registry structure is hierarchical). Assignments of Internet Addresses do not entitle the assignees to sub-allocate the Internet Addresses to other entities, and they may only use the Addresses for themselves.

An allocation of Internet Addresses is for a term of one year, renewable annually, if (a) “the original basis of the allocation or assignment remains valid”; and (b) “. . . address space is properly registered at the time of renewal”.³⁷ However, compared to RIPE NCC, no such term is provided.³⁸

36 The guideline was issued in November 1996, and is at <http://www.isi.edu/in-notes/rfc2050.txt>, accessed on 12 February 2005.

37 APNIC Policies for Internet Protocolv4 Address Space Management in the Asia Pacific Region, 16 August 2004, at <http://www.apnic.net/docs/policy/add-manage-policy.html#8.3>.

38 RIPE NCC Policy on Internet Protocolv4 Address Allocation and Assignment Policies for the RIPE NCC Service Region, Document RIPE-324, October 2004, at <http://www.ripe.net/ripe/docs/ipv4-policies.html#ipv4>.

The differences identified above indicate that the processes for allocating Internet Addresses by RIRs are not uniform.

(iv) Regulatory Issues

By ensuring a proper and orderly assignment of Internet Protocol Addresses, the uniqueness of the Internet Protocol Address system is preserved. This enables both origination and destination of messages to be known in cyberspace. Therefore, the management of Internet Protocol Addresses is an essential requirement to avoid clashes and confusion, and to create the stability needed for the Internet and the Web to function.

First, while recognizing the importance of Internet Protocol Addressing, the issue which governments are concerned about is why should this be undertaken by the private sector (meaning non-government entities).

Telecommunication regulation has been identified as:

... one of the earliest examples of international regulatory cooperation between states ... [b]ut in other respects ... [regulation] is a story of territorial containment.³⁹

This “cooperation between states” has not been pursued or given an opportunity to be pursued with respect to the allocation of Internet Addresses. It is assumed (rightly or wrongly) that having governments cooperate in this regard will be bad for the development of the Internet.

Furthermore, the right of ICANN⁴⁰ to allocate Internet Protocol Addresses to RIRs arises not because national governments have agreed to such an arrangement, but because the United States Department of Commerce has entered into a memorandum of understanding with ICANN. Consequently, it is necessary to ask whether the United States was authorized by other countries to do so. If not, what is the authority of the United States in entering an arrangement which affects all other countries?

The principal issue is one of national sovereignty — and whether a national government is perceived as being subordinate to another. These organizations owe their origin not to government cooperation, but to cooperation among a few individuals. The informality which existed at the time is argued to continue until today. Yet, these organization have become very formal in their organizational structure, their operations and functions, and their development of policies. Effectively, these organization perform quasi-governmental functions.

Second, the rise of United States political dominance and supremacy is of concern among other nation states. This rise is particularly manifested in the

39 Braithwaite and Drahos, “Telecommunications”, *Global Business Regulation* (2000), at p. 322.

40 The functions and responsibilities of IANA are being transferred to ICANN.

administration and management of Internet Protocol Addresses. IANA's right to manage and administer Internet Protocol Addresses arises not because of cooperation among nation-states, but because of a contract that IANA has with the United States government. This arrangement alters the peer-to-peer relationship which exists among nation-states to one which is hierarchical, meaning that there are some states that are supreme (or primary) and some that are secondary.

Countries such as Taiwan, China, Vietnam, Japan, Indonesia, and Korea have taken steps towards reclaiming some degree of sovereignty by setting up NIRs to allocate Internet Protocol Addresses. However, the establishment of NIRs does not alter the main issue, i.e., that ICANN/IANA allocates Internet Protocol Addresses to RIRs which, in turn, allocate the addresses to NIRs. The entire hierarchical structure is based on RFC2050 of November 1996.

Furthermore, ICANN has set up a Governmental Advisory Committee⁴¹ which:

. . . should consider and provide advice on the activities of ICANN as they relate to concerns of governments and where they may affect public policy issues. The Advice of the Governmental Advisory Committee on public policy matters shall be duly taken into account by ICANN, both in the formulation and adoption of policies.

The central administration and management of the Internet Protocol Address system by a single entity of itself is not objectionable, simply because it is necessary to enable central coordination to occur. What is perhaps objectionable is that the authority granted to ICANN by the United States government indicates that all other governments are subordinate to the United States.

What is needed is for ICANN to seek approval from national governments for what it does. This may help to alleviate the concern that governments are being marginalized as to a resource (i.e., Internet Protocol Addresses) that is crucial for the effective participation in the knowledge economy and which is subject to United States control or dominance.

(c) Regulating Internet Access

The evolution of the Internet and the privatization of government-owned telecommunications providers created the environment that saw the rise of the Internet as a medium by which individuals anywhere in the world could communicate with one another at a fraction of the cost of a long-distance telephone call.

With this, governments began exploring ways and means by which Internet access could be regulated. Some governments viewed Internet access as a form of telecommunication service, while others did not. The approach by governments towards regulating Internet access has been piecemeal. Most

41 See <http://194.78.218.67/web/index.shtml>.

governments had in place telecommunication laws, and they used these laws to regulate access to the Internet.

However, since the 1990s, Internet access regulation has evolved. Governments today recognize that the Internet brings about a convergence of what were once separate and distinct functions or activities, i.e., telecommunications and broadcasting.

Table 2, below, summarizes the various types of Internet access regulation used by selected countries in regard to licensing of Internet Service Providers or Internet Access Providers. It is non-exhaustive but is representative of the dominant types of regulatory regimes.

Table 2 — Types of Internet Access Regulation

Country Name	No license required (Qualifications)	Individual license or concession required (Qualifications)	Class license required (Qualifications)
Anguilla		Yes	Yes (the regulator may decide that ISPs may be subject to a class license)
Australia	Yes (must comply with Schedule 2 of the Telecommunications Act 1997)		
Bahrain			Yes
Barbados		Yes	
Brunei Darulsalam			Yes (only registration required, and class license automatically applies)
Bulgaria	Yes		
China		Yes	
Cook Islands		Yes	
European Union			Yes (as a general authorization)
Germany		Yes	
Grenada		Yes (Internet Network/Services)	Yes (Internet Service provision Type A Class License)

Hong Kong SAR			Yes
India		Yes	
Indonesia		Yes	
Jamaica		Yes	
Japan		Yes	
Korea		Yes (but apply by way of registration)	
Macau SAR		Yes	
Malaysia			Yes (only registration required)
New Zealand	Yes		
Russian Federation		Yes (Telemetric services license (to provide e-mail and hosting services if a company does not have its own lines). Data transmission and telematic services licenses (for companies that use their own external lines). Licenses for additional services (e.g., Internet Protocol (Internet Protocol telephone)	
Singapore ⁴²		Yes (applies to Public Internet Access Service)	Yes (Registration required; Internet based voice and data service)
South Africa		Yes	
Uganda		Yes	
United States	Yes		
Vietnam		Yes	
Zambia		Yes (including tele-centers)	

The licensing regimes as introduced in these countries can be grouped into three categories, as identified in Table 3, below.

42 See http://www.ida.gov.sg/idaweb/doc/download/I1301/SBO_Guidelines-8Sep2004.pdf, accessed on 12 January 2005.

Table 3 — Licensing Regimes

Licensing Regime	Description	Explanation
<i>Group 1:</i> A strict licensing regime (usually identified as an individual licensing regime)	Where the state authority reviews the formal license application and grants a license to operate an Internet service or access business. This is usually termed as an individual license regime. ⁴³	This regime is used by most countries when they first embark on allowing Internet access. The rationale is that the government is able to control the access point and is therefore able to continue to exercise influence over what people access. For example, Singapore requires providers of Public Internet Access Services to have an individual Service-Based Operator license. ⁴⁴ The difference between countries using an individual license regime is the degree of transparency and bureaucratic discretion that exist. The greater the transparency and the less discretionary, the easier it is for businesses to operate.
<i>Group 2:</i> A less formal or more liberal licensing regime (usually identified as a class licensing regime)	Where the state authority permits entities wishing to offer Internet access to do so without the need for a formal license application. The license conditions are published, and individuals may either register or merely undertake the business and be deemed to be licensed.	This regime is used when a country determines that providing Internet access is a necessity to be able to participate in the knowledge economy. In addition, the economic philosophy of the country is a liberal and open market economy. If these elements are present, it is likely that a class licensing regime will be introduced. Class licensing regimes do not require formal license applications. The nature of being licensed varies, where some countries merely require entities to be registered with the national regulatory authority (i.e., a simple process to get licensed), whereas other countries deem entities that provide the service to be subjected to a class license (i.e., an automatic license).

43 Although this process lends itself to the grant of concessions by the government, which is usually adopted when the country does not have a clear set of regulations. The concession agreement sets out the rights and obligations of both the private enterprise and the government.

44 Guidelines For Submission of Application for Services-Based Operator License, Info-Comm Development Authority, at http://www.ida.gov.sg/idaweb/doc/download/I1301/SBO_Guidelines-8Sep2004.pdf accessed on 28 December 2004.

		<p>In both situations, the conditions of the class licensed are published and entities are aware of the conditions that they must abide by.</p> <p>For example, in Malaysia, the provision of Internet access is a class-licensed activity (categorized as a class application service provision) and merely requires providers to be registered. The licensed conditions are gazetted and are publicly available.⁴⁵</p>
Group 3: No license required	Where the activity does not require a license from the state authority, but the provider may or may not be obligated to comply with certain rules and regulations.	<p>The belief that the market can best discipline participants leads to the approach that there should be no requirement for licenses to provide access to the Internet. In this situation, the regulatory framework is viewed as imposing unnecessary burdens on a fledgling industry and the regulator.</p> <p>This belief has been proven accurate as evidenced by the rise of the number of Internet Access Providers and Internet users in countries such as Australia and the United States, where such a system is practiced.</p>
		<p>For example, the United States does not require Internet Service Providers or Internet Access Providers to be licensed as it considers them to be providers of “information services”.⁴⁶ In Australia,⁴⁷ ISPs and IAPs are unlicensed, but they must comply with specific provisions in the Telecommunications Act 1997 and the Telecommunications (Consumer Protection and Service Standards) Act 1999.</p> <p>This does not mean that Internet Access Providers are totally unregulated. All it means is that there is no requirement for them to obtain a license before providing a service. They are subject to various regulations such as in Australia, where they are subjected to the Internet Content Code enforced by the Australian Broadcasting Authority.</p>

45 Communications and Multimedia Act 1998 and the Communications and Multimedia (Licensing) Regulations 2000.

There are various approaches taken by developing countries towards the regulation of Internet Service Providers, as set out in the tables, below.⁴⁸ The approach by developing countries towards regulating Internet service follows the same “tri-chotomy” as set out in Table 3, above, namely:

1. Requiring no licensing;
2. Requiring a simple licensing process (i.e., class license regime); or
3. Requiring a formal and strict licensing process (i.e., individual licensing regime).

Table 4 — Prior Approval Not Required

Country	Year Regulator Established	Approval Required for ISP to Start Operations	ISP Prices Regulated?
Brazil	1997	None	No
Bulgaria	1998	None	No
Chile	1977	None	No
El Salvador	1996	None	No
Moldova	N/A	None	No
Tanzania	1993	None	Yes

Table 5 — Only Notice Required

Country	Year Regulator Established	Approval Required for ISP to Start Operations	ISP Prices Regulated?
Bolivia	1995	Notification	No
Bosnia and Herzegovina	2001	Notification	N/A
Czech Republic	2000	Notification	No

46 “Licensing Options for Internet Service Providers”, at http://www.Internetpolicy.net/practices/licensing_options.pdf, accessed on 28 December 2004.

