

LEGAL AND REGULATORY ISSUES
IN THE
INFORMATION ECONOMY

RODOLFO NOEL S. QUIMBO

May 2003

e-ASEAN Task Force

UNDP-APDIP

PREFACE

One of the many challenges facing the countries in the Asia-Pacific today is preparing their societies and governments for globalization and the information and communication revolution. Policy-makers, business executives, NGO activists, academics, and ordinary citizens are increasingly concerned with the need to make their societies competitive in the emergent information economy.

The e-ASEAN Task Force and the UNDP Asia Pacific Development Information Programme (UNDP-APDIP) share the belief that with enabling information and communication technologies (ICTs), countries can face the challenge of the information age. With ICTs they can leap forth to higher levels of social, economic and political development. We hope that in making this leap, policy and decision-makers, planners, researchers, development practitioners, opinion-makers, and others will find this series of e-primers on the information economy, society, and polity useful.

The e-primers aim to provide readers with a clear understanding of the various terminologies, definitions, trends, and issues associated with the information age. The primers are written in simple, easy-to-understand language. They provide examples, case studies, lessons learned, and best practices that will help planners and decision makers in addressing pertinent issues and crafting policies and strategies appropriate for the information economy.

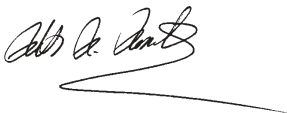
The present series of e-primers includes the following titles:

- The Information Age
- Nets, Webs and the Information Infrastructure
- e-Commerce and e-Business
- Legal and Regulatory Issues for the Information Economy
- e-Government;
- ICT and Education
- Genes, Technology and Policy: An Introduction to Biotechnology

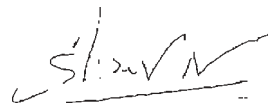
These e-primers are also available online at www.eprimers.org. and www.apdip.net.

The primers are brought to you by UNDP- APDIP, which seeks to create an ICT enabling environment through advocacy and policy reform in the Asia-Pacific region, and the e-ASEAN Task Force, an ICT for development initiative of the 10-member Association of Southeast Asian Nations. We welcome your views on new topics and issues on which the e-primers may be useful.

Finally, we thank all who have been involved with this series of e-primers-writers, researchers, peer reviewers and the production team.



Roberto R. Romulo
Chairman (2000-2002)
e-ASEAN Task Force
Manila, Philippines



Shahid Akhtar
Program Coordinator
UNDP-APDIP
Kuala Lumpur, Malaysia
www.apdip.net



TABLE OF CONTENTS

INTRODUCTION	5
I. THE RULE OF LAW AND THE INTERNET	5
What principles underpin the UNCITRAL Model Law?	5
What kind of protection does the Model Law seek to provide?	6
II. JURISDICTION AND CONFLICTS OF LAW	6
When is there conflict of laws?	6
How can jurisdiction be asserted or acquired?	7
Why is it necessary to establish laws governing jurisdiction?	8
III. LEGAL RECOGNITION OF ELECTRONIC DOCUMENTS AND ELECTRONIC SIGNATURES	8
What Asian countries have enacted e-commerce rules/laws?	9
What are the different legislative approaches toward electronic authentication?	9
IV. IDEAS, TRADE SECRETS AND INTELLECTUAL PROPERTY	12
How is information used in the Internet?	12
Is information a property right?	13
What is a trade secret?	13
What are business method patents?	15
What are the requirements for acquiring a patent?	16
What is the impact of the Internet on intellectual property?	16
How vulnerable is digital work to copyright infringement?	16
What is “copyleft”?	17
What is “GPL”?	17
What are the key issues in intellectual property rights protection in the Internet?	18
Are there international initiatives to protect intellectual property in the Internet? What Internet-specific treaties are in place?	18
Why is there a need for such initiatives?	19
V. DOMAIN NAME DISPUTES	19
What are domain names?	19
When and how can disputes over domain names arise?	20
Who controls the registration of domain names?	20
How are disputes resolved?	20
Is there an international organization that can arbitrate disputes?	21
VI. CONSUMER PRIVACY AND PROTECTION	21
What is information privacy?	22
Why protect privacy?	22
Is there such a thing as protecting privacy too much?	22
Are there other existing guidelines for data protection?	23
How can consumers be protected in electronic commerce transactions?	23
How will the OECD guidelines be used?	25
What about jurisdiction and consumer redress?	25

Should the government be involved in consumer protection and privacy? What role can the private sector play?	26
VII. CYBERCRIMES	26
Is crime possible in the Internet?	26
What are computer crimes or cybercrimes?	27
What are examples of common misdemeanors on the Internet?	27
What is the reach of cybercrimes?	28
What legal policies should be in place for the prevention, apprehension and prosecution of cybercrimes?	28
What is being done to prevent and/or prosecute cybercrimes?	28
Are there intergovernmental efforts at combating cybercrimes?	29
Are there anti-cybercrime efforts in developing countries?	30
What lies ahead in the fight against cybercrimes?	30
Who should be involved in preventing cybercrimes?	30
VIII. CENSORSHIP OR CONTENT REGULATION	31
What is content regulation?	31
How are governments approaching content regulation?	31
Do developed countries regulate internet content?	32
What are the British and American approaches to Internet censorship?	33
Which developing countries regulate Internet content?	34
Are there countries that do not regulate content?	35
Is regulating the Net similar to regulating the telephone, radio or TV?	36
Is censorship of the Internet the answer?	36
What about self-regulation?	36
How can self-regulation be made effective?	36
Is there a role for government under a regime of self-regulation?	38
What about empowering the end-users?	39
What should be considered when choosing a particular regulatory mechanism?	40
FOR FURTHER READING	41
NOTES	42
ABOUT THE AUTHOR	44
ACKNOWLEDGMENT	45



INTRODUCTION

As the Internet's sphere of influence as a communications network widens to include commercial and other exchanges, legal authorities have become more interested in asserting authority over it and the activities of those who use it. The legal questions arising from the increasingly complex world of the Internet has raised questions about the role and the rule of law in this new domain. These concerns range from the nature of self-identity to national sovereignty.

This primer aims to help developing nations define and determine their requirements for shaping appropriate e-commerce legislation, as well as corresponding regulatory and institutional frameworks that balance such complex issues as competition, privacy, consumer protection, equal access/opportunity and intellectual property.

The primer also discusses the implications for developing countries in the Asia Pacific of failure to or delay in putting in place the appropriate legal/policy and regulatory infrastructure necessary for them to participate in the information economy.

I. THE RULE OF LAW AND THE INTERNET

As technology grows by leaps and bounds, the laws have to be made more responsive to changing times. The lack of a legal framework, in many jurisdictions, to address problems of validity of electronic transactions is a significant barrier to the growth of e-commerce. For one thing, while there are laws on contracts and other business transactions, these require written, signed, or so-called "first" documents. In e-commerce transactions, however, electronic data or documents or digitally signed contracts make up the whole transaction.

To address this conundrum, the United Nations Commission on International Trade Law (UNCITRAL) has drafted a model law on e-commerce that can serve as a guide for governments when they draft their own e-commerce laws.

What principles underpin the UNCITRAL Model Law?

The UNCITRAL Model Law operates on the following principles:

1. Equivalence. Electronic communications shall be the functional equivalent of paper-based documents. Given proper standards, electronic documents can be treated and given the same value as paper documents.
2. Autonomy of contracts. Contracts may be in the form of electronic documents. However, this should not result in a change in the substantive terms and conditions of a transaction.
3. Voluntary use of the electronic communication. Parties may choose to enter into an electronic transaction or not at all. It is not mandatory.

4. Solemnity of the contract and the primacy of statutory requirements respecting formalities of contracts. The requirements for a contract to be valid and enforceable, such as notarization, remain the same.
5. Application to form rather than substance. The law should be applicable to the form rather than the substantive terms of the contract. Whatever statutory elements are required to be present must still be present, e.g., consent freely given, an object, cause or consideration.
6. Primacy of consumer protection laws. Consumer protection laws may take precedence over the provisions of the Model Law.

What kind of protection does the Model Law seek to provide?

The Model Law hopes to provide adequate legal protection for those who wish to engage in e-commerce. It ensures that electronic transactions are legally recognized and that a course of action, if necessary, is available and may be taken to enforce transactions entered into electronically.