47 See [http://Internet.aca.gov.au/Australian Communications AuthorityINTER2097602:STANDARD:1167708603:pp=PC_1621,pc=PC_1622](http://Internet.aca.gov.au/Australian%20Communications%20AuthorityINTER2097602:STANDARD:1167708603:pp=PC_1621,pc=PC_1622), accessed on 28 December 2004.

48 Wallsten, “Regulation and Internet Use in Developing Countries”, at <http://www.aei-brookings.org/admiN/Authorpdfs/page.php?id=262>, accessed on 12 December 2004.

Estonia	1998	Notification	No
Malaysia	1998	Notification	Yes (dial up)
Mexico	1996	Notification	No
Pakistan	1996	Notification	No
Poland	2000	Notification	No
Slovakia	1993	Notification	No

Table 6 — Approval Required

Country	Year Regulator Established	Approval Required for ISP to Start Operations	ISP Prices Regulated?
Argentina	1990	Formal	No
Barbados	2001	Formal	No
Colombia	1994	Formal	No
Costa Rica	1996	Formal	N/A
Côte d'Ivoire	1995	Formal	Yes
Dominican Republic	1998	Formal	No
Ecuador	1995	Formal	No
Ghana	1996	Formal	No
Guatemala	1996	Formal	No
Honduras	1995	Formal	No
Hungary	1990	Formal	No
India	1997	Formal	No
Jamaica	1997	Formal	No
Jordan	1995	Formal	Yes
Kenya	1999	Formal	No
Malawi	1998	Formal	Yes
Mongolia	1995	Formal	No

Panama	1996	Formal	No
Peru	1991	Formal	No
Romania	2001	Formal	No
South Africa	2000	Formal	No
Sri Lanka	1991	Formal	Yes
Venezuela	1991	Formal	No

Table 7 — Approval Not Available

Country	Year Regulator Established	Approval Required for ISP to Start Operations	ISP Prices Regulated?
Belize	1997	N/A	Yes
Latvia	1992	N/A	No
Morocco	1998	N/A	No
Thailand	2001	N/A	N/A
Turkey	2000	N/A	No
Uganda	1997	N/A	No

The use of formal licensing regimes arises partially because of the political concerns that the political elite has with permitting full access, namely the dangers (real or perceived) of political instability. As a result, the borderless nature of the Internet has not stopped governments from controlling access of its people to the Internet or the Web. Ultimately, what is important in developing a regulatory framework is that the framework must:

1. Enable the nation's goals or objectives to be achieved or materialized;
2. Be transparent;
3. Have a certain and fair process; and
4. Avoid the creation of unnecessary transactional costs.

It should be noted that the regulation of Internet Service Providers by national regulatory authorities is a highly contentious issue as it relates to economic and competition regulation. These areas are considered outside the scope of this chapter, but readers should bear in mind these other areas when considering the regulation of Internet Service Providers.

(d) Regulating Online Content*(i) In General*

The concept of “content” in the Internet world encompasses anything that is created and would apply, from ordinary email to Web sites and weblogs. The wide scope of the word “content” provides a difficulty for governments when they consider content regulation. How far should such regulation go (i.e., a jurisdictional issue)? How wide should it reach (i.e., a scope issue)?

Control of content exists despite article 19 of the Universal Declaration of Human Rights, which provides that:

... [e]veryone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

The International Chamber of Commerce defines Internet content regulation as:

... any type of legislation by governments or regulatory authorities directed at:

censoring information and communication on the Internet based on its subject matter, and
controlling, or attempting to control, access to Internet sites based on subject matter.⁴⁹

The control of access to particular Web sites based on their content is achieved by controlling access to the Internet. Hence, governments which advocate tight control of access to content tend to use individual licenses to control access to the Internet. In addition to tighter licensing controls, such governments tend to use filtering software or proxy server farms to manage access to content by blocking access based on the Internet Protocol Address of the server where the content is hosted. By controlling the providers of access, content which is prohibited can be similarly controlled.

The issue of regulating content is not a new one. It is part of an on-going debate between those who believe that the state has a role to ensure that harmful content is prohibited and those who believe that the individual must have a right to choose. The chasm between community rights and individual rights divides the debate over Internet content regulation. It has been pointed out that:

... [t]he key concern in the area of telecommunications regulation is not to attempt to alter or overlook these strictures in the drive to unleash market forces and economic growth through information technology. Rather, it should be to seek means to accommodate legal and

49 See http://www.iccwbo.org/home/statements_rules/statements/2002/Internet_content.asp, accessed on 5 February 2005.

cultural reservations about unfettered communications without building unnecessary new barriers to electronic commerce.⁵⁰

While it is beyond the scope of this examination to consider all other laws that are applicable to content (whether online or otherwise), such as the law of defamation and publication of seditious material, the chapter will focus on identifying what some countries are doing with respect to regulating online content and will identify the regulatory approaches.

(ii) Regulatory Approaches

In General It is possible to categorize various regulatory approaches taken by the selected countries as follows:

1. A legal prohibition regime, where providing or accessing certain types of content (whether online or not) is criminalized, requiring law enforcement authorities to monitor and prosecute offenders;
2. A legal prohibition regime and a technical “gatekeeper” system, where the legal regime prohibits the provision of or access to certain types of online content and the state controls access by means of filtering software and proxy server farms, where blocking techniques are used; and
3. A co-regulatory regime, where the Internet industry sets out the applicable rules in respect of controlling access to online content, and where the regulatory authority will only step in should the industry code not function adequately.

The choice of regime reflects the political views of the ruling elite. If they hold extremely conservative views or are less tolerant of dissent, it is more likely that they would employ the legal prohibition with a gatekeeper system. On the other hand, if the ruling elite recognizes that banning online content is difficult because of available software that allows one to by-pass such filters, coupled with the fact that it is necessary that knowledge be available so as to enable greater economic development, a co-regulatory regime will be adopted.

Approaches to Regulating Online Content The choice of countries below reflects a broad spectrum as to the regulation of online content. The United States is excluded because attempts by government to introduce legislation (such as the Communications Decency Act or the Child Online Protection Act) to control access to certain types of content, especially those that affect minors, have been met with successful challenges in the courts.

50 Townsend, “Telecommunications Regulatory Issues for Electronic Commerce”, Report to the International Telecommunication Union, 8th Regulatory Colloquium, at <http://www.infodev.org/projects/ecommerce/341itu8/341.pdf>, accessed on 12 February 2005.

Consequently, the approach of the United States is that online content should not be censored or controlled. Thus, the United States does not provide any appropriate means to consider how to control online content.

Singapore Singapore has a three-prong approach to Internet content regulation,⁵¹ as follows:

1. A light-touch, class license scheme, which provides minimum standards to safeguard values and promote healthy growth;
2. The encouragement of industry self-regulation; and
3. An active public education program to promote parental supervision.

The class license scheme is an automatic licensing scheme that requires IASPs and content providers to comply with an Internet Code of Practice. IASPs are not required to monitor or censor Internet content. They are, however, required to limit public access to 100 mass-impact pornography sites. Personal communications, such as email or Internet relay chat, personal websites, and corporate Internet use by employees or for business transactions, are not regulated.⁵²

Since its formation on 1 October 1994, the [Singapore Broadcasting Authority] has been tasked with the job of developing quality broadcasting, building a well-informed and culturally rich society and making Singapore a dynamic broadcasting hub. The SBA is, in addition to its various other functions, responsible for regulating Internet Service Providers and Internet Content Providers. This is done chiefly through the Internet Class License Scheme and the Internet Code of Practice which was first introduced in July 1996 via *Gazette* Notification Number 2400/96. The Internet Code of Practice was subsequently revised to remedy some of the shortcomings and perceived inadequacies of the earlier version of the Code as well as to take into account the recommendations made by the National Internet Advisory Committee (NIAC) in its report released in September 1997. The revised Code of Practice came into effect on 1 November 1997 via *Gazette* Notification Number 3810/97.⁵³

Malaysia Malaysia operates a co-regulatory scheme for Internet content, as set out in the Communications and Multimedia Act 1998. It requires a

51 UNPAN, "Singapore's Legal and Policy Environment for E-commerce", at <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN002010.pdf>, accessed on 5 February 2005.

52 SBA (Class License) Notification, 15 July 1996; SBA Internet Code of Practice, 1 November 1997.

53 Anil, "Re-Visiting the Singapore Internet Code of Practice", 2001(2) *Journal of Information, Law and Technology*, at <http://elj.warwick.ac.uk/jilt/01-2/anil.html/>, accessed on 5 February 2005.

designated industry group (the Communications and Multimedia Content Forum of Malaysia)⁵⁴ to develop a content code, with which members are to comply. The code is required to be registered with the Commission after it has undergone a public consultation process. However, once the code is registered, it affords any one who complies with it a defense to any action brought.

This provides the incentives for compliance. In addition, the Communications and Multimedia Commission may direct a licensee to comply with the content code, and a failure to do so is a breach of a legal instrument, with the possibility of criminal sanctions being imposed.

The code defines and describes the various types of prohibited content enabling content providers to have clearer guidance on what is prohibited and what is not. This arose because the previous regimes did not have any clear guidelines. By section 213 of the Communications and Multimedia Act 1998, the areas which are to be in the content code include model procedures for dealing with offensive or indecent content, as well as addressing such matters as:

1. The restrictions on the provision of unsuitable content;
2. The methods of classifying content;
3. The procedures for handling public complaints and for reporting information about complaints to the Commission;
4. The representation of Malaysian culture and national identity;
5. Public information and education regarding content regulation and technologies for the end user control of content; and
6. Other matters of concern to the community.

The need for the content code to explain and define the types of prohibited content exists because of the prohibition in the Communications and Multimedia Act 1998, which makes it an offense to provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten, or harass any person. Consequently, the code elaborates in some detail what is indecent, obscene, false, menacing, or offensive content.

With respect to online content, the general approach is to place the responsibility for the content with the end-user. The end-user determines what he wants. The ISPs and other content hosts act as mere intermediaries and, hence, the concept of an “innocent carrier” is introduced. The “innocent carrier” concept introduced by the content code recognizes that IASPs are nothing more the carriers and that they do not have control over the content

54 See <http://www.cmcf.org.my/>.

which their subscribers access to. This inability to control, and the futility of imposing legal obligations on ISPs to control access, has produced this concept. However, once the IASP (including content hosts and aggregators) is aware of the type of content (and this is through a direction from the Complaints Bureau), the IASP (including content hosts and aggregators) is to remove the offending content.

Australia According to the Australian Broadcasting Authority (ABA),⁵⁵ it administers a “co-regulatory” scheme for Internet content. The scheme aims to address community concerns about offensive and illegal material on the Internet and, in particular, to protect children from exposure to material that is unsuitable for them. The scheme is established under Schedule 5 of the Broadcasting Services Act 1992, which gives the ABA the following functions:

1. Investigation of complaints about Internet content and Internet gambling services;
2. Encouragement of development of codes of practice for the Internet industry, registering, and monitoring compliance with such codes;
3. Provision of advice and information to the community about Internet safety issues, especially those relating to children’s use of the Internet;
4. Undertaking of research into Internet usage issues and informing itself and the Minister of relevant trends; and
5. Liaison with relevant overseas bodies.

In performing its role, the ABA is guided by principles laid down in legislation which have the aim of minimizing the financial and administrative burdens on industry and encouraging the supply of Internet services at performance standards that meet community needs. Furthermore:

... the co-regulatory scheme for Internet content allows for and encourages the development of three codes of practice. . . one for Internet content hosts (ICHs) and two for Internet Service Providers (ISPs).

The codes are registered with the ABA, and compliance is voluntary, unless the ABA directs an ISP or Internet content host to comply with the code. Once this direction is given, if the directed entity fails to comply, it commits an offence under the Broadcasting Services Act 1992.

The Australian approach is one which is led by industry. Industry determines what it wishes to abide by, and the code is then developed. This code is then registered after it goes through a public consultation process. This form of “co-regulation” is seen as empowering industry to govern themselves, with the regulatory authority taking a back seat and only intervening when there has been a failure.

55 See <http://www.aba.gov.au/Internet/>.

China China, in “1995, . . . began permitting commercial Internet accounts, [and] at least 60 sets of regulations have been issued aimed at controlling Internet content”.⁵⁶ Some rules are directly aimed towards content control, such as:

1. The Decision of the Standing Committee of the National People’s Congress on Maintaining Internet Security (2000);
2. The Measures for Managing Internet Information Services (2000);
3. The Provisional Rules for the Administration of the Operation of News Publication Services by Web Sites (2000);
4. The Rules for the Administration of Internet Bulletin Board System Services (2000);
5. The Rules for the Administration of Computer & Internet Bulletin Board System Services in the Colleges (2001); and
6. The Interim Provisions on the Administration of Internet Publication (2002).

Other rules are aimed at Internet cafes, state secrecy, network security, and encryption, but they also indirectly have a strong impact on Internet content regulation.

Article 15 of the Measures for Managing Internet Information Services provides that “[i]nformation that is detrimental to the honor and interests of the state” is banned on the Internet. Yet, an Internet user has no way of knowing what topics might be considered injurious. Online speech which only criticizes the current leaders or expresses some discontent with the government will perhaps be interpreted to violate this provision. Such obscurity gives the government wide discretion, and a stronger basis on which to arrest and punish persons who engage in such forms of expression. Sometimes, the result is unpredictable. The public notice at one chat room identifies what type of content is prohibited:

Please take note that the following issues are prohibited according to Chinese law:

1. Criticism of the PRC Constitution
2. Revealing State secrets, and discussion about overthrowing the Communist government
3. Topics that damage the reputation of the State
4. Discussions that ignite ethnic animosity, discrimination or regional separatism

⁵⁶ Li, “Internet Content Control in China”, *International Journal of Communications Law and Policy*, Issue 8, Winter 2003/2004, at http://www.ijclp.org/8_2004/pdf/charlesli-paper-ijclp-neu.pdf, accessed on 12 February 2005.

5. Discussion that undermines the state's religious policy, as well as promotes evil cults and superstition
6. Spreading rumors, perpetrating and disseminating false news that promotes disorder and social instability
7. Dissemination of obscenity, sex, gambling, violence, and terror. Cyber-sex is not permitted within the English chat-room.
8. Humiliating or slandering innocent people
9. Any discussion and promotion of content which PRC laws prohibit.

“These rules grant various government authorities full power to monitor organizations and individuals on the Internet”.⁵⁷ China spends a considerable amount of time and resources in implementing these content control rules and uses drastic enforcement measures to ensure compliance with them, such as arresting “Lin Hai, who was considered the first detained ‘Internet dissident’ in China”.⁵⁸ The rules have shifted the:

... primary responsibility for control of the Internet from the government to ... Internet Service Providers. The regulations decentralize responsibility. As a result, content is not double- but triple-checked: at the gateway of the dominant connectors such as China Telecom, at the network responsible for delivering the content, and the receiver itself ... [which] is a very effective way to make Internet participants adhere to those norms beneficial to the Communist Party of China's control.⁵⁹

All of these regulations make surveillance on the Internet legal in China.

There are other laws which apply to controlling access to or production of online content, such as:

1. The Measures on the Administration of Broadcasting Audio/Visual Programs over the Internet or Other Information Networks,⁶⁰ which impose a licensing requirement for any person who transmits audio/visual or news programs to the public via the Internet;

57 Li, “Internet Content Control in China”, *International Journal of Communications Law and Policy*, Issue 8, Winter 2003/2004, at http://www.ijclp.org/8_2004/pdf/charlesli-paper-ijclp-neu.pdf, accessed on 12 February 2005.

58 Li, “Internet Content Control in China”, *International Journal of Communications Law and Policy*, Issue 8, Winter 2003/2004, at http://www.ijclp.org/8_2004/pdf/charlesli-paper-ijclp-neu.pdf, accessed on 12 February 2005.

59 Li, “Internet Content Control in China”, *International Journal of Communications Law and Policy*, Issue 8, Winter 2003/2004, at http://www.ijclp.org/8_2004/pdf/charlesli-paper-ijclp-neu.pdf, accessed on 12 February 2005.

60 See <http://www.cecc.gov/pages/virtualAcad/exp/explaws.php>, accessed on 12 February 2005.

2. The Interim Provisions on the Administration of Internet Publishing, which require that Internet publishing activities can be done if prior permission be obtained; and
3. The Provisions on the Administration of Internet Electronic Bulletin Board Services, which require that bulletin board services be specifically set out when applying for the appropriate license, e.g., a commercial Internet Information Service License.⁶¹

Finally, China practices a gatekeeper system to control access to online content. This is done by strictly regulating the backbone network connections to the Internet outside China. By limiting the number of backbone network connections, China can effectively limit access to online content, thus controlling what its people are able to access.

Saudi Arabia In Saudi Arabia, the online content rules are contained in the Council of Ministers Resolution of 2001,⁶² which provides:

Publishing or accessing restricted data should be refrained;

Setting up websites or publishing Web pages must observe defined requirements as detailed below:

All Internet users in the Kingdom of Saudi Arabia shall refrain from publishing or accessing data containing some of the following:

1. Anything contravening a fundamental principle or legislation, or infringing the sanctity of Islam and its benevolent Shari'ah, or breaching public decency.
2. Anything contrary to the state or its system.
3. Reports or news damaging to the Saudi Arabian armed forces, without the approval of the competent authorities.
4. Publication of official state laws, agreements or statements before they are officially made public, unless approved by the competent authorities.
5. Anything damaging to the dignity of heads of states or heads of credited diplomatic missions in the Kingdom, or harms relations with those countries.
6. Any false information ascribed to state officials or those of private or public domestic institutions and bodies, liable to cause them or their offices harm, or damage their integrity.

61 The subject matter of the bulletin board is subject to prior approval. One is not allowed to provide a bulletin board on a subject which has not been approved. Bulletin board providers must monitor the content placed on the board and delete it if it is prohibited under article 9, retain records, and report to the authorities.

62 See <http://www.al-bab.com/media/docs/saudi.htm>, accessed on 13 February 2005.

7. The propagation of subversive ideas or the disruption of public order or disputes among citizens.
8. Anything liable to promote or incite crime, or advocate violence against others in any shape or form.
9. Any slanderous or libelous material against individuals.

Furthermore, certain trade directives stipulate that all companies, organizations, and individuals benefiting from the service may not:

1. Carry out any activity through the Internet, such as selling, advertising, or recruitment, except in accordance with the commercial licenses and registers in force;
2. Carry out any financial investment activity or offer shares for subscription, except when in possession of the necessary licenses to do so;
3. Promote or sell medicines or foodstuff carrying any medicinal claims, or cosmetics, except those registered and approved by the Ministry of Health;
4. Advertise or promote or sell substances covered by other international agreements to which the Kingdom is a party, except for those with the necessary licenses; and
5. Advertise trade fairs or organize trade delegations visits or tourist tours or trade directories, except those with the necessary licenses.

All private and government departments, and individuals, setting up websites or publishing files or pages, must:

1. Respect commercial and information conventions;
2. Have the approval of government authorities for setting up websites or publishing files or pages for or about themselves;
3. Have the approval of the Ministry of Information for setting up media-type websites which publish news on a regular basis, such as newspapers, magazines, and books;
4. Observe good taste in the design of websites and pages;
5. Assure the effective protection of data on websites and pages; and
6. Take full responsibility for websites and pages and the information contained therein.

The Resolution refers to a set of regulatory and technical procedures aimed at ensuring the safety of the constituents of the national network

(the Internet inside the Kingdom) through effective programming and mechanical means. These include:

1. Service providers must determine Internet access eligibility through access accounts, user identification, and effective passwords for the use of the access point or subsequent points and linking that through tracing and investigation programs that record the time spent, addresses accessed or to which or through which access was attempted, and the size and type of files copied, when possible or necessary;
2. Anti-virus programs and protection against concealing addresses or printing passwords and files must be employed;
3. Providers must endeavor to avoid errors in applications that may provide loopholes that may be exploited for subversive activities or to obtain data not permitted for use for whatever reason;
4. Provision of Internet services must be restricted to the end-user through the Internet service unit at King Abdulaziz City for Science and Technology;
5. Providers must maintain a manual and electronic register with comprehensive information on end-users, their addresses, telephone numbers, purpose of use, and private Internet access accounts, and provide the authorities with a copy thereof, if necessary; and
6. Providers may not publish any printed directories containing subscriber and end-user names and addresses, without their agreement.

The government utilizes content-filtering technologies and proxy servers to maintain control over access to certain contents.⁶³ According to the Internet Services Unit (ISU) of the King Abdulaziz City for Science and Technology (KACST), the content-blocking policy⁶⁴ states that:

A security committee chaired by the Ministry of Interior was [formed], with one of its tasks . . . is the selection of sites to be blocked and the oversight of this process. However, due to the wide-spread and diverse nature of pornographic sites, KACST was [requested] to directly block these types of sites. Other non-pornographic sites are only blocked based on direct requests from the security bodies within the government. KACST has no authority in the selection of such sites and its role is limited to carrying out the directions of these security bodies.

63 Zittrain and Edelman, "Documentation of Internet Filtering in Saudi Arabia", Berkmen Centre for Internet and Society, Harvard Law School, at <http://cyber.law.harvard.edu/filtering/saudi-arabia/>, accessed on 12 February 2005.

64 See <http://www.isu.net.sa/saudi-Internet/content-filtering/filtration-policy.htm>, accessed on 12 February 2005.

Filtering is undertaken by passing all incoming Web traffic to Saudi Arabia through a proxy system operated by the ISU, which uses a content-filtering software to filter out prohibited content. Furthermore, a list of Internet Protocol Addresses for banned sites is maintained by the filtering system. The list is updated daily based on the content-filtering policy. However, individuals can report to the ISU and request that content from certain sites be blocked.⁶⁵

The Philippines The Philippines does not have any specific rules governing access to online content, and it relies on its general law that makes it an offence to provide obscene and pornographic material.⁶⁶ Furthermore, specific statutes are believed to provide adequate control of online content. These include:

1. Republic Act Number 7610, the Special Protection of Children Against Child Abuse, Exploitation, and Discrimination Act, 1992, which seeks “to provide special protection to children from all forms of abuse, neglect, cruelty exploitation and discrimination and other conditions” and makes criminally liable “any person who shall hire, employ, use, persuade, induce, or coerce a child to perform in obscene exhibitions and indecent shows, whether live or in video, or model in obscene publications or pornographic materials or to sell or distribute the said materials”;⁶⁷
2. Republic Act Number 6955 of 13 June 1990, which criminalizes the practice of establishing and carrying on businesses that match Filipino women for marriage to foreign nationals on a mail-order basis and other similar practices;⁶⁸ and
3. Republic Act Number 9208, the Act to Institute Policies to Eliminate Trafficking in Persons, Especially Women and Children, Establishing the Necessary Institutional Mechanisms for the Protection and Support of Trafficked Persons (the “Anti-Trafficking in Persons Act of 2003”),

65 See <http://www.isu.net.sa/saudi-Internet/content-filtrng/filtrng-mechanism.htm>, accessed on 12 February 2005.

66 Monte-Medina, “Policy Directions To Regulate Harmful Internet Content: The Philippine Experience”, a Paper Presented at the Forum on ICTs and Gender, 20–23 August 2003, Kuala Lumpur, Malaysia, at http://www.globalknowledge.org/gkps_portal/view_file.cfm?fileid=1111, accessed on 11 February 2005.