II. JURISDICTION AND CONFLICTS OF LAW

It has been said that: "For several years, some of the most difficult legal issues on the Internet have involved one of the medium's greatest assets: its lack of boundaries. Although the free-flowing, borderless nature of cyberspace has revolutionized communication and commerce, it has also led to many lawsuits. And, as if resolving those lawsuits weren't difficult enough, it's often just as tough to determine where they should take place."¹

When is there conflict of laws?

A resident of Manila who decides to file a malpractice suit against a Manila-based doctor who had done her an injury may do so in a Manila court. The Manila courts have jurisdiction over the doctor. But if the injured person later on moves to Hanoi, and decides to file the case there, the doctor in Manila will surely object-and validly-that no Hanoi court can have personal jurisdiction over him. That's an easy case.

Consider a Web site selling pornographic materials set up in Hong Kong, hosted in the Caribbean, with a Web master residing in the Netherlands and owners who are British nationals, and broadcast throughout the world? If a complaint for pornography were to be filed, whom do you sue and where do you sue them?

For our third case, suppose A, in Hanoi, enters into a contract for the delivery of heavy machinery with B, in Yangon. If B fails to deliver the goods, where does A file the case? If A files the case for breach of contract in a Hanoi court, how does the Hanoi court acquire jurisdiction over B?

These examples show that jurisdiction is not straightforward in the Internet.



How can jurisdiction be asserted or acquired?

In the United States, there are ways by which courts are able to acquire jurisdiction over Web-based activities:

1. Gotcha. Where the court obtains jurisdiction over an out-of-State defendant, provided that when he visits the State, that person is served with a summons and a complaint (documents that give the person notice of the lawsuit). This was applied to the case of the Russian programmer sued by the publishers of e-book (Adobe). While attending a convention in Nevada, he was served with a notice and was subsequently arrested.
2. Causing an injury within the State. An Internet business can also be subject to jurisdiction for purposefully causing an injury in another state. This principle derives from a series of cases where courts of another State acquired jurisdiction over non-residents who entered the State, caused an accident and left. If someone uses the Internet to cause an injury in one State, the person causing the damage may be hauled into court in the State where the injury occurred. In cases where the connection between the activity and the injury is not clear, courts also look for evidence that the activity was "purposefully directed" at the resident of the forum State or that the person causing the injury had contacts with the State.²
3. Minimum contacts. A business or person with sufficient contacts with a particular State can be hauled to court even if he/she does not live or has a business in that State. Usually, the basis is the regularity of solicitation of business, derivation of substantial income from goods or services sold in that other State, or engaging in some other persistent course of conduct there. For example, passive Internet sites, which merely advertise but do not really offer to sell goods or services, may be said not to have achieved the required minimum contacts for courts to acquire jurisdiction over them. But with Web sites that actively offer to sell and then subsequently take orders from that State, it can be said that the minimum contacts have been satisfied for purposes of acquiring jurisdiction.
4. Effects. When one's conduct in cyberspace though emanating from another State creates or results in an injury in another, courts in the latter State can acquire jurisdiction over the offender. To illustrate: A case was filed by the DVD Copy Control Association against the creator of DeCCS³, a software that decrypts the copy-protection system in Digital Versatile Discs (DVDs) to allow ordinary CD-ROM drives to play or read DVDs. An issue in the case was whether the courts of California had jurisdiction over the person, who was a student in Indiana when the suit was filed and who later on moved to Texas. The court said that the California courts had jurisdiction, citing a 17-year-old US Supreme Court case involving defamation, because the California movie and computing industry was affected by the "effects" of the defendant's conduct in Indiana. This decision signals an expansion of personal jurisdiction in cyberspace. If other courts chart their course by California standards, any Web publisher could be hauled to court wherever its site has an effect. The attorney general of Minnesota has issued this

statement of caution: “Warning to all Internet Users and Providers: Persons outside of Minnesota who transmit information via the Internet knowing that information will be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violations of State criminal and civil laws.”

Why is it necessary to establish laws governing jurisdiction?

Due to the global nature of the Internet, it is important to establish which law governs a contract formed, perfected, or conducted online. Without an express choice of governing law, complex and difficult issues can arise. For the time being, it may be prudent for businessmen to determine which existing law and regulations apply and ensure that they are well versed in the local laws of the areas where they wish to set up their Web presence. This is to avoid unexpected liabilities that may arise as well as possible un-enforceability of contracts into which they enter. Better still, when they conduct transactions online, parties must first agree on the legal regimes under which they may operate, so that when a dispute arises, the questions of jurisdiction-what law and what courts-would have already been settled.

III. LEGAL RECOGNITION OF ELECTRONIC DOCUMENTS AND ELECTRONIC SIGNATURES

In an APEC seminar on electronic commerce in early 1998⁴, the uncertain policy environment, among other things, was cited by those from the Asia-Pacific region as a major inhibitor to the growth of electronic commerce. Of particular concern was the uncertainty resulting from the fact that laws are rooted in the paper world, requiring writing, manual signatures, and the creation and retention of original documents using paper.

Take the case of Philippine rules on formation and perfection of contracts. The Philippine Civil Code, enacted in 1950, says that a contract is a meeting of the minds between two persons whereby one person binds him/herself to the other to give something or to render some service. What happens then if one person programs a computer to make successive bids for himself, say on E-bay? As the bids for a particular item goes higher and as his or the Web site’s computer makes bids for him, as programmed, will the successive bids be binding on him, when he had did not commit what in law is referred to as contemporaneous interventions at that time? Would there be a valid meeting of the minds in this case? Assuming that the contract between E-bay and the person is valid, will it be enforceable?

Another problem is the provision called Statute of Frauds, which was adopted from United States rule. The Statute requires that certain contracts, such as an agreement for the sale of goods at a price of no less than five hundred pesos (or about \$10.00), or, *inter alia*, an agreement for the leasing for more than one year or the sale of real property, be made in writing. Unwritten contracts, though valid, cannot be enforced in courts. The Rules of Court also require paper-based documents and not electronic ones.



Clearly there is a need for a change in the legal framework that would not only allow the recognition of electronic documents and/or signatures, but also provide an assurance that the courts will allow these into evidence in cases of disputes.

What Asian countries have enacted e-commerce rules/laws?

In East Asia, Hongkong has enacted the Electronic Transactions Ordinance (effective April 7, 2000; enacted January 7, 2000.), which covers electronic and digital signatures and electronic records. This act is generally applicable to all communications. Japan's Law Concerning Electronic Signatures and Certification Authorities (effective April 1, 2001; enacted May 24, 2000.) is about digital signatures and is generally applicable to all communications. South Korea's Basic Law on Electronic Commerce also covers digital signatures and is generally applicable to all communications.

In Southeast Asia, Malaysia has its Digital Signature Bill of 1997, which became effective on October 1, 1998. Singapore's Electronic Transactions Act of 1998 (enacted June 29, 1998) covers digital and electronic signatures as well as electronic records, and is generally applicable to all communications. Similarly, Thailand's Electronic Commerce Law (which passed second and third readings in October 2000) covers electronic signatures and is generally applicable to all communications. In the Philippines the Electronic Commerce Act of 2000 (enacted June 14, 2000) encompasses electronic signatures, electronic transactions, and crimes related to e-commerce. The Electronic Transactions Order of Brunei (enacted November 2000) covers electronic contracts, as well as digital and electronic signatures.

India's Information Technology Act of 2000 (Presidential Assent June 9, 2000; passed by both Houses of the Indian Parliament May 17, 2000; implemented in October 2000) covers digital signatures and electronic records, and is generally applicable to all communications.

What are the different legislative approaches toward electronic authentication?

It is not easy to classify the existing legislation with respect to electronic authentication because of the many differences that exist. It is possible, however, to sketch the main approaches at a national and international level. Three approaches can be identified: (1) the digital signature approach; (2) the two-prong approach; and (3) the minimalist approach.⁵

What is the digital signature approach?