67 Special Protection of Children Against Child Abuse, Exploitation, and Discrimination Act, 1992, section 9.

68 Section 2(a)(2) of Republic Act Number 6955 makes it unlawful “to advertise, publish, print, or distribute or cause the advertisement, publication, printing, or distribution of any brochure, flier, or any propaganda material” to promote the matching of Filipino women to foreign nationals for marriage on a commercial basis.

which specifically contemplates Internet content in defining “pornography” and the crime of trafficking in persons.⁶⁹

United Kingdom The United Kingdom’s Internet Service Providers Association developed a Code of Conduct 1999 (amended 2002),⁷⁰ which its members agree to adopt on becoming a member. It is an industry-led regulatory framework in the form of industry self-regulation. In essence, the Code of Conduct, as it applies to online content, provides:

1. Content must comply with United Kingdom law;
2. Material ought not to be provided which incites violence, cruelty, or racial hatred; and
3. Contents should not mislead by being inaccurate, ambiguous, exaggerated, omissive, or otherwise.

The Code refers to actions which may be taken by the Internet Watch Foundation (IWF),⁷¹ such as where members of Internet Service Providers Association agree that:

... where the IWF has notified them that Internet sites and Usenet news groups contain material which the IWF considers to be illegal child pornography, members will remove such materials, wherever it is technically possible to do so Where requested by the IWF (on behalf of a legitimate law enforcement authority), and where technically able to do so, members must retain copies of removed material for a reasonable period of time. . Members should take careful consideration of all other IWF notices and recommendations.

In effect, the use of a self-regulatory regime to control online content is seen as a more practicable approach than through legislation, although what is

69 Section 3(h) of the Anti-Trafficking in Persons Act defines “pornography” as any “representation, through publication, exhibition, cinematography, indecent shows, information technology, or by whatever means, of a person engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a person for primarily sexual purposes”. Section 5(c) of the Act makes it unlawful “to advertise, publish, print, broadcast, or distribute or cause the advertisement, publication, printing, broadcasting, or distribution by any means, including the use of information technology and the Internet, of any brochure, flyer, or any propaganda material that promotes trafficking in persons”.

70 A copy of ISPA’s Code of Conduct is available at http://www.ispa.org.uk/html/index3.html?frame=http%3A//www.ispa.org.uk/html/about_isp/ispa_code.html, accessed on 18 April 2005.

71 “The Internet Watch Foundation was formed in 1996 following an agreement between the government, police, and the Internet service provider industry that a partnership approach was needed to tackle the distribution of child abuse images (often referred to as child pornography) online”. Internet Watch Foundation web site, available at <http://www.iwf.org.uk/public/page.103.htm>.

prohibited content is dependent on the local legislation. In the United Kingdom, for example, legislation exists which renders certain types of content prohibited, as shown in the table below.

Subject Matter	Prohibited Because
Child abuse images	Protection of Children Act 1978 Civic Government Act 1982 (Scotland) Sexual Offences Act 2003
Obscene Publications — There is no definition, other than it must be content which tends to “deprave and corrupt” those likely to read, see, or hear the matter contained or embodied in it. As the possible width of the words “deprave and corrupt”, the IWF identifies as a guide and for ease the following types of content which are considered as obscene, “images featuring acts of extreme sexual activity such as bestiality, necrophilia, rape, or torture”.	Obscene Publications Act 1959 and 1964
Racist Content — Content which stirs up racial hatred against a group of persons in Great Britain, by reference to color, race, nationality, ethnic or national origins.	Public Order Act 1936 (amended by the Race Relations Act 1976)

In two cases in the United Kingdom, *R. v. Bowden*⁷² and *R. v. Jayson*,⁷³ the court in the former case held that pseudo-photo is sufficiently wide to include what appears to be a photo; hence, downloading an image from a web site would be within the ambit of “pseudo” for the purposes of the Protection of Children Act 1978. The wording in section 1 of the Act, as amended, was clear and unambiguous. The words “to make” had to be given their natural and ordinary meaning, and in the instant context, that was “to cause to exist; to produce by action, to bring about”.

In the latter case, the Court of Appeal had to address the issue as to what constitutes “making” a photograph or “pseudo photograph” for the purposes of section 1(1)(a) of the Protection of Children Act 1978. It was held that “the act of voluntarily downloading an indecent image from a web page on to a computer screen is an act of making a photograph or

⁷² *R. v. Bowden* (2000) Cr. App. R. 438.

⁷³ *R. v. Jayson* (2002) E.W.C.A. Crim. 683; see also *R. v. Smith* (2002) E.W.C.A. Crim. 683.

pseudo-photograph”. The requisite *mens rea* is that the act of making should be a deliberate act with the knowledge that the image was, or was likely to be, an indecent photograph or pseudo-photograph of a child. No intention to store the image was required to satisfy the *mens rea* requirement. The case of *R. v. Smith* held that opening an email attachment containing an indecent image was sufficient to constitute “making” for the purposes of the Act.

These cases indicate the extent by which the United Kingdom courts are prepared to construe the word “making”, so that activities such as downloading or opening of email attachments may become criminalized, unless before the person opened the attachment he was unaware that it contained, or was likely to contain, such an image.⁷⁴

What is observable is that the United Kingdom uses both legislative and self-regulatory means by which online content is regulated. Laws are used to render certain activities offences and, at the same time, industry acts as a watch dog reporting the existence of such content to bodies such as INHOPE or to the law enforcement authorities. Yet, the question whether the online provider itself is exposed to liability needs to be addressed. According to European Directive 2000/31/EC, three areas are considered, i.e., hosting, caching, and mere conduit.⁷⁵

Area	Scope of Defense/Exclusion of Liability
Mere conduit	No criminal liability for that transmission where the service provider: (a) did not initiate the transmission; (b) did not select the receiver of the transmission; and (c) did not select or modify the information contained in the transmission.
Caching	No criminal liability where caching is done because of technical purposes (e.g., making more efficient onward transmission of the information to other recipients of the service on their request) or does not modify the data.
Hosting	No criminal liability if the service provider was unaware of the content, or on becoming aware, act expeditiously to remove the content or the recipient was not acting under the control of the service provider.

⁷⁴ *Atkins v. Director of Public Prosecution* (2000) 2 Cr. App. R. 248.

⁷⁵ See sections 17, 18, and 19 of the E-Commerce Regulations which implement the Directive.

The scope of the Directive is to enable the concept of “innocent carrier” to exist and be a defense recognizing that it is impossible to impose any effective legislative restriction on service providers to act as gatekeepers, as the cost to do so is prohibitive.

United States The United States has several statutes dealing with child pornography, making it an offence to own, distribute, advertise, or persuade any child to participate in any pornographic act. These statutes are:

1. The Sexual Exploitation of Children Act 1977;
2. The Child Protection Act 1984;
3. The Child Sexual Abuse and Pornography Act 1986;
4. The Child Protection and Obscenity Enforcement Act 1988;
5. The Telecommunications Act of 1996; and
6. The Child Pornography Prevention Act 1996.

Furthermore, the Children’s Internet Protection Act 2000 mandated schools and libraries to install Internet filters on all their computers as a condition for receiving federal funds. The law was upheld by the Supreme Court in June 2003.⁷⁶

In addition, the United States Internet Service Providers Association⁷⁷ identifies some key principles in respect of illegal online/internet content.⁷⁸ These are summarized below:

1. The liability for content should lie with the creators, and not with an entity that retransmits, hosts, stores, republishes, or receives such content;
2. If ISPs are mere conduits, they should have no liability (this is the concept of “innocent carrier”); and
3. If ISPs are content hosts, they should not be liable for content created by others, but they should have the responsibility to disable access to such content.

Interestingly, the reference used is “illegal content”, and this would appear to mean that the principles must be read with the existing legislation in the United States which renders a type of content as illegal. This eliminates the imposition of individual moral standards in an assessment of whether a particular type of content is or is not suitable.

⁷⁶ *United States v. American Library Association*, 123 S.Ct. 2297 (2003).

⁷⁷ The United States Internet Service Providers Association web site is at <http://www.usispa.org/index.html>.

⁷⁸ See <http://www.usispa.org/founding.html>, accessed on 24 April 2005.

The United States attempted to introduce legislation that prohibited “Internet users from using the Internet to communicate material that, under contemporary community standards, would be deemed patently offensive to minors under the age of 18” (under the Communications Decency Act 1996). It was challenged by the American Civil Liberties Union as being contrary to the First Amendment to the United States Constitution. The challenge was upheld by the Supreme Court,⁷⁹ which declared the Communications Decency Act 1996 unconstitutional on the basis that:

... [t]he CDA’s ‘indecent transmission’ and ‘patently offensive display’ provisions abridge ‘the freedom of speech’ protected by the First Amendment.

The Supreme Court also found that:

... the CDA differs from the various laws and orders upheld in [earlier] cases in many ways, including that it does not allow parents to consent to their children’s use of restricted materials; is not limited to commercial transactions; fails to provide any definition of ‘indecent’ and omits any requirement that ‘patently offensive’ material lack socially redeeming value; neither limits its broad categorical prohibitions to particular times nor bases them on an evaluation by an agency familiar with the medium’s unique characteristics; is punitive; applies to a medium that, unlike radio, receives full First Amendment protection; and cannot be properly analyzed as a form of time, place, and manner regulation because it is a content based blanket restriction on speech.

Subsequently, the United States government sought to introduce the Child Online Protection Act in 1998. The legislation was intended to protect minors from exposure to sexually explicit materials on the Internet. The Child Online Protection Act covers communications that are made for commercial purposes on the World Wide Web, and it requires commercial Web publishers to ensure that minors do not access “material harmful to minors” on their Web sites.

The Act was challenged as being unconstitutional in *Ashcroft v. ACLU* (2004).⁸⁰ The Supreme Court held that the Child Online Protection Act was inconsistent with the First Amendment and should be nullified.

79 Reno, *Attorney General of States, et al. v. American Civil Liberties Union et al.* (1997), available at <http://supct.law.cornell.edu/supct/html/96-511.ZS.html>.

80 See <http://supct.law.cornell.edu/supct/search/display.html?terms=COPA&curl=/supct/html/03-218.ZS.html> for an extract of the case.

Regional Supervision The Internet Hotline Providers in Europe Association (INHOPE),⁸¹ a Dutch registered association, is concerned with:

1. Child pornography;
2. Commercial sites;
3. Morphed and edited images;
4. Chat rooms and abduction;
5. Pedophile rings;
6. Racism;
7. Adult pornography; and
8. Grooming and conditioning of individuals to accept certain sexual behavior.

INHOPE is, however, not a law enforcement agency but has as its purpose to “facilitate and coordinate the work of Internet hotlines in responding to illegal use and content on the Internet”. This means that content which falls within the above-mentioned groups would be provided to law enforcement authorities in the countries where the content is located. INHOPE acts in some ways as a coordinating center for such exchange so that law enforcement authorities are able to take action in their respective countries.

Summary Attempts to control access to online content have been varied and with different measures of successes. What is perhaps clear is that the cost to a country to control access to online content is perhaps much higher than not to do so. The impetus for controlling online content is more to do with political control than it is to do with protecting individuals.

Despite this, it is recognized that there must be some element of control of access, especially with respect to minors. The choice of regime is very much a reflection of the particular country’s political development. Those countries who have moved out of a form of “paternalism” tend to be more liberal than those who have not.

(e) Co-Regulatory Regimes — A Comparative Analysis

The following section provides a comparative analysis of co-regulatory regimes in Australia, Malaysia, and Singapore in respect of controlling online content.

81 INHOPE’s web site is available at <http://www.inhope.org/en/index.html> (for the English language version).

(i) Comparative Analysis

Country Area	Singapore	Malaysia	Australia
Regulatory Instrument	Internet Code of Practice	Industry-developed content code Section 211, Communications and Multimedia Act 1998	Internet Industry Codes of Practice Schedule 5 of the Broadcasting Services Act 1992 (as amended)
Applies to	ISPs and Internet Content Providers	Providers of online content or those who provide access to online content, including Internet Access Service Providers (IASP), Internet Content Hosts, Online Content Developers, Online Content Aggregators, and Link Providers.	ISPs Internet Content Hosts
Type of content that is not allowed	Prohibited Material 4(1) Prohibited material is material that is objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws.	Part 2 of the Code provides definitions and examples of the following types of content, which are prohibited: 2.0 — Indecent Content 2.1 Indecent Content is material which is offensive, morally improper, and against current standards of accepted behavior. This includes nudity and sex.	Prohibited or Potentially Prohibited Content. Schedule 5 defines prohibited content as being: (a) the content has been classified “RC” (Refused Classification) or “X” by the Classification Board; or

	<p>(2) In considering what is prohibited material, the following factors should be taken into account:</p> <p>(a) whether the material depicts nudity or genitalia in a manner calculated to titillate;</p> <p>(b) whether the material promotes sexual violence or sexual activity involving coercion or non-consent of any kind;</p> <p>(c) whether the material depicts a person or persons clearly engaged in explicit sexual activity;</p> <p>(d) whether the material depicts a person who is, or appears to be, under 16 years of age in sexual activity, in a sexually provocative manner, or in any other offensive manner;</p> <p>(e) whether the material advocates homosexuality or lesbianism, or depicts or promotes incest, pedophilia, bestiality, and necrophilia;</p> <p>(f) whether the material depicts detailed or relished acts of extreme violence or cruelty;</p> <p>(g) whether the material glorifies, incites or endorses ethnic, racial, or religious hatred, strife, or intolerance.</p>	<p>i) Nudity Nudity cannot be shown under any circumstances, unless approved by the Film Censorship Board.</p> <p>ii) Sex and Nudity Sex scenes and nudity cannot be shown under any circumstances, unless approved by the Film Censorship Board.</p> <p>3.0 — Obscene Content 3.1 Obscene Content gives rise to a feeling of disgust by reason of its lewd portrayal and is essentially offensive to one's prevailing notion of decency and modesty. The test of obscenity is whether the Content has the tendency to deprave and corrupt those whose minds are open to such communication. Specific regard is to be had to:</p> <p>i) Explicit Sex Acts / Pornography Any portrayal of sexual activity that a reasonable adult considers explicit and pornographic is prohibited. The portrayal of sex crimes, including rape or attempted rape and statutory rape, as well as bestiality is not permitted, including the portrayal of such sexual acts, through animation and whether consensual or otherwise.</p>	<p>(b) the content has been classified "R" by the Classification Board and access to the content is not subject to a restricted access system.</p> <p>Potentially prohibited content is defined as being if the content has not been classified by the Classification Board, but if it were to be classified, there is a substantial likelihood that the content would be prohibited content.</p> <p>Australia applies the general law on classification of content as contained in the Classification (Publications, Films and Computer Games) Act 1995.</p>
--	---	--	---

<p>(3) A further consideration is whether the material has intrinsic medical, scientific, artistic, or educational value.</p> <p>(4) A licensee who is in doubt as to whether any content would be considered prohibited may refer such content to the Authority for its decision.</p>	<p>ii) Child Pornography Child pornography, including the depiction of any part of the body of a minor in what might be reasonably considered a sexual context, and any written material or visual and/or audio representation that reflects sexual activity, whether explicit or not, with a minor are strictly prohibited.</p> <p>iii) Sexual Degradation The portrayal of women, men or children as mere sexual objects or to demean them in such manner is prohibited.</p> <p>4.0 — Violence 4.1 Violence occurs through the ravages of natural disaster, outrageous acts of terrorism, war, human conflict both in fact and through popular fiction, the antics of cartoon characters, (body) contact sports, and more. Violence is a reality and Code Subjects need to be able to reflect, portray, and report on it. 4.2 To deny narration or depiction of hard truths about the world would tantamount to a substantial disservice to understanding of the human condition. The portrayal of violence, with careful editorial justification, is permitted</p>
--	--

	<p>4.3 Violence, psychological, but especially physical or incitement to violence, should be portrayed responsibly, and not exploitatively. Presentation of violence must avoid the excessive, the gratuitous, the humiliating, and the instructional. The use of violence for its own sake and the detailed dwelling on brutality or physical agony, by sight or sound, is to be avoided. Programs involving violence should venture to present the consequences to its victims and perpetrators. Particular care should be exercised where children may see, or be involved in, the depiction of violent behavior. Specific considerations are as follows:</p> <p>i) Offensive Violence</p> <p>The portrayal of violence, whether physical, verbal, or psychological, can upset, alarm, and offend viewers. It can be accused of causing undue fear among the audience and of encouraging imitation.</p> <p>The portrayal of violence is permitted to the extent of news reporting, discussion, or analysis and in the context of recognized sports events. In these matters:</p>	

	<p>a) The portrayal of violence, whether physical, verbal, or psychological, can upset, alarm, and offend viewers. It can cause undue fear among the audience and encourage imitation.</p> <p>b) Such public concerns require due consideration whenever violence, real or simulated, is portrayed. The treatment of violence must be appropriate to the context and audience expectations.</p> <p>c) Gratuitous and wanton presentation of sadistic practices and torture, explicit, and excessive imageries of injury and aggression, and of blood, are to be avoided.</p> <p>d) The portrayal of violence is permitted to the extent of news reporting, discussion, or analysis and in the context of recognized sports events in the following instances:</p> <p>i) Use of appropriate editorial judgment in the reporting of audio and visual representation of violence, aggression, or destruction within their content.</p> <p>ii) Exercise of caution and discretion in the selection of, and repetition of, Content which depicts violence.</p>	
--	---	--

	<p>iii) Viewers are to be cautioned in advance of showing scenes of extraordinary violence, or graphic reporting on delicate subject matter, with appropriate warnings to audiences in the case of gore or actual scenes of executions or of people clearly being killed.</p> <p>ii) Imitable Violence</p> <p>Due consideration must be given to the fact that violence portrayed visually may be imitated in real life. The presentation of dangerous behavior, which is easily imitated, must be justified and, ideally, excluded.</p> <p>iii) Sexual Violence</p> <p>Graphic representations of sexual violence, such as rape or attempted rape or other non-consensual sex, or violent sexual behavior are not allowed.</p> <p>iv) Violence and Young, Vulnerable Audiences</p> <p>The susceptibility of younger audiences, particularly those impressionable minds, must be considered.</p> <p>5.0 — Menacing Content</p> <p>5.1 Content that causes annoyance, threatens harm or evil, encourages or</p>	
--	---	--

	<p>or incites crime, or leads to public disorder is considered menacing and is prohibited.</p> <p>5.2 Hate propaganda, which advocates or promotes genocide or hatred against an identifiable group, may not be portrayed. Such material is considered menacing in nature and is not permitted.</p> <p>5.3 Information which may be a threat to national security or public health and safety also is not to be presented.</p> <p><i>Illustration</i></p> <ul style="list-style-type: none"> <i>i) Making available instructions and guidance on bomb-making, illegal drug production, or counterfeit products;</i> <i>ii) Disseminating false information with regards to outbreak of racial disturbances in a specific part of the country;</i> <i>iii) Circulating information and statements with regards to possible terrorist attacks;</i> <i>iv) Circulating or making available information with regards to the outbreak of a deadly or contagious diseases.</i> 	

	<p>6.0 — Bad Language</p> <p>6.1 Bad language, including expletives and profanity, is offensive to many people. The use of crude words and derogatory terms is most likely to cause offense, especially if the language is contrary to audience expectation. Bad language includes the following:</p> <p>i) Offensive Language The use of disparaging or abusive words which is calculated to offend an individual or a group of persons is not permitted.</p> <p>ii) Crude References Words, in any language commonly used in Malaysia, which are considered obscene or profane are prohibited, including crude references to sexual intercourse and sexual organs. It is, however, permissible to use such words in the context of their ordinary meaning and not when intended as crude language.</p> <p>iii) Hate Speech Hate speech refers to any portrayal (words, speech, or pictures), which denigrates, defames, or otherwise devalues</p>	
--	--	--

	<p>a person or group on the basis of race, ethnicity, religion, nationality, gender, sexual orientation, or disability and is prohibited. In particular:</p> <p><i>Descriptions of any of these groups or their members involving the use of strong language, crude language, explicit sexual references, or obscene gestures are considered hate speech.</i></p> <p>iv) Violence</p> <p>Where the portrayal of violence is permitted with appropriate editorial discretion as in news reporting, discussion or analysis, and in the context of recognized sports events, care must be taken to consider the use of explicit or graphic language related to stories of destruction, accidents, or sexual violence, which could be disturbing for general viewing.</p> <p>7.0 — False Content</p> <p>7.1 Content which contains false material and is likely to mislead, due among others to incomplete information, is to be avoided. Content providers must observe measures outlined in specific parts of this Code to limit the likelihood of perpetuating untruths via the communication of false content.</p>
--	---

<p>Scope of Obligations / Responsibilities</p>	<p>Burden on ISPs to use best efforts to ensure that prohibited material is not broadcast via the Internet to users in Singapore.</p>	<p>7.2 Content is false where, prior to communications, reasonable measures to verify its truth have not been adopted or taken. 7.3 Content which is false is expressly prohibited except in any of the following circumstances: (a) satire and parody; (b) where it is clear to an ordinary user that the content is fiction. 7.4 Code Subjects must take all necessary steps outlined in the specific parts of this Code to limit the likelihood of provision of false Content.</p>	
		<p>To take down if aware, but Code subject possess a degree of immunity based on the concept of an “innocent carrier”. There is a burden on users to exercise caution. The ultimate responsibility for content lies with content creators and providers.</p>	<p>1. The primary focus is on controlling children’s access to content. (a) Accounts for Minors ISPs cannot provide access accounts, or Internet Content Hosts cannot provide subscription accounts to persons below 18 years of age, unless parental or guardian’s consent is obtained. (“Reasonable steps” are required, and these are identified in the code, albeit non-exhaustively.)</p>

<p>(b) Unsuitable Content for Children ISPs and ICHs who encourage content providers to use appropriate labeling system in respect of content likely to be considered unsuitable for children although such content is not prohibited or potentially prohibited content, including their responsibilities. This is satisfied by a link to the ABA.</p> <p>ISPs and ICHs must provide users with information (via a link to the ABA) about supervising and controlling children's access to Internet content.</p>			
<p>2. Supervision of others by ISPs and ICHs</p> <p>(a) Monitoring other Content Providers Once ISPs or ICHs are aware that an ICH (or a second ICH) is hosting prohibited content in Australia, they must advise the ICH about the fact and the existence of the prohibited content.</p> <p>(b) Duty to Inform ISPs and ICHs must inform subscribers that placing content on the Net may entail legal responsibilities. The manner of informing such people is a notice on the</p>			

<p>Power of regulator</p>	<p>Notify IASPs to bar access to specified sites and deny access to sites notified to them by the Authority as containing prohibited material.</p>	<p>The Malaysian Communications and Multimedia Commission has no authority to notify IASPs about particular sites because it amounts to censoring the Internet and is prohibited by section 3(3) of the Communications and Multimedia Act. However, the provision of content which is offensive, obscene, false, and menacing is a criminal offence under the Communications and Multimedia Act.</p>	<p>ISP home page or a prominent Web page or, in the case of an ICH, via a relevant term in the hosting contract or in the acceptable use policy.</p> <p>3. Complaint Process</p> <p>ISPs must provide a complaint process for unsolicited commercial emails. ICHs must provide a link to tell users about the complaint process.</p>
			<p>a) Notify ISP of prohibited or potentially prohibited content and, once notified, the ISP must provide for use a filter [technology] as prescribed in the code.</p> <p>(b) Notify an ICH if it is hosting prohibited or potentially prohibited content in Australia, upon which the ICH is to remove it; if it is R-rated content, the ICH must apply a restricted access system and take other action as may be prescribed. Furthermore, it must inform its customer that it is in breach of customer service conditions.</p>

(f) Spamming*(i) In General*

The Internet has experienced phenomenal growth in terms of number of users — 687-million Internet users⁸² and more than 240-million people who have email accounts with free email providers such as Hotmail and Yahoo!.