The digital signature approach is characterized by its focus on the digital signature technique. Legislation under this category is truly digital signature legislation because it regulates (on the basis of) digital signatures. Legislation under this approach is concerned solely with the (evidentiary) status of the digital signature. The approach has three variants:

Table 1. Three Approaches to Electronic Authentication

		Technology-neutral	Technology-specific	Examples	Definition
Digital signature approach	Technical variant	-	+	Germany	Setting digital signatures as the technical standard (no explicit legal consequences)
	Legal variant	-	+	Utah, Italy	Legal recognition of digital signatures under certain conditions
	Organizational variant	-	+	Japan, Netherlands	Requirements for Certification Authorities
Two-prong approach		+	+/-	UNCITRAL (e-signature), EU, Singapore	Legal recognition of (secure) electronic signatures under certain conditions
Minimalist approach		+	-	UNCITRAL (e-commerce), Victoria (Australia)	Equation of electronic signatures with hand-written signatures

Source: "Synthesis," Approaches in Electronic Authentication Legislation; available from <http://rechten.uvt.nl/simone/Ds-art4.htm#sy2>

1. Technical variant. The technical variant amounts to setting the digital signature technique as a technical standard by means of a legal instrument. The technical variant does not deal with legal consequences, although such consequences may implicitly follow from the use of digital signatures in accordance with the law concerned.
2. Legal variant. The legal variant of the digital signature approach is found in legislation that specifically regulates digital signatures in order to provide this technique with a legal status similar to that of the hand-written signature. The general purpose of these laws is to provide legal security for the use of digital signatures. Often legislation of this kind also includes the implementation and regulation of a Public Key Infrastructure (PKI).
3. Organizational variant. The organizational variant of the digital signature approach neither sets the digital signature as a technical standard nor provides for explicit legal recognition of the digital signature. Instead, it addresses the organisation of Certification Authorities (CAs) and the use of digital certificates in connection with digital signature applications. The aim is to promote trust and reliability in electronic transactions by ensuring that CAs are reliable and secure.⁶



What is the two-prong approach?

The second approach is called two-prong because of its hybrid way of dealing with electronic authentication. In this approach, legislators aim to make their legislation more time-resistant by addressing certain technological requirements and by leaving room for new technological developments. With this approach, legislation sets requirements for electronic authentication methods that will receive a certain minimum legal status (the minimum prong) and assigns greater legal effect to certain electronic-authentication techniques (the maximum prong). The technologies given this higher legal status are referred to as secure electronic signatures.⁷

What is the minimalist approach?

The minimalist approach does not address specific techniques and therefore intends to be technology-neutral. Legislation relates to the functions that signatures may have to fulfil in trade, and the different levels of reliability with respect to the purposes the signatures are used for. Because the main focus of this approach is on the relevant functions of signatures and the ways in which these functions may be translated into technological applications, it is also called the functionalist approach. Within the minimalist approach, the focus on functions of signatures (and writings) can be more or less explicit.⁸

Which is the better approach?

The market is constantly changing and we do not know what lies ahead with respect to technological and e-commerce developments. Thus, it might be unwise to issue detailed regulations and to determine specific business models, such as the PKI model, since their viability cannot be ascertained.

Viewed in this light, the digital signature approach is seriously flawed. Although the legislators and regulators subscribing to this approach may do so for all the right reasons (legal certainty, trustworthiness with respect to legal matters), we do not recommend the approach as such.

The same is true, but to a lesser extent, of the two-prong approach, which attempts to skirt the uncertainties by presenting an opening for new technologies aside from setting criteria for certain advanced electronic signatures which at present cover digital signatures. The approach is understandable in the sense that there seems to be a strong inclination to look for clear and trustworthy solutions, while at the same time there is a need to leave room for new solutions. Still, within the two-prong approach legislation often deals with issues and situations (e.g., CAs, liability, qualities that focus mainly on certain techniques) that have not yet been determined.

Finally, both the digital signature approach and the two-prong approach are in many instances focused too narrowly on signatures as such and not on formal requirements as a whole.

The minimalist approach taken in the UNCITRAL Model Law offers the most sensible solution to legislators wanting to tackle the problem of formal requirements in their legislation. Under this approach, legal requirements of form are generally dealt with in their entirety. Moreover, the minimalist approach allows for different functions which techniques have to fulfil under national legal systems, while creating room for new techniques and adventitious developments. Recent legislative initiatives recognise the advantages of the minimalist approach and have explicitly taken the UNCITRAL Model Law on Electronic Commerce as an example.⁹

III. IDEAS, TRADE SECRETS AND INTELLECTUAL PROPERTY

In the information economy, the possession and safeguarding of ideas are of paramount importance. Ideas themselves are commodities in the information economy. Ideas also provide their owners the competitive edge in the information age. Therefore, it is necessary that a legal regime for the protection of ideas be put in place. The lack of such a legal system will not only stunt growth but also hinder prosperity in the information economy.

How is information used in the Internet?

Today, the Internet works basically by transmitting data and information between and among networks. Often, the data and information transmitted are compiled and collected by network administrators to establish a profile of the users. This profile will then be used to tailor-fit products and services for the customers, as well as predict their buying and spending patterns. There are also cases when the data collected are sold to or shared with other companies. These are often large corporations dependent on a revenue stream that consists, at least in part, of personal consumer data. Nearly every modern company in the world today uses personal information, at some level. However, some companies depend on this revenue stream more than others. Among the most well known companies that depend almost entirely on personal information are DoubleClick, which distributes online banner ads, and credit reporting companies such as Equifax and Experian.¹⁰

It is also important to remember that trade in personal information was widespread long before the rise of the Internet. One of the first companies to discover the value of personal information was the Polk Company, founded in 1870. Polk's first product was a directory of Michigan-based businesses, organized by railroad station. The idea was to make it easier for consumers who lived near one railroad station to shop near another. In the 20th century, Polk became the country's leading purchaser of motor vehicle registration records. Polk used the records to contact car owners on behalf of the automotive industry in the event of a safety recall and made profits by combining the make and model of car with census information, and then selling this information to marketers who used it to determine lifestyle, income, and the likelihood of purchasing any given product.¹¹



Is information a property right?

Individuals instinctively regard personal information as their individual property and any use thereof without their knowledge and consent as equivalent to “identity theft.” Thus, one school of thought proposes that data or information, specifically personal information, be accorded a corresponding property right and protection so that its use may be granted appropriate monetary value.

This is fundamentally different from the legal architecture currently in place. At present, privacy is protected by a set of liability rules. A person who invades another’s privacy can be sued. If DoubleClick tracks consumers by installing cookies in their computer storage devices, and if enough consumers feel that their collective privacy has been violated, then DoubleClick may be involved in a class action lawsuit. A property regime, on the other hand, gives control and power to the individual holding the property right, and requires negotiation before transference. In a property regime, the rights holder negotiates a price; in a liability regime, a court does.¹²

A property regime, though contentious, has become more and more appealing given the rampant misuse of personal information in the Web. Treating data as a property right and giving it adequate protection may help solve the problem of abuse. However, it may yet become a source of problems in the future.

What is a trade secret?

A trade secret is any formula, pattern, physical device, idea, process, compilation of information or other information that:

- provides the owner of the information with a competitive advantage in the marketplace; and
- is treated in a way that can reasonably be expected to prevent the public or competitors from learning about it, except through improper acquisition or theft.

In the physical world, trade secrets and ideas are revealed, copied by or sold to business rivals, leaving owners with a diminished competitive advantage. The same is true, and probably easier to do, in the Internet.

How are trade secrets compromised?

Trade secrets can be compromised either through outright theft of the information, or violation of a confidentiality agreement. The former constitutes industrial espionage, which may involve either the old “spy” paradigm or the newer paradigm of the computer hacker. In violations of confidentiality agreements, the obligation of confidentiality that has been breached may be an implied obligation, as with a company employee who is expected not to act against the interests of the company, or an explicit, contractual obligation signed between two companies.¹³

Are there ways of protecting trade secrets?

To emphasize the need for confidentiality, and to ensure proof of the existence of such an obligation, it has become customary in most high tech companies to require employees to sign a confidentiality agreement.

A trade secret owner can enforce rights against someone who steals confidential information by asking a court to issue an order (called an injunction) preventing further disclosure. It can also collect damages for any economic injury suffered as a result of the trade secret's improper acquisition and use.

An example of a trade secret violation suit involved Wal-Mart and Amazon.com. In October 1998, Wal-Mart filed suit in Arkansas against Amazon.com "to bring an immediate stop to what appears to be a wholesale raiding of its proprietary and highly confidential information systems by Amazon.com and others through the use of former Wal-Mart associates." In dismissing the suit, the court said it should have been filed in Washington State, where Amazon is based.