The large number of users is an incentive for businesses which wish to market their products. In addition to this “pull” factor, the ease by which such marketing can be done, and most importantly its low cost, make it a compelling case for businesses to undertake direct marketing using the Internet globally. Thus, such businesses use the simplest form of communication on the Internet — email — to send their marketing materials to potential buyers and customers.

(ii) What Is Spam?

In General There is much debate⁸³ over the origins of the term “spam” in its use in respect of the Internet. Spam has come to be associated with the following:

1. “Electronic junk mail or junk newsgroup postings”;⁸⁴
2. “Unsolicited email”;⁸⁵
3. “Unsolicited commercial email (UCE) or unsolicited bulk email (UBE)”;⁸⁶
and
4. Any email which the recipient did not ask for, but receives from senders whom the recipient does not know, but who wish to sell something to the recipient. It is usual for there to be many recipients of the same email.⁸⁷

An industry definition of spam is an “unsolicited, commercial e-mail, usually sent in bulk”.⁸⁸ Interestingly, spam does not mean “ads”. It does not mean “abuse”. It does not mean “posts whose content I object to”.⁸⁹ This perspective identifies spam as a message which is repeatedly posted.

82 International Telecommunication Union Statistics as at 2003, available at http://www.itu.int/ITU-2D/ict/statistics/at_glance/Internet03.pdf, accessed on 22 January 2005.

83 *Webopedia*, at <http://www.webopedia.com/TERM/s/spam.html>, accessed on 22 January 2005.

84 *Webopedia*, at <http://www.webopedia.com/TERM/s/spam.html>, accessed on 22 January 2005.

85 *Webopedia*, at <http://www.webopedia.com/TERM/s/spam.html>, accessed on 22 January 2005.

86 Indiana University Knowledge Base, at <http://kb.indiana.edu/data/afne.html>, accessed on 22 January 2005.

87 See <http://email.about.com/library/weekly/aa090197a.htm>, accessed on 22 January 2005.

88 Emigh, “Stomping Out Spam: The Spam Series 1”, at <http://www.esecurityplanet.com/trends/article.php/2107121>, accessed on 22 January 2005.

89 Southwick and Falk, “The Net Abuse FAQ”, at <http://www.cybernothing.org/faqs/net-abuse-faq.html>, accessed on 22 January 2005, and cited in Khong, “Spam Law for the Internet”, *Journal of Information, Law, and Technology*, at <http://elj.warwick.ac.uk/jilt/01-3/khong.html#Southwick>, accessed on 22 January 2005.

Malaysia The Malaysian Communications and Multimedia Commission proposed the following definition of spam:

Spam may be elucidated as the activity of sending unsolicited messages (for example Internet emails or mobile short messages).⁹⁰

The definition covers both the Internet and short messaging services using mobile telephones.

However, in Malaysia, there is no legislative prohibition on the sending of spam, other than a statutory prohibition against providing “content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten, or harass any person”.⁹¹

United States The United States CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing) identifies spam as a “commercial electronic mail message” and which is defined in section 3 as “mean[ing] any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)”.

Australia In Australia, the definition is set out in the Spam Act 2003,⁹² where spam is identified as “unsolicited commercial electronic messages” and covers both email as well as short message services provided by mobile phone service providers. Furthermore, section 6 of the Australian Spam Act 2003 defines commercial electronic messages as:

. . . an electronic message, where, having regard to:

- (a) the content of the message; and
- (b) the way in which the message is presented; and
- (c) the content that can be located using the links, telephone numbers or contact information (if any) set out in the message;

it would be concluded that the purpose, or one of the purposes, of the message is:

- (d) to offer to supply goods or services; or
- (e) to advertise or promote goods or services; or
- (f) to advertise or promote a supplier, or prospective supplier, of goods or services; or
- (g) to offer to supply land or an interest in land; or
- (h) to advertise or promote land or an interest in land; or

90 See <http://www.mcmc.gov.my/Admin/FactsAndFigures/Paper/PC-SPAM-04.pdf>, accessed on 22 January 2005.

91 Communications and Multimedia Act 1998, section 211.

92 See <http://scaleplus.law.gov.au/html/comact/11/6735/top.htm>.

- (i) to advertise or promote a supplier, or prospective supplier, of land or an interest in land; or
- (j) to offer to provide a business opportunity or investment opportunity; or
- (k) to advertise or promote a business opportunity or investment opportunity; or
- (l) to advertise or promote a provider, or prospective provider, of a business opportunity or investment opportunity; or
- (m) to assist or enable a person, by a deception, to dishonestly obtain property belonging to another person; or
- (n) to assist or enable a person, by a deception, to dishonestly obtain a financial advantage from another person; or
- (o) to assist or enable a person to dishonestly obtain a gain from another person; or
- (p) a purpose specified in the regulations.

South Africa South Africa, which introduced the Electronic Communications and Transaction Act 2002,⁹³ provides in section 45 that unsolicited commercial messages can only be sent to persons who have subscribed for them.

It specifies that the sender must give the recipient an option to unsubscribe from the mailing list, and the sender must identify the source from which the sender obtained the recipient's personal information. If this is not provided, the sender commits an offence. It is interesting that there is no definition of unsolicited commercial messages in the Electronic Communications and Transaction Act 2002.

Summary The table below summarizes the legal definition of spam.

	Malaysia	United States	Australia	South Africa
What is spam	The activity of sending unsolicited messages	Commercial electronic mail messages	Unsolicited commercial electronic messages	Unsolicited commercial messages

(iii) Characteristics of Spamming

From the various regulatory definitions of spam, there are certain characteristics attributable to spam, namely:

1. It is unsolicited by the recipient;
2. The same message is sent in bulk; and

⁹³ See <http://www.gov.za/gazette/acts/2002/a25-02.pdf>, accessed on 30 January 2005.

3. The recipient's address is obtained not from the recipient voluntarily and the recipient did not knowingly provide it.

Spam, by definition, is not concerned with the content of the messages, rather with the fact that a message was sent to many people. Consequently, the focus by some regulatory authorities on the content of spam, as opposed to the activity of sending the same message to many people, may be misdirected.

(iv) Why Is Spam of Concern?

The easy way by which the problem of junk mail is resolved in the physical world may not necessarily extend to the online world. When an email is sent, it consumes network resources, it costs the recipient money (in connection time to download the messages), and possibly loss of income (if legitimate emails are "bounced back" because the mail box is full).

The Australian Communications Authority states that spam is a problem because:

... [s]pam now makes up more than 60 per cent of all email traffic, and is having a significantly negative effect on both businesses and individuals. The billions of unwanted email messages circulating across the Internet disrupt email delivery, clog up computer systems, reduce productivity, waste time, raise the cost of Internet access fees, irritate users, and erode their confidence in using email. Many spam messages also contain material that is offensive or fraudulent, and spam is sometimes used to spread computer viruses.⁹⁴

A recent Working Group on Internet Governance⁹⁵ working paper on spam⁹⁶ states that:

... spam [was found to raise] different kinds of governance issues [such as:]

Spam can be annoying or offensive to consumers and imposes various additional costs, especially on individuals who access the network through pay-per-use or low bandwidth connections, thereby hampering the development of Internet access.

Spam imposes significant costs on organizations in the private, public and not-for-profit sectors, whose employees may spend substantial amounts of work time sorting through email messages to determine which are legitimately related to their work, and in deleting the rest.

Spam also imposes significant costs on Internet Service Providers and other network operators, since it requires investment in a range of tools that are needed to counter spam, including anti-spam technologies (e.g., filtering

94 See [http://Internet.aca.gov.au/Australian Communications AuthorityINTER3997752:STANDARD:731001197:pp=DIR2_12,pc=PC_1793,#problem](http://Internet.aca.gov.au/Australian%20Communications%20AuthorityINTER3997752:STANDARD:731001197:pp=DIR2_12,pc=PC_1793,#problem), accessed on 22 January 2005.

95 See <http://www.wgig.org/index.html>.

96 "Draft Working Group on Internet Governance Issues Paper on Spam", at <http://www.wgig.org/docs/WP-Spam.pdf>, accessed on 5 February 2005.

technologies), server and transmission capacity, human resources, and anti-spam information sharing, cooperation, and regulatory structures. This is a particularly important concern in developing countries.

Spam provides a cover for spreading viruses, worms, trojans, spyware, etc., which typically are sent as attachments to e-mail messages, which may cause harm to individual consumers and user organizations, as well as to network operators and service providers.

As well causing inconvenience and reducing the utility of the Internet for consumers and users, spam may violate national law, e.g., if it constitutes an invasion of privacy (e.g., spyware), leads to malicious attacks on their personal property (e.g., viruses), or results in the unauthorized use of this property, possibly for illegal purposes (e.g., zombie networks).

Spam also provides a cover for other forms of cyber crime, such as identity theft through “phishing” and other forms of online fraud, which cause harm to individual consumers and impose costs on corporations (e.g., in the financial services sector), and government agencies (e.g., that issue licenses).

For all these reasons, there is growing concern that, if spam is not controlled, it will constitute a serious impediment to Internet use for consumers and users, and a significant roadblock to the development of e-commerce, e-government, and online public services, thereby reducing the “social value” of the Internet. This is of particular concern to government policymakers in developed and developing countries, although the specific concerns it presents may vary according to the level of technological and economic development within a country.

At the same time, it also is generally recognized that commercial e-mail, which does not raise the kinds of issues listed above, has a legitimate place in the development of e-commerce and the economy and that measures to control spam must distinguish between acceptable and unacceptable commercial e-mail practices. This is of particular concern to businesses in both developed and developing countries, which see the new commercial opportunities made possible by e-mail and want to avoid being subjected to overly onerous laws and regulations.

The United States CAN_SPAM Act exemplifies the United States concern with spamming and spam messages, as follows:

Section 2. Congressional Findings and Policy.

(a) Findings. — The Congress finds the following:

(1) Electronic mail has become an extremely important and popular means of communication, relied on by millions of Americans on a daily basis for personal and commercial purposes. Its low cost and global reach make it extremely convenient and efficient, and offer unique opportunities for the development and growth of frictionless commerce.

(2) The convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail. Unsolicited commercial electronic mail is currently estimated to account for over half of all electronic mail traffic, up from an estimated seven percent in 2001, and the volume continues to rise. Most of these messages are fraudulent or deceptive in one or more respects.

(3) The receipt of unsolicited commercial electronic mail may result in costs to recipients who cannot refuse to accept such mail and who incur costs for the storage of such mail, or for the time spent accessing, reviewing, and discarding such mail, or for both.

(4) The receipt of a large number of unwanted messages also decreases the convenience of electronic mail and creates a risk that wanted electronic mail messages, both commercial and non-commercial, will be lost, overlooked, or discarded amidst the larger volume of unwanted messages, thus reducing the reliability and usefulness of electronic mail to the recipient.

(5) Some commercial electronic mail contains material that many recipients may consider vulgar or pornographic in nature.

(6) The growth in unsolicited commercial electronic mail imposes significant monetary costs on providers of Internet access services, businesses, and educational and non-profit institutions that carry and receive such mail, as there is a finite volume of mail that such providers, businesses, and institutions can handle without further investment in infrastructure.

(7) Many senders of unsolicited commercial electronic mail purposefully disguise the source of such mail.

(8) Many senders of unsolicited commercial electronic mail purposefully include misleading information in the messages' subject lines to induce the recipients to view the messages.

(9) While some senders of commercial electronic mail messages provide simple and reliable ways for recipients to reject (or "opt-out" of) receipt of commercial electronic mail from such senders in the future, other senders provide no such "opt-out" mechanism, or refuse to honor the requests of recipients not to receive electronic mail from such senders in the future, or both.

(10) Many senders of bulk unsolicited commercial electronic mail use computer programs to gather large numbers of electronic mail addresses on an automated basis from Internet websites or online services where users must post their addresses to make full use of the website or service.

...

(b) Congressional Determination of Public Policy — On the basis of the findings in subsection (a), the Congress determines that:

- (1) there is a substantial government interest in regulation of commercial electronic mail on a nationwide basis;
- (2) senders of commercial electronic mail should not mislead recipients as to the source or content of such mail; and
- (3) recipients of commercial electronic mail have a right to decline to receive additional commercial electronic mail from the same source.

There are three different perspectives when considering spam, namely:

1. End-users (ultimate recipients);
2. Network administrators; and
3. Third, parties (innocent bystanders).⁹⁷

The table below summarizes their respective concerns, and it identifies the possible costs.

Perspective of	Reasons for Concern	Possible Costs
End-users (recipients)	Spam fills mail boxes and hinders legitimate email in getting through. The user installs spam filters to mitigate the concern, but this has other effects.	Costs include those for connection, purchase of anti-spam filters, and loss of business if legitimate email is lost.
Network administrators (intermediaries)	Khong points out that “a deluge of emails to a mail server may severely cripple the network of an email service provider”. ⁹⁸	Khong indicates that “spam increases the cost of support by 15 per cent to 20 per cent, administration by 20 per cent, incoming delivery by 10 per cent, disk space by 15 per cent, and overall equipment cost of 10 per cent to 15 per cent”. ⁹⁹ The intermediary suffers further loss of reputation and the burden of having to deal with customer complaints.

97 Khong, “Spam Law and Internet”, 2001 (3) *Journal of Information, Law, and Technology*, available at <http://elj.warwick.ac.uk/jilt/01-3/khong.html#2>, accessed on 22 January 2005.

98 Khong, “Spam Law and Internet”, 2001 (3) *Journal of Information, Law, and Technology*, available at <http://elj.warwick.ac.uk/jilt/01-3/khong.html#2>, accessed on 22 January 2005.

99 Khong, “Spam Law and Internet”, 2001 (3) *Journal of Information, Law, and Technology*, available at <http://elj.warwick.ac.uk/jilt/01-3/khong.html#2>, accessed on 22 January 2005.

Third parties (innocent bystanders)	Their email addresses are hijacked by spammers without their knowledge or consent.	They receive angry emails, and the deluge of responses may have an impact on third-party systems.
Spammers (the sender)	Spammers are not concerned and view the sending of bulk email as a cost-effective way to market their products. Preparing and sending the email costs almost nothing.	

In the Hong Kong case of *Goetz Trading Limited v. Pacific Supernet Limited*,¹⁰⁰ the judge found that:

... spam could have come from the plaintiff's server in four ways. The first is "open relay", whereby spam from an outside transmitter is relayed by the server; it can be stopped by the use of an anti-spam program which will prevent the spam from coming into the server in the first place. The second is hacking, whereby an outside spammer obtains control of the server. The parties have agreed that neither of these in fact applied. The third way is wrongful use by someone within the plaintiff's network of the service to transmit the spam through the plaintiff's e-mail server. The fourth way is "IP forgery", i.e., the sending of messages by a third party which appear to come from a particular IP address when in fact they do not.

The Goetz case nicely summarizes how third parties may be innocent bystanders and be affected by the activities of spammers, including the costs incurred. Furthermore, the open relay system that is used in Internet email may be used by spammers to send emails with illegal content or to perpetrate a fraud.

Unlike junk postal mail, where the costs was borne by the sender (i.e., the costs of printing, paper, postage, and envelopes) and the recipient does not incur any costs, the situation with spam is the total reversal, i.e., senders incur no costs and recipients and intermediaries incur most of the costs. The reversal of the cost burden has not only made spamming a viable advertising option for businesses, but has become the subject of governmental action.

Spamming has become a method by which illegitimate activities are undertaken, such as bank fraud, spoofing (where one uses a legitimate email account but it is

100 *Goetz Trading Limited v. Pacific Supernet Limited* (2002), available at <http://www.hklii.org/cgi-hklii/disp.pl/hk/jud/en/hkdc/2004/DCCJ005427%5f2002.html?query=%22spam%22>, accessed on 30 January 2005.

not actually used), or the famous Nigerian scams. Essentially, spamming can be divided into two groups (from the sender's perspective), namely:

1. Spamming as a form of direct marketing by legitimate businesses (commercial); and
2. Spamming as a form of perpetrating fraud or some other scam (criminal).

(v) Regulatory Approach

In General The nature of spam as unsolicited commercial messages or unsolicited bulk messages has meant that the focus of most regulatory approaches tries to balance two competing philosophies, i.e., the right of individual privacy and the right of businesses to market and promote their goods and services.

As a result of these competing philosophies, regulatory frameworks have been designed to achieve a balance between the two interests. However, the regulatory approach starts from the basis that spamming is a legitimate business activity (akin to junk mail). From this perspective, the solutions designed in regulatory frameworks have become known as the "opt-in" approach and the "opt-out" approach. These approaches are, however, unsuitable for non-commercial spam (or spam which is a step towards perpetrating a fraud).

Opt-In Approach The opt-in approach is based on the primacy of the individual's right to privacy. Based on this primary right, regulation prohibits absolutely the sending of any commercial message to any person, whether such message is an email, SMS, or MMS. The only exception to the absolute prohibition is that before such emails are sent, the prospective recipients must have expressly chosen or consented to receive such emails.

If no such choice or consent is made (i.e., opt-in), the sender cannot send any messages. Express consent must be provided unless the sender and recipient have an existing customer relationship. The European Union adds that senders must clearly indicate the use of cookies or other tracking devices (including spyware)¹⁰¹ so that recipients can make informed decisions.

Opt-Out Approach The opt-out approach is based on the rights of a business to promote its activity, and it may use all available means to do so. However, once individual recipients have informed the business that they do not wish to receive any such messages, the business must remove their contact details from its databases.

Hence, this approach requires businesses to specifically state that recipients have the right to "unsubscribe" or be removed from the mailing list of the business enterprise, i.e., "opt-out".

101 See <http://www.itu.int/osg/spu/spam/law.html#countries>, accessed on 29 January 2005.

Combined Approach Countries such as Finland have adopted a unique approach, whereby spamming individuals are subject to an opt-in requirement, while spamming corporations are subject to an opt-out requirement.

While this may enable marketing materials to be sent to corporations by legitimate spammers, it also may have a far greater effect if such spamming can critically affect the corporate network. This duality approach does not take into account the costs of spamming to corporate network administrators and the possible loss of legitimate business opportunities.

Opt-In and Opt-Out Problems The problem with either the opt-in or opt-out approaches is that, while legitimate business enterprises will comply with the legislative environment, it is those enterprises which use spam for illegal activities, such as fraud or to spread viruses, where there is greater concern. This is the duality of spamming.

Australia addresses this duality of spamming by prohibiting the sending of unsolicited commercial messages (as prescribed in section 16 of the Spam Act 2003)¹⁰² and by defining the phrase “unsolicited commercial messages” widely to encompass the assisting or enabling a person, by a deception, to dishonestly obtain property belonging to another person or to take financial advantage of another person. By comparison, the United States CAN-SPAM Act provides that:

1. False or misleading header information in emails is banned so as to be able to accurately identify the person who initiated the email;

102 Section 16 of the Spam Act 2003 provides: “(1) A person may not send, or cause to be sent, a commercial electronic message that: (a) has an Australian link; and (b) is not a designated commercial electronic message. (2) Subsection (1) does not apply if the relevant electronic account-holder consented to the sending of the message. (3) Subsection (1) does not apply if the person: (a) did not know; and (b) could not, with reasonable diligence, have ascertained that the message had an Australian link. (4) Subsection (1) does not apply if the person sent the message, or caused the message to be sent, by mistake. (5) A person who wishes to rely on subsection (2), (3) or (4) bears an evidential burden in relation to that matter. (6) A person may not send, or cause to be sent, a commercial electronic message to a non-existent electronic address if: (a) the person did not have reason to believe that the electronic address existed; and (b) the electronic message: (i) has an Australian link; and (ii) is not a designated commercial electronic message. (7) Subsection (6) does not apply if the person: (a) did not know; and (b) could not, with reasonable diligence, have ascertained; that the message had an Australian link. (8) A person who wishes to rely on subsection (7) bears an evidential burden in relation to that matter. (9) A person may not: (a) aid, abet, counsel or procure a contravention of subsection (1) or (6); or (b) induce, whether by threats or promises or otherwise, a contravention of subsection (1) or (6); or (c) be in any way, directly or indirectly, knowingly concerned in, or party to, a contravention of subsection (1) or (6); or (d) conspire with others to effect a contravention of subsection (1) or (6). (10) A person does not contravene subsection (9) merely because the person supplies a carriage service that enables an electronic message to be sent. (11) Subsections (1), (6), and (9) are civil penalty provisions”.

2. The subject line cannot mislead the recipient about its contents or subject matter;
3. The email must enable recipients to opt-out from receiving future emails;¹⁰³
4. One entity may not assist another to send email to that address; nor can another entity send email on the original spammer's behalf to that address;
5. Selling or transferring the email addresses of people who choose not to receive spam email is illegal; and
6. Commercial email must be identified as an advertisement and include the sender's valid physical postal address.¹⁰⁴

The United States approach is to prescribe what must be stated in emails and, as most spammers of illegal or fraudulent activities do not specify genuine headers, these are subject to the general prohibition.

(vi) Jurisdictional Issues

Most spam that is received originates outside the recipient's home country. This raises the difficult issue of jurisdiction. Because spamming is an activity that can commence in one country and affect individuals in another country, the jurisdictional difficulties in enforcing anti-spam laws become acute. Traditional public international law rules do not allow penal statutes to be enforced in other countries, thus rendering the usefulness of anti-spam legislation nugatory. Spammers will simply locate to a "friendly jurisdiction" to undertake their activities or, worse still, they may use the many cyber cafes to launch their emails. The latter renders their identification almost untraceable, as they are only in the cyber cafe for a short while.

To permit the enforcement of anti-spam laws of one country against individuals of another country would be to go against the fundamental principle of national sovereignty. Hence, cross-jurisdictional issues are a major concern which may need international cooperation in the form of a treaty or multi-lateral arrangement, such as the trilateral memorandum¹⁰⁵ entered into by the United States, Australia, and the United Kingdom on 2 July 2004.

103 The opt-out method requires that a valid return email address or another Internet-based response mechanism that allows a recipient to ask that future email messages not be sent, which request must be honored. After receipt of an opt-out request, the sender has 10 business days to stop sending email to the requestor's email address.

104 See detail summary at <http://www.ftc.gov/bcp/online/pubs/buspubs/canspam.htm>, accessed on 13 February 2005.

105 See <http://www.ftc.gov/os/2004/07/040630spammoutext.pdf>, accessed on 30 January 2005.

This memorandum of understanding on mutual enforcement assistance in commercial email matters provides for cooperation among Australia, the United Kingdom, and the United States by:

1. Sharing of evidence to facilitate enforcement of spam laws, coordination of investigations, and education and research; and
2. Informing each other as to developments in their respective countries.

Such cooperative approaches do help in mitigating the activities of spammers since these countries have formalized (albeit in a non-legally binding arrangement) their mutual cooperation and assistance. This approach is an example of what countries can do to militate against the activities of spammers, and overcome the jurisdictional issues.

(vii) Comparison of Anti-Spam Laws

The International Telecommunication Union, as at 1 January 2005,¹⁰⁶ has produced a list of legislative frameworks affecting the issue of spam.