In January 1999, Wal-Mart again sued Amazon.com and its protégé, Drugstore.com, but this time in a Washington state court. The lawsuit alleged that Amazon hired away 15 key Wal-Mart technology executives for their knowledge of its computerized retailing systems. Amazon's chief information officer had served as vice president of information systems at Wal-Mart prior to being hired by Amazon in August 1997. In March 1999, Amazon filed a countersuit against Wal-Mart based "in part on unfair competition and intentional interference," setting up a complex legal Web of lawsuits. The cases were not resolved by the courts as the parties reached a settlement agreement in April 1999.¹⁴

How is ownership of a trade secret proven?

To prevail in a trade secret infringement suit, a trade secret owner must show that the information alleged to be confidential really is a trade secret. Again, a confidentiality agreement is usually the best way to do this. In addition, the trade secret owner must show that the information was either improperly acquired by the defendant (if the defendant is accused of making commercial use of the secret) or improperly disclosed-or is likely to be so-by the defendant (if the defendant is accused of leaking the information).

What if the secret is discovered within legal means?

However, people who discover the secret independently-that is, without using illegal means or violating agreements or state laws-cannot be stopped from using information protected under trade secret law. For example, it is not a violation of trade secret law to analyze (or "reverse engineer") any lawfully obtained product and determine its trade secret.



Some software companies have intentionally revealed their trade secrets to reveal whatever flaws are in them and for other people to offer solutions to these flaws. For example, Netscape published its source code after Netscape discovered that the program had security flaws that could be exploited by hackers or crackers. Netscape developers hoped that by revealing and posting the source code, other software developers can scrutinize it, find out the glitch, and provide patches that Netscape users can then download for free.

What are business method patents?

Business method patents are part of a family of patents known as utility patents that protect inventions, chemical formulas, and other discoveries. A business method is classified as a process because it is not a physical object like a mechanical invention or chemical composition.¹⁵

In July 1998, a federal court ruled that patent laws were intended to protect any method, whether or not it required the aid of a computer, so long as it produced a “useful, concrete and tangible result.”¹⁶

Some examples of business method patents are:

- Amazon.com’s famous “1-click” patent (U.S. Patent No. 5,960,411) issued September 28, 1999, is directed to a system and method for placing an order to purchase an item via the Internet. The patent is essentially directed to a methodology whereby information associated with a user is pre-stored by a Web site, and the user may thereafter order items from it with only one click of the mouse on a link associated with the item.
- Priceline “Reverse Auction” Patent (U.S. No. 5,794,207), for a “method and apparatus for a cryptographically assisted commercial network system designed to facilitate buyer-driven conditional purchase offers.” In October 1999, priceline.com sued Microsoft, accusing Microsoft’s Hotel Price Matcher of infringing its U.S. Patent No. 5,794,207 for reverse auctioning.
- DoubleClick Banner Ad Patent (U.S. No. 5,948,061), for a “method of delivery, targeting, and measuring advertising over networks.” In November 1999, DoubleClick filed a suit against L90 Inc. in the Eastern District of Virginia for its method of delivering advertising on the Internet.
- Open Market Electronic Shopping Cart Patent (U.S. No. 5,715,314) for a “network sales system.”

Business method patents can be used effectively against a major competitor. For example, in December 1999 Amazon.com successfully stopped BarnesandNoble.com from using a one-click shopping system and forced it to adopt a more complicated ordering system.

What are the requirements for acquiring a patent?

The US courts have since mandated that the Patent Office grant patents on business methods that satisfy the three-pronged test for patentability. That is, the invention must be:

1. Useful. A business need only demonstrate that its method or software provides some concrete tangible result. For example, the Amazon 1-Click patent provides a tangible result-an expedited purchase.
2. New. The method or software must be novel. This means it must have an aspect that is different in some way from all previous knowledge and inventions.
3. Non-obvious. The method or software must be non-obvious, meaning that someone who has ordinary skill in the specific technology cannot easily think of it. For example: An economist devised a method of avoiding taxes by using a credit card to borrow money from a 401(k) fund. The method did not exist previously and differed substantially from previous methods of avoiding taxes. Since the method was new and was not obvious to accountants or tax experts, the economist acquired a patent for it (U.S. Pat. No. 5,206,803).

What is the impact of the Internet on intellectual property?

The borderless character of the Internet, particularly electronic commerce, raises questions regarding the continued applicability of traditional legal systems in the enforcement of intellectual property laws. As discussed previously, traditional legal systems are based on notions of sovereignty and territoriality. In contrast, the Internet largely ignores distinctions based on territorial borders. Thus, the Internet has been described as “the world’s biggest copy machine.”

Given the capabilities and characteristics of digital network technologies, electronic commerce can have a tremendous impact on the system of copyright and related rights, and the scope of copyright and related rights in turn can have an effect on how electronic commerce will evolve. If legal rules are not set and applied appropriately, digital technology has the potential to undermine the basic tenets of copyright and related rights. In the Internet, one can make an unlimited number of copies of programs, music, art, books and movies virtually instantaneously, and without a perceptible degradation of quality. In fact, there is practically no difference between the original and the copy. And the copies can be transmitted to locations around the world in a matter of minutes. The result could be a disruption of traditional markets for these works.

How vulnerable is digital work to copyright infringement?

The digitalization of copyrighted works has made them more vulnerable to piracy. Because they hardly cost anything, downloading and pirating just about any available software, electronic books, or music from the convenience of one’s home computer is often irresistible.



This is cause for concern because e-commerce often involves the sale and licensing of intellectual property, and its full potential will not be realized if intellectual property products are not effectively safeguarded. Content providers and other owners of intellectual property rights will not put their interests at risk unless appropriate regimes—at the international and national levels—are in place to guarantee the terms and conditions under which their works are made available.

The music and movie industry has initiated copyright infringement actions against the use of mp3, a compression technology, which compresses music so it may not be as bulky to download. Aside from its successful action against Napster, a recent decision barred a site (2600.com) from distributing software to de-scramble DVD codes. In the latter case, a suit was filed against 2600.com centering on the site's practice of posting software that de-scrambles the code meant to prevent DVDs from being copied and linking to more than 500 other sites worldwide that make similar software available. The judge ruled against 2600.com, saying that "the plaintiffs have been gravely injured because the use of the program threatens to reduce the studio's revenue from the sale and rental of DVDs and thwarts new, potentially lucrative initiatives for the distribution of motion pictures in digital form, such as video-on-demand via the Internet."¹⁷

In May 2002, Audiogalaxy.com, a Napster-like clone that has facilitated and encouraged the unauthorized trading of millions of copyrighted songs, was taken to court by the Recording Industry Association of America (RIAA) and the National Music Publishers Association, Inc. (NMPA) for wholesale copyright infringement.¹⁸ Less than a month after the lawsuit, Audiogalaxy.com settled and agreed to a "filter-in" system that requires the consent of the songwriter, publisher and/or recording company before a song can be shared over the Internet.¹⁹

The music and movie industry have since brought lawsuits against several other similar companies, including *Kazaa BV*, *Grokster Ltd.* and *Streamcast Networks Inc.*

What is "copyleft"?

Copyleft is "a copyright notice that permits unrestricted redistribution and modification, provided that all copies and derivatives retain the same permissions."²⁰ *Copyleft* is a method for making a program "free software". Free software allows the user to run, copy, distribute, study, change or improve the software. Accordingly, it gives the user the freedom to: (1) run the program for any purpose; (2) study how the program works and makes it conform to the user's needs; (3) redistribute copies to other users; and (4) improve the program and release such improvements to the public.²¹

What is "GPL"?

GPL stands for General Public License. While licenses for most software prohibit sharing and program alteration, a GPL software gives the user the freedom to share

and change it. Under a GPL, the user is free to receive or request the source code, change the program or use such program, or portions of it, into an improved or altogether new free software. A GPL software, however, is subject to the condition that the enjoyment of the right to share and change is passed on to subsequent recipients or users.²²

What are the key issues in intellectual property rights protection in the Internet?

The most fundamental issue is the determination of the scope of protection in the digital environment—that is, how rights are defined, and what exceptions and limitations are permitted. Other important issues include how rights are enforced and administered in this environment; who in the chain of dissemination of infringing material can be held legally responsible for the infringement; and questions of jurisdiction and applicable law.

Are there international initiatives to protect intellectual property in the Internet? What Internet-specific treaties are in place?

The World Intellectual Property Organization (WIPO), through its 179 member States, has assumed responsibility for the formulation of a legal and policy framework at the international level to encourage the creation and protection of intellectual property. Its ultimate goal is to achieve an appropriate balance in the law, providing strong and effective rights, but within reasonable limits and with fair exceptions. Since trade in copyrighted works, performances and phonograms has become a major element of global electronic commerce, rights-holders should be legally secured in their ability to sell and license their property over the Internet subject to appropriate limitations and exceptions to safeguard public interest uses.

WIPO administers 23 international treaties dealing with different aspects of intellectual property protection.

Under the Berne Convention, the most important international copyright convention, copyright protection covers all “literary and artistic works.” This term encompasses diverse forms of creativity, such as writings, both fiction and non-fiction, including scientific and technical texts and computer programs; databases that are original due to the selection or arrangement of their contents; musical works; audiovisual works; works of fine art, including drawings and paintings; and photographs. Related rights protect the contributions of others who add value to the presentation of literary and artistic works to the public, namely, performing artists, such as actors, dancers, singers and musicians; the producers of phonograms, including CDs; and broadcasting organizations.

Likewise, in 1996 WIPO concluded two treaties: the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT). Commonly referred to as the “Internet treaties”, these seek to address the issues of the definition and scope of rights in the digital environment, and some of the challenges of online enforcement and licensing. The WCT and the WPPT also clarify the extent of rights-



holders' control when works, performances and phonograms are made available to the public for downloading or access on the Internet. This type of transmission differs from broadcasting, in that the material is not selected and delivered by an active transmitter like a broadcaster to a group of passive recipients. Rather, it is transmitted interactively, that is, on demand from the individual users, at a time and place of their choosing. The treaties require that an exclusive right be granted to control such acts of "making available", while leaving it to individual countries to decide how to classify this right under national law.

The treaties came into effect in March and May 2002, respectively. The provisions of both treaties were adopted by consensus by more than 100 countries, and thus represent broad international agreement regarding the appropriate approach to copyright in the digital environment. They are useful today as a guide and as a model for national legislation. In order for the treaties to be truly effective in cyberspace, they must become widely adopted in countries around the world. WIPO is therefore devoting substantial resources to promoting the treaties and to offering advice to governments on their implementation and ratification.

Why is there a need for such initiatives?

Issues of enforcement and licensing are not new, but they take on added dimensions and urgency when works are exploited on digital networks. In order for legal protection to become meaningful, rights-holders must be able to detect and stop the dissemination of unauthorized digital copies, which is accomplished at levels of speed, accuracy, volume and distance that in the past were unimaginable. In addition, for electronic commerce to develop to its full potential, workable systems of online licensing in which consumers can have confidence must evolve.

V. DOMAIN NAME DISPUTES

What are domain names?

Domain names provide the address of companies in the Internet and are equivalent to the business address in the physical world. As more and more companies use the Internet, the number of disputes arising from the use of domain names is increasing as well.

Domain names are divided into hierarchies. The top-level of the hierarchy appears after the last dot (.) in a domain name. In "microsoft.com", the top level domain name is .com, the most common top-level domain name, indicating that the domain name is owned by a commercial enterprise. Other common top-level domain names are .org (for non-profit organizations), .net (for network and Internet related organizations), .edu (for four-year colleges and universities), and .gov (for government entities).

Aside from these generic domain names, each country has a unique top-level domain name. For instance, .ca indicates a domain in Canada, and .ie indicates an Irish domain.

When and how can disputes over domain names arise?

The disputes that arise over domain names involve “second level” domain names, which refer to the name directly to the left of the top-level domain name in an Internet address. For instance, in the address “www.microsoft.com”, the second level domain name is Microsoft.

Two identical second level domain names cannot coexist under the same top level domain. For example, even though both the Delta Faucet Company and Delta Airlines would like the “delta.com” domain name, only one Delta company can have delta.com. Unfortunately for both Delta Faucet Company and Delta Airlines, that Delta company is Delta Financial of Woodbury, New York. (Delta Airlines uses deltaairlines.com, while Delta Faucet Company uses deltafaucet.com.)

Some well publicized examples of domain name disputes are:

- mcdonalds.com - This domain name was taken by an author from Wired magazine who was writing a story on the value of domain names. In his article, the author requested that people contact him at ronald@mcdonalds.com with suggestions on what to do with the domain name. In exchange for returning the domain name to McDonalds, the author convinced the company to make a charitable contribution.
- micros0ft.com - The company, Zero Micro Software, obtained a registration for micros0ft.com (with a zero in place of the second ‘o’), but the registration was suspended after Microsoft filed a protest.
- mtv.com - The MTV domain name was originally taken by MTV video jockey, Adam Curry. MTV at first showed little interest in the domain name or the Internet. But when Adam Curry left MTV, the company wanted to control the domain name. After a federal court action was taken, the dispute was settled out of court.
- taiwan.com - The mainland China news organization Xinhua was allowed to register the domain name taiwan.com, to the disgust of the government of Taiwan.

Who controls the registration of domain names? How are disputes resolved?

Prior to December 1999, a company called Network Solutions Inc. (NSI) was almost solely responsible for the registration of second level domain names for the most popular top-level domains, including .com, .net, and .org. NSI dictated the policy on domain name registration and had a great deal of control over how domain names were registered, and how disputes would be resolved. To avoid having to arbitrate in disputes, NSI adopted a first-come, first-served arrangement. Under this scheme, NSI would not question an applicant’s right to have a particular domain name. If the domain name was available, the applicant was given the name.



This policy has now been replaced with the Uniform Domain Names Disputes Resolution Policy created by ICANN (Internet Corporation for Assigned Names and Numbers) and used by all accredited registrars. Under this new policy, a trademark owner can initiate a relatively inexpensive administrative procedure to challenge the existing domain name. In order to prevail, the trademark owner must show that:

1. the trademark owner owns a trademark (either registered or unregistered) that is the same or confusingly similar to the registered second level domain name;
2. the party that registered the domain name has no legitimate right or interest in the domain name; and
3. the domain name was registered and used in bad faith.

Those disputing the grant of a domain name can go to the courts for this purpose. In the United States, the Anti-Cybersquatting Consumer Protection Act in November of 1999 made it easier for individuals and companies to take over domain names that are confusingly similar to their names or valid trademarks. However, they must establish that the domain name holder acted in bad faith.

One portion of this Act is related to famous individuals. This portion allows individuals to file a civil action against anyone who registers their name as a second level domain name for the purpose of selling the domain name for a profit. Take the case of the domain name juliaroberts.com. An individual who intended to sell it later to actress Julia Roberts registered the name. Citing bad faith on the part of the registrant, the court ruled that the domain name be transferred to its rightful owner.

Is there an international organization that can arbitrate disputes?

WIPO has set up an Arbitration and Mediation Center, described by its Web site as "internationally recognized as the leading institution in the area of resolving Internet domain name disputes". Since December 1999, the Center has administered proceedings in the generic Top Level Domains (gTLDs) .com, .org, .net.

Following ICANN's decision of 16 November 2000 to admit seven new gTLDs, WIPO has been working with the operators of the new gTLDs to develop domain name dispute resolution mechanisms for their domains. The Center has also been designated to provide dispute resolution services for these domains.

In addition, the Center administers dispute procedures in a number of country code Top Level Domains (ccTLDs), such as .ph for Philippines or .th for Thailand.

VI. CONSUMER PRIVACY AND PROTECTION

Advances in information technology and data management offer the promise of a new and prosperous cyberspace-based economy. New communications and information systems allow organizations to gather, share and transmit growing quantities of information with unprecedented speed and efficiency. But this technology also poses a

serious threat to privacy. Private individuals and organizations now have the access, means, methods and tools to encroach into the privacy of another-and in a manner that is not so obtrusive.

What is information privacy?

Of utmost importance is information privacy, “individual’s claim to control the terms under which personal information-information identifiable to the individual-is acquired, disclosed and used.”²³

Disclosural privacy is similarly defined as “the individual’s ability to choose for him/herself the time, circumstance, and extent to which his/her attitudes, beliefs, behavior and opinion are to be shared with or withheld from others.”²⁴

Why protect privacy?

The right to privacy is fundamental to any democratic society. The slightest apprehension on the part of a person using the Internet about who will see his personal information and how it will be used would by itself mean that he has lost a basic freedom. Moreover, the more others know about the details of a person’s life, the greater their opportunity to influence, interfere with, or judge the choices the person makes.

Having knowledge and control of how personal information is provided, transmitted and used is the key to protecting privacy

Is there such a thing as protecting privacy too much?