Argentina In 2001, anti-spam legislation (*Anteproyecto de Ley de Regulación de las Comunicaciones Publicitarias por Correo Electrónico*) was proposed to combat spam. In November 2003, the Federal Court heard its first spam case. The judge issued an injunction relying on the Personal Data Protection Act of 2000, particularly its article 25.

Under the injunction, the spammer on trial was ordered to stop sending e-mail after an opt-out was requested. It also was ordered that the spammer could not give the addresses to a third party under the Act.

In 2004, the national legislature introduced a new Bill allowing the government to block the Internet Protocols and cancel domain names of spammers. The Bill proposes an opt-out system (*Proyecto de ley para regular el Spam en Argentina*). The legal regime relevant to regulation of spam includes:

1. The Constitution, section 43;
2. Decree Number 995 of 2000; and
3. Decree Number 1558 of 2001.

Australia The Spam Act 2003 and the Spam (Consequential Amendments) Act 2003 were passed by Parliament in 2003. The two Acts came into effect on 10 April 2004 and are due for review within two years.

Legislation will be administered by the Australian Communications Authority. In addition to a set of industry codes and standards, under the Spam Act,

¹⁰⁶ The online version is available at <http://www.itu.int/spam/>.

the Australian Communications Authority has the ability to pursue a number of enforcement options.

As part of the changes, the National Office for the Information Economy becomes the Australian Government Information Management Office, with some functions transferring to the Department of Communications, Information Technology, and the Arts. Australia uses an opt-in approach. The legal regime relevant to regulation of spam includes:

1. The Spam Act 2003;
2. The Spam (Consequential Amendments) Act 2003; and
3. The Spam Regulations 2004.

Canada The Privacy Commissioner of Canada is an Officer of Parliament who reports directly to the House of Commons and the Senate as an advocate for the privacy rights of Canadians. In May 2004, the Economic Development Agency of Canada for the Regions of Quebec launched an Anti-Spam Action Plan and announced the creation of a ministerial task with the Electronic Commerce Branch of Industry Canada to combat spam. The legal regime relevant to regulation of spam includes:

1. The Privacy Acts of 1980, 1981, 1982, and 1983; and
2. The Personal Information Protection and Electronic Documents Act, section 11.

European Union The European Union uses an opt-in approach. The legal regime relevant to regulation of spam includes:

1. The E-Privacy Directive, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector;
2. The E-Commerce Directive, Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market;
3. The Telecommunications Privacy Directive, Directive 97/66/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (repealed and replaced by Directive 2002/58/EC);
4. The Distance Contracts Directive, Directive 97/7/EC on the Protection of Consumers in Respect of Distance Contracts; and
5. The Data Protection Directive, Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

France The competent authority is the *Commission Nationale de l'Informatique et des Libertés*, an independent administrative agency which enforces the Data Protection Act of 1978 and other related laws. In July 2002, it created a Spam Mailbox to combat Spam. In July 2003, a Contact Group was established by the government within the *Direction du Développement des Médias* to fight against spam. France employs the opt-in approach. The legal regime relevant to regulation of spam includes:

1. Law Number 78-17 of 6 January 1978;
2. Decision Number 496 of 2004; and
3. Deliberation Number 2-075 of 24 October 2002.

Japan In April 2002, the Japanese government passed the Law on Regulation of Transmission of Specified Electronic Mail. This law addresses “specified electronic mail”, which is defined as e-mail for advertisement purposes sent to users who have not opted in for the service.

The Law controls spam disseminated by anyone under the jurisdiction of the Ministry of Public Management, Home, Affairs, Posts and Telecommunications (MPHPT), which includes the entire country and the solitary islands. In July 2002, the MPHPT established the Japan Data Communications Association to determine appropriateness of sending specified e-mail messages. Japan uses the opt-out approach.

Ireland The Irish government has signed a law outlawing spam. The law gives effect to new EU regulations banning the sending of unsolicited e-mails or text messages to the general public.

Ireland passed the self-titled European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003. Regulation 13 relates to spam, and it provides for mandatory opt-in for unsolicited spamming.

Regulation 19 grants enforcement powers to the Commission for Communications Regulation (the “Regulator” in the regulations). The Regulator, in consultation with the Data Protection Commissioner, also may specify the form and any other requirements regarding the obtaining, recording, and rescinding of consent of subscribers for the purposes of these Regulations. The punishment granted to the Commission is a warning. The legal regime relevant to regulation of spam includes:

1. The Data Protection Act, 1988; and
2. Statutory Instrument Number 535 of 2003, European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003.

Italy Italy has enacted an anti-spam law that makes spamming a criminal offense punishable by up to three years' imprisonment. The Italian Data Protection Authority is an independent agency created to ensure personal data protection and deal with Spam problems. Italy employs the opt-in approach. The legal regime relevant to regulation of spam includes:

1. Decree-Law Number 675/1996 on privacy protection;
2. Decree-Law Number 171/1998 on telecommunications privacy protection;
3. Decree-Law Number 185/1999 on customer protection in respect of long-distance contracts; and
4. Decree-Law Number 196/2003, the Personal Data Protection Code.

New Zealand The Office of the Privacy Commissioner is an independent Crown entity established by the Privacy Act. The government has issued a discussion paper to outlaw unwanted Spam.

The Privacy Commissioner's principal powers and functions include promoting the objects of the Privacy Act 1993, monitoring proposed legislation and government policies, dealing with complaints at first instance, approving and issuing codes of practice and authorizing special exemptions from the information privacy principles, and reviewing public-sector information-matching programs.

Republic of Korea The Korea Spam Response Center was constituted within the Korea Information Security Agency, which is an agency of the Ministry of Information and Communication, to deal with problems regarding spam. Korea uses an opt-out approach. The legal regime relevant to regulation of spam includes:

1. The Anti-Spam Regulations; and
2. The Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001 and its 2002 Revisions.

United Kingdom The United Kingdom Department for Trade and Industry implemented the Privacy and Electronic Communications (EC Directive) Regulation, a new anti-spam regulation based on EU Directive 58/2002, which came into force on 11 December 2003.

Enforcement is the responsibility of the Information Commissioner; however, considering that several issues relating to spam concern also consumer protection and trade, the Office of Fair Trading also is active in this field, in particular on the subject of online scams. The United

Kingdom uses the opt-in approach. The legal regime relevant to regulation of spam includes:

1. Statutory Instrument 2003 Number 2426, the Privacy and Electronic Communications (EC Directive) Regulations 2003;
2. The Data Protection Act 1998;
3. The Electronic Commerce (EC Directive) Regulations 2002;
4. The Control of Misleading Advertisements Regulations 1988 (amended 2000);
5. The Consumer Protection (Distance Selling) Regulations 2000;
6. The Ecommerce Regulations 2002; and
7. The Unfair Terms in Consumer Contracts Regulations (amended 2001).

United States On 1 January 2004, the CAN-SPAM Act came into effect in the United States. The law imposes specific requirements on senders of commercial e-mail and places enforcement in the hands of the Federal Trade Commission and State Attorneys General.

The Federal Trade Commission¹⁰⁷ summarizes the anti-spam law as follows:

It bans false or misleading header information. Your emails “From”, “To”, and routing information — including the originating domain name and email address — must be accurate and identify the person who initiated the email.

It prohibits deceptive subject lines. The subject line cannot mislead the recipient about the contents or subject matter of the message.

It requires that your email give recipients an opt-out method. You must provide a return email address or another Internet-based response mechanism that allows a recipient to ask you not to send future email messages to that email address, and you must honor the requests. You may create a “menu” of choices to allow a recipient to opt out of certain types of messages, but you must include the option to end any commercial messages from the sender. Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your commercial email. When you receive an opt-out request, the law gives you 10 business days to stop sending email to the requestor’s email address. You cannot help another entity send email to that address, or have another entity send email on your behalf to that address. Finally, it’s illegal for you to sell or transfer the email addresses of people who choose not to receive your email, even in the form of a mailing list, unless

107 See <http://www.ftc.gov/bcp/online/pubs/buspubs/canspam.htm>, accessed on 13 February 2005.

you transfer the addresses so another entity can comply with the law.

It requires that commercial email be identified as an advertisement and include the sender's valid physical postal address. Your message must contain clear and conspicuous notice that the message is an advertisement or solicitation and that the recipient can opt out of receiving more commercial email from you. It also must include your valid physical postal address.

7.03 International Activities

Since the commercial expansion of the Internet in the early 1990s, there have been many activities on the international front. These range from the Model Law on E-Commerce of the United Nations International Trade Law Commission (UNCITRAL) to the Hague Conference on Private International Law. Various regional groupings, such as the Association of South East Asian Countries (ASEAN) and the Asia-Pacific Economic Cooperation (APEC), also have focused on the issues affecting e-commerce.

Agency or Grouping	Activities
UNCITRAL	UNCITRAL developed a model law in 1996 on e-commerce. ¹⁰⁸ UNCITRAL developed a model law in 2001 on electronic signatures. ¹⁰⁹
ASEAN	ASEAN developed the e-ASEAN initiative: “[which is to] facilitate the establishment of the ASEAN Information Infrastructure — the hardware and software systems needed to access, process and share information — and promote the growth of electronic commerce in the region”. ¹¹⁰ The e-ASEAN initiative requires that: “[e]lectronic commerce will be facilitated through the adoption of laws and policies based on international norms that promote trust and confidence of the general population and, in particular, those who transact business over the Internet. This task will involve the establishment of a system of mutual recognition of digital signatures; secure electronic transactions, payments and settlements; protection of intellectual property rights arising from e-commerce; measures to promote personal data protection and consumer privacy; and dispute settlement mechanisms”.

108 See <http://www.uncitral.org/en-index.htm>, accessed on 28 December 2004.

109 See <http://www.uncitral.org/en-index.htm>, accessed on 28 December 2004.

110 See <http://www.aseansec.org/7659.htm>, accessed on 29 December 2004.

APEC	The Electronic Commerce Steering Group (ECSG) was created to provide a coordinating role for APEC e-commerce activities. ¹¹¹ The ECSG is committed to promoting and facilitating the development and use of electronic commerce by creating legal, regulatory, and policy environments in the APEC region that are predictable, transparent, and consistent. In addition, the ECSG is working to promote mechanisms to increase trust and confidence of participants in electronic commerce to encourage greater use of the Internet to perform transactions. Finally, the ECSG is using information technology and electronic commerce methods to facilitate trade transactions among member economies.
ICANN	ICANN has developed gTLDs, such as .info; .firm; and .museum to enable new participants on the World Wide Web to have better choice of domain names. ¹¹² ICANN has promoted the Internationalized Domain Name to enable a domain name in a language other than English to be recognized by the Domain Name System, without causing technical difficulties for existing operations.
World Intellectual Property Organization (WIPO)	WIPO has developed a Uniform Dispute Resolution Procedure to handle disputes about domain names and trade marks. ¹¹³ WIPO2 extends the UDRP to cover situations, such as “confusingly similar domain names, geographical locations, and identifications”.
Hague Conference on Private International Law	The Hague Conference is examining the issues and concerns affecting e-commerce and designing and re-examining existing conventions to bring them in line with the requirements of the Information Society. ¹¹⁴

Most international activities are centered around the sharing of information and experiences in order for there to be developed some form of “harmonized” regulatory framework affecting the Internet through e-commerce. The rationale is that, with such harmonization, the risks of conflicts between national laws may be reduced.

Other than the work of UNCITRAL on model laws, there has been little substantive development of international cooperative arrangements on, for example, anti-spam arrangements.

111 See http://www.apecsec.org.sg/content/apec/apec_groups/som_special_task_groups/electronic_commerce.html, accessed on 29 December 2004.

112 See <http://www.icann.org/>.

113 See <http://www.icann.org/committees/JWGW2/final-report/JWGW2-final-report-part-1.pdf>.

114 See http://www.hcch.net/index_en.php?act=progress.listing&cat=9, accessed on 9 December 2004.