Foremost among the arguments used against the adoption of a stringent information disclosure regime is that it would ultimately hinder commerce. To require an individual’s prior consent before personal data can be elicited may actually hamper the growth of commerce that is largely based on a “better information equals better markets” theory. If the markets can profile their consumers accurately, a better match between interested buyers and sellers can be made.

Another argument is the need for truthfulness. The ethical or legal duties of disclosure inherent in a relationship command an openness that information privacy prevents.²⁵

What challenge does the protection of privacy pose? How can proper use of information be assured?

Finding a balance between the legitimate need to collect information and the need to protect privacy has become a major challenge. The following OECD guidelines may be considered as fundamental requirements for the proper use or processing of information online:



- Information Privacy Principle. Personal information should be acquired, disclosed, and used only in ways that respect an individual's privacy.
- Information Integrity Principle. Personal information should not be improperly altered or destroyed.
- Information Quality Principle. Information should be accurate, timely, complete and relevant for the purpose for which it is provided or used.
- Collection Limitation Principle. Personal data should be obtained by lawful and fair means, and where appropriate, with the knowledge and consent of the data object.
- Purpose Specification Principle. The purposes of data at the time of its collection should be specified.
- Security Safeguards Principle. Personal data should be protected by reasonable safeguards against risks like loss or unauthorized access, destruction, use, modification or disclosure of data.
- Openness Principle. There should be a policy of openness about developments, practices and policies with respect to personal data.
- Accountability Principle. A data controller has the responsibility to comply with measures based on the foregoing principles.

Are there other existing guidelines for data protection?

The European Union has issued Directive 95/46/EC, which establishes a regulatory framework to guarantee free movement of personal data, while giving individual EU countries room to maneuver with respect to how to implement the Directive. Free movement of data is particularly important for all services with a large customer base and dependent on processing personal data, such as distance selling and financial services. In practice, banks and insurance companies process large quantities of personal data, *inter alia*, on such highly sensitive issues as credit ratings and credit-worthiness. If each Member State had its own set of rules on data protection (for example on how data subjects could verify the information held on them), cross-border provision of services, notably over the information superhighways, would be virtually impossible and this extremely valuable new market opportunity would be lost.

The Directive also aims to narrow divergences between national data protection laws to the extent necessary to remove obstacles to the free movement of personal data within the EU. As a result, any person whose data are processed in the Community will be afforded an equivalent level of protection of his rights, in particular his right to privacy, irrespective of the Member State where the processing is carried out.²⁶

How can consumers be protected in electronic commerce transactions?

In December 1999, the OECD issued the Guidelines for Consumer Protection in the Context of Electronic Commerce to help ensure protection for consumers when shopping online and thereby encourage:

- fair business, advertising and marketing practices;
- clear information about the identity of an online business, the goods or services it offers and the terms and conditions of any transaction;
- a transparent process for the confirmation of transactions;
- secure payment mechanisms;
- fair, timely and affordable dispute resolution and redress; privacy protection; and consumer and business education.²⁷

Box 1.OECD Guidelines on Consumer Protection

A. TRANSPARENT AND EFFECTIVE PROTECTION

Consumers who participate in electronic commerce should be afforded transparent and effective consumer protection that is not less than the level of protection afforded in other forms of commerce.

B. FAIR BUSINESS, ADVERTISING AND MARKETING PRACTICES

Businesses engaged in electronic commerce should pay due regard to the interests of consumers and act in accordance with fair business, advertising and marketing practices.

C. ONLINE DISCLOSURES

I. INFORMATION ABOUT THE BUSINESS

Businesses engaged in electronic commerce with consumers should provide accurate, clear and easily accessible information about themselves sufficient to allow, at a minimum:

II. INFORMATION ABOUT THE GOODS OR SERVICES

Businesses engaged in electronic commerce with consumers should provide accurate and easily accessible information describing the goods or services offered; sufficient to enable consumers to make an informed decision about whether to enter into the transaction and in a manner that makes it possible for consumers to maintain an adequate record of such information.

III. INFORMATION ABOUT THE TRANSACTION

Businesses engaged in electronic commerce should provide sufficient information about the terms, conditions and costs associated with a transaction to enable consumers to make an informed decision about whether to enter into the transaction.

IV. CONFIRMATION PROCESS

To avoid ambiguity concerning the consumer's intent to make a purchase, the consumer should be able, before concluding the purchase, to identify precisely the goods or services he or she wishes to purchase; identify and correct any errors or modify the order; express an informed and deliberate consent to the purchase; and retain a complete and accurate record of the transaction.

V. PAYMENT

Consumers should be provided with easy-to-use, secure payment mechanisms and information on the level of security such mechanisms afford.



Dispute resolution and redress

Consumers should be provided meaningful access to fair and timely alternative dispute resolution and redress without undue cost or burden.

Privacy

Business-to-consumer electronic commerce should be conducted in accordance with the recognized privacy principles set out in the OECD Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data (1980), and taking into account the OECD Ministerial Declaration on the Protection of Privacy on Global Networks (1998), to provide appropriate and effective protection for consumers.

Education and awareness

Governments, business and consumer representatives should work together to educate consumers about electronic commerce, to foster informed decision-making by consumers participating in electronic commerce, and to increase business and consumer awareness of the consumer protection framework that applies to their online activities.

Source: Organisation for Economic Co-operation and Development, *Guidelines for Consumer Protection in the Context of Electronic Commerce* (2000); available from <http://www1.oecd.org/publications/e-book/9300023E.PDF>

How will the OECD guidelines be used?

The OECD Guidelines are designed to be a technology-neutral tool to help governments, business and consumer representatives by providing practical guidance to help build and maintain consumer confidence in electronic commerce. The Guidelines address the principal aspects of business-to-consumer electronic commerce and reflect existing legal protections available to consumers in more traditional forms of commerce. They stress the importance of transparency and information disclosure and the need for cooperation among governments, businesses and consumers at the national and international levels.

The Guidelines are intended to provide a set of principles to help:

- Governments - as they review, and (if necessary) adapt, formulate and implement consumer policies and initiatives for electronic commerce.
- Businesses, consumer groups and self-regulatory bodies - by providing guidance on the core characteristics of consumer protection that should be considered in the development and implementation of self-regulatory schemes.
- Individual businesses and consumers - by outlining the basic information disclosures and fair business practices they should provide and expect online.

What about jurisdiction and consumer redress?

The OECD Guidelines discuss at length the issues related to jurisdiction, applicable law and access to redress. Because of the broad and horizontal nature of these issues, questions about how they might best be addressed within the context of electronic commerce are not unique to consumer protection. However, the Internet's potential to increase the number of direct business-to-consumer cross-border transactions makes it important that consumer interests be fully taken into account.

The language on jurisdiction and applicable law within the Guidelines reflects the complexity and the current lack of international consensus on these issues. The Guidelines recognize that all business-to-consumer cross-border transactions are subject to the existing framework on jurisdiction and applicable law, but that electronic commerce poses certain challenges to that framework. The Guidelines call for further work in addressing these issues and ensuring that consumer interests are given appropriate consideration as the jurisdictional framework for electronic commerce evolves.

The Guidelines also focus particular attention on the importance of providing consumers with access to fair, timely and inexpensive means for redress, and encourage the development of effective alternative dispute resolution (ADR) mechanisms. Taking legal action to resolve a consumer dispute is generally an expensive, difficult and time-consuming process for everyone involved. These are problems that could be amplified in the event of cross-border disputes. As in other forms of commerce, the development and promotion of ADR can help to avoid more formal and costly legal options. Responding to consumer complaints quickly, easily and fairly, and establishing affordable and effective online dispute resolution mechanisms can go a long way toward building consumer confidence and trust.

Should the government be involved in consumer protection and privacy? What role can the private sector play?

In the end, the issue of consumer protection and privacy is a concern of both the government and the private sector. Government must ensure that there are adequate laws that offer protection to consumers; the private sector must implement meaningful, user-friendly, self-regulatory privacy regimes. Until users are confident that their communications and data are safe from interception and unauthorized use, they are unlikely to routinely use of the Internet for commerce. Only with consumer trust can we make e-commerce work.

VII. CYBERCRIMES

Is crime possible in the Internet?

The Internet has the potential to be one of humankind's greatest achievements. Telecommunications, banking systems, public utilities, and emergency systems rely on the network. But there are those who use it to inflict harm on others. In the short life of the Internet, we have already seen a wide array of criminal conduct. Although it is often difficult to determine the motives of these digital outlaws, the result of their conduct threatens the promise of the Internet by reducing public confidence and consumer trust in the whole system.²⁸

The threat of growing criminal conduct in the Internet is such that the US Federal Bureau of Investigation (FBI) has taken the unprecedented step of making the fight against cybercrime and cyber terrorism the bureau's No. 3 priority, behind counter-



terrorism and counterintelligence. In addition, the FBI has changed its hiring practices to focus on recruiting a new type of agent that can bring a bedrock of experience from the world of IT.²⁹

What are computer crimes or cybercrimes?

“Computer crime” or cybercrime refers to a misdeed involving the use of a computer. Cybercrimes can be divided into three major categories: cybercrimes against persons, property and government.

Cybercrimes against persons include transmission of child pornography, harassment with the use of a computer such as e-mail, and cyber stalking.

Cybercrimes against property include unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs, and unauthorized possession of computerized information. Hacking and cracking are among the gravest of this type of cybercrimes known to date. The creation and dissemination of harmful computer programs or viruses to computer systems is another kind of cybercrime against property. Software piracy is also a distinct kind of cybercrime against property.

A distinct example of cybercrimes against government is cyber terrorism, in which cyberspace is used by individuals and groups to threaten governments and to terrorize the citizens of a country. This crime may take the form of individuals “cracking” into a government or military-maintained Web site.³⁰

What are examples of common misdemeanors on the Internet?

1. Mail bombing involves the sending of messages to a target recipient repeatedly. The mailboxes of the recipients are then flooded with junk mail.
2. Spamming is often used as a tool for trade or promotion. It targets multiple recipients and floods selected mailboxes with messages.
3. List linking involves enrolling a target in dozens-sometimes hundreds-of e-mail listings.
4. Spoofing is faking the e-mail sender’s identity and tricking the target recipient into believing that the e-mail originated from the supposed mail sender.
5. Linking/Framing involves displaying one’s site content on another’s Web page without permission.
6. Denial of Service (DoS) is an explicit attempt by attackers to prevent legitimate users of a service from using that service.
7. Cracking is the act of gaining unauthorized access to a system and subsequently destroying or causing damage thereto.

In cyber stalking the “victim” is repeatedly flooded with messages of a threatening nature.

What is the reach of cybercrimes?

Crimes in cyberspace do not respect geographical boundaries or national jurisdictions. If left unchecked or unpunished, cybercrimes will adversely affect the growth of e-commerce. In addition, there is the rapid migration of real-world crimes such as child pornography, fraud, forgery, falsification, intellectual property theft, theft of information and money, as well as grave threats, to the virtual world.

What legal policies should be in place for the prevention, apprehension and prosecution of cybercrimes?

Legal provisions on theft or stealing need to be reviewed. In many jurisdictions, or in the real world, stealing or theft refers to taking a thing or depriving the victim of ownership thereof. What happens when a person accesses without authorization another person's file and then proceeds to copy it? In this case, it may be argued that theft did not occur because the thing was simply copied, not taken. Making things even less clear is a case in the US where it was held that the law pertaining to inter-State transportation of stolen property refers only to corporeal things and does not apply to intangible property.³¹

The US Department of Justice has classified the challenges to international as well as State prosecution of cybercrimes into three categories:

1. Technological challenges - While it is possible to trace an electronic trail, the task has become very difficult because of the skill and technology that allow near-absolute anonymity for the cyber-culprit.
2. Legal challenges - Laws and other legal tools to combat crime lag behind the rapid changes afforded by technology.
3. Resource challenges - These refer to the problem of lack of sufficient experts, or the lack of an adequate budget for new technologies as well as for the training of personnel.

What is being done to prevent and/or prosecute cybercrimes?

The US has passed the Computer Fraud and Abuse Act (18 USC 1030); 18 USC 2701 which punishes unlawful access to stored communications; 18 USC 2702 which prohibits divulging to any person the contents of a communication while in electronic storage; and 18 USC 2703 which allows government disclosure of the contents of electronic communications but only upon valid order of a court pursuant to a warrant.

After the terrorist attacks of September 11, 2001, the US Congress enacted the USA Patriot Act. This is a comprehensive legislation aimed specifically at countering the threat of terrorism, including cyber terrorism. The new law gives sweeping powers to both domestic law enforcement agencies of the US Government and US international intelligence agencies to help thwart terrorist attacks. The Patriot Act expands all four traditional tools of surveillance-wiretaps, search warrants, pen/trap orders and subpoenas-to make it easier for US law enforcement and intelli-



gence agencies to combat terrorism. For instance, the US government may now spy on Web surfing of Americans by merely telling a judge that the spying could lead to information that is “relevant” to an ongoing criminal investigation.

The Patriot Act likewise made two changes on how much information the government may obtain about users from their ISPs. First, Section 212 of the law allows ISPs to voluntarily hand over all “non-content” information to law enforcement with no need for any court order or subpoena. Second, Sections 210 and 211 expand the records that the government may seek with a simple subpoena to include records of session times and durations, temporarily assigned network addresses, means and sources of payments, including credit card or bank account numbers.³²

Are there intergovernmental efforts at combating cybercrimes?

The 41-nation Council of Europe has approved a Convention on Cybercrime. The treaty provides for the coordinated criminalization of the following:

1. Offenses against the confidentiality, integrity, and availability of computer data and systems, such as illegal access, illegal interception, data or system interference, and illegal devices;
2. Computer-related offenses like computer-related forgery and computer-related fraud;
3. Content-related offenses like child pornography; and
4. Copyright-related offenses.

The Treaty also urges its members to enter into cooperative efforts, through mutual assistance, extradition agreements and other measures, in order to combat cybercrime. The call for international cooperation is important given the fact that cybercrimes do not respect State, sovereign or national borders.

Similarly, the Asia Pacific Economic Cooperation (APEC) has endorsed the following action items to combat the growing threat of cybercrime:

- immediate enactment of substantive, procedural and mutual assistance laws relating to cyber security;
- making cybercrime laws as comprehensive as those proposed in the Council of Europe Cybercrime Convention;
- assistance between and among the economies in developing threat and vulnerability assessment capabilities;
- security and technical guidelines that can be used by governments and corporations in their fight against cybercrime; and
- outreach programs to economies and consumers regarding cyber security and cyber ethics.

The member-countries of the Association of Southeast Asian Nations (ASEAN) have agreed to create an ASEAN Network Security Coordination Center that will help combat cybercrimes and cyber terrorism. Computer emergency response teams

(CERTs) will also be established in each ASEAN country to serve as early warning systems against viruses. The ASEAN nations will likewise focus on strengthening their respective ICT infrastructure to attract more investors.

Are there anti-cybercrime efforts in developing countries?

In the Philippines, the E-commerce Act also penalizes hacking or cracking, as well as the introduction of viruses.

Malaysia's Computer Crimes Act of 1997 penalizes unauthorized access to computer material, unauthorized access with intent to commit an offense, unauthorized modification of the contents of a computer, and wrongful communication.

The Computer Misuse Act of Singapore criminalizes unauthorized access to computer material, access with intent to commit or facilitate an offense, unauthorized modification of computer material, unauthorized use or interception of computer service, unauthorized obstruction of use of computers, and unauthorized disclosure of access code.

In India, the Information Technology Act of 2000 prohibits tampering with computer source documents and hacking.

What lies ahead in the fight against cybercrimes?

It is thought that the best tool against cyber attacks and cybercrimes is still prevention. Available to many corporate users are a host of technologies that prevent, if not minimize, the occurrence of these attacks. Some of these are firewalls, encryption technologies, and public key infrastructure systems.

Aside from legislation, adequate resources must be provided to law enforcement agencies so that they can acquire the tools, equipment, and know-how necessary for the successful defense of network systems from cyber attacks. Laws to combat cybercrimes are useless if law enforcement agencies do not have the education and training necessary to even operate a computer. Judges, too, must be trained.

In addition, consultation, coordination and cooperation between and among governments and the private sector are important, in order to harmonize as completely as possible measures, practices, and procedures that will be utilized in combating this problem. Harmonization of laws at the international, regional and national levels is necessary to meet the challenges of a worldwide technology and its accompanying problems.

Who should be involved in preventing cybercrimes?

Security and privacy are not the responsibility of governments alone. There is a need for the private sector to implement user-friendly, self-regulatory policies.



Governments will have to work with industry and other cybercrime advocates to develop appropriate solutions to cybercrime concerns that may not be addressed adequately by the private sector.

An overarching task is to increase awareness at every level of society-in government, in the private sector, in civil society, and even among individuals-of the need for, and the goals of, security, privacy and cybercrime prevention and control. Also needed is awareness of the crimes that are committed in cyberspace and the possible measures against them. Finally, and perhaps most important, it is vital that we develop a social consensus about the proper and ethical use of computers and information systems.

VIII. CENSORSHIP OR CONTENT REGULATION

What is content regulation?

Internet content regulation refers to any type of legislation by governments that are 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.

How are governments approaching content regulation?

Many governments around the world have sought to address the problems posed by materials on the Internet that are illegal under their offline laws, and those considered harmful to or unsuitable for minors. The nature of material of principal concern has varied substantially, from political speeches, to material promoting or inciting to racial hatred, to pornographic material.

Government policies concerning censorship of the Internet may be grouped into four categories:

1. Government policy to encourage Internet industry self-regulation and end-user voluntary use of filtering/blocking technologies. This approach is taken in the United Kingdom, Canada, and many Western European countries. It also appears to be the current approach in New Zealand where applicability of offline classification/censorship laws to Internet content seems less than clear. In these countries, laws of general application apply to illegal Internet content such as child pornography and incitement to racial hatred. It is not illegal to make content "unsuitable for minors" available on the Internet, nor is access to the same controlled by a restricted access system. Some governments encourage the voluntary use and ongoing development of technologies that enable Internet users to control their own, and their children's, access to content on the Internet.

2. Criminal law penalties (fines or jail terms) applicable to content providers who make content “unsuitable for minors” available online. This approach is taken in some Australian State jurisdictions and has been attempted in the USA. In these countries, in addition, laws of general application apply to content that is illegal for reasons other than its unsuitability for children, such as child pornography.
3. Government-mandated blocking of access to content deemed unsuitable for adults. This approach is taken in Australian Commonwealth law (although it has not been enforced in this manner to date) and in China, Saudi Arabia, Singapore, the United Arab Emirates and Vietnam, among others. Some countries require Internet access providers to block material while others allow only restricted access to the Internet through a government-controlled access point.
4. Government prohibition of public access to the Internet. A number of countries, like China, either prohibit general public access to the Internet, or require Internet users to be registered/licensed by a government authority before permitting them restricted access.

Do developed countries regulate Internet content?

Yes. The Internet censorship regime in Australia consists of legislation at both Commonwealth and State/Territory Government levels. The Commonwealth regime is a complaints-based system and applies to content hosts, including ISPs, but not to content creators/providers. Content hosts are required to delete Australian hosted content from their server (Web, Usenet, FTP, etc.) that is deemed “objectionable” or “unsuitable for minors” on receipt of a take-down notice from the government regulator. The law does not require ISPs to block access to content hosted outside Australia. Instead, the ABA notifies filtering/blocking software providers of content hosted outside Australia to be added to their blacklists. Australian Internet users are not required by law to use blocking software. In addition, State and Territory criminal laws apply to content providers/creators. These laws enable prosecution of Internet users who make available material that is deemed “objectionable” or “unsuitable for minors”. The detail of the criminal offence provisions is different in each jurisdiction that has enacted or proposed laws of this nature.

Recent regulatory activity in France concerning illegal material on the Internet has focused on enforcing French laws prohibiting race hate material. In May 2000, a French judge ruled that USA Yahoo! Inc must make it impossible for French users to access sites auctioning race hate memorabilia. Yahoo! said it is technically impossible for it to block Internet users in France from seeing Nazi-related content on its USA Web site and that its French site complied with France’s laws prohibiting advertising Nazi memorabilia. In November 2001, a US District Court ruled that Yahoo! does not have to comply with the French court’s order concerning access to its USA site. The Court ruled that the USA First Amendment protects content generated in the US by American companies from being regulated by authorities in countries that have more restrictive laws on freedom of expression.



In the mid-1990s, German ISPs blocked access to some Internet content outside Germany containing material that is illegal under German laws of general application, particularly race hate propaganda and child pornography. In July 2000, it was reported that the German government had ceased trying to bar access to content outside Germany but police would continue to aim to stop illegal “homegrown” material. In 2001 and 2002, German authorities issued take-down notices to a number of Web hosts in the USA which refused to comply. The Ministry for Families, Seniors, Women and Children continues to issue take-down notices to foreign Web hosts under the “Act of the Dissemination of Publications and Other Media Morally Harmful to Youth” in relation to offshore sites that contain material “harmful to youth”. The Ministry claims jurisdiction over Web sites worldwide that contain “pornographic, extreme violence, war-mongering, racist, fascist and/or anti-Semitic content”. The notices require the Web host (as opposed to the Web site owner or content provider) to either remove the material or subject it to an age-verification system based on, for example, credit card checks.

What are the British and American approaches to Internet censorship?

The United Kingdom has not enacted censorship legislation specific to the Internet and appears to have no intention of so doing. In September 1996, a non-government organization named the UK Internet Watch Foundation (IWF) was established by ISP associations to implement proposals for dealing with illegal material on the Internet, with particular reference to child pornography. The IWF was established after the London Metropolitan Police sent a letter to all ISPs on August 9, 1996 requesting them to censor Usenet news groups or else police would find it necessary to prosecute ISPs in relation to illegal material made available via their systems.

The IWF operates a hotline to enable members of the public to report child pornography or other illegal material on the Internet. When the IWF receives a report, it reviews the material and decides whether it is potentially illegal. It then tries to determine the origin of the material and notifies the UK police or appropriate overseas law enforcement agency. It also notifies UK ISPs that they should take the material down from their servers; if they do not, they risk prosecution.

In February 2002, the IWF announced it would henceforth also deal with “criminally racist content” and that the Home Office had provided IWF with “an extended guide to the application of the [UK] law to racism on the Internet-’Racially Inflammatory Material on the Internet’”.

In 1996, the United States government began the push for Internet censorship when it passed into law the Communications Decency Act (CDA), which criminalized the sending of anything “indecent” over the Internet. In June 1996, a Philadelphia court struck down the CDA as unconstitutional as it went against the free speech guarantee. The Court ruled that the Internet is a “free marketplace of ideas” and should not be treated like television. One of the judges wrote, “...the Internet may fairly be regarded as a never-ending worldwide conversation. The Government

may not, through the CDA, interrupt that conversation. As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from governmental intrusion.”³³

Another failed Internet content regulation legislation is the Children’s Internet Protection Act (CIPA), a US federal law passed in December 2000 that ties crucial library funding to the mandated use of blocking programs on Internet terminals used by both adults and minors in public libraries. A federal court decisively rejected the CIPA on the ground that blocking programs cannot effectively screen out only material deemed “harmful to minors”. The court called the software a “blunt instrument”, adding that “the problems faced by manufacturers and vendors of filtering software are legion”.³⁴

The 9/11 attacks in New York and Washington and the presumed use of the Internet by terrorists to contact each other and prepare the operation resulted in the imposition of tough security measures and strict regulation of the Internet. A few hours after the attacks, FBI agents visited the head offices of the country’s main ISPs, including Hotmail, AOL and Earthlink, to confiscate details of possible e-mail messages between the terrorists. The monitoring of data on the Internet was legalized on October 24, 2001 with the enactment of the USA Patriot Act. This anti-terrorist measure confirmed the authority already given to the FBI to install the Carnivore program on an ISP’s equipment to monitor the flow of e-mail messages and store records of Web activity by people suspected of having contact with a foreign power. This requires only the permission of a special court.

Which developing countries regulate Internet content?

In September 1996, China reportedly banned access to certain Web sites by using a filtering system to prevent delivery of offending information. The banned sites included Western news outlets, Taiwanese commentary sites, anti-China dissident sites, and sexually explicit sites. A study by the Harvard Law School found that China has the most extensive Internet censorship in the world, regularly denying users access to 19,000 Web sites that the government deems threatening. The study, which tested access from multiple points in China over six months, found that Beijing blocked thousands of the most popular news, political and religious sites, along with selected entertainment and educational destinations. China also does not allow users to connect to major Western religious sites. News media sites are also often blocked. Among the sites users had trouble reaching in the test period were those of National Public Radio, *The Los Angeles Times*, *The Washington Post*, and *Time* magazine.

In Saudi Arabia public access to the Internet has been funnelled through a single government-controlled center since February 1999, when Internet access was first made available. From this center, the government blocks access to Internet content deemed unsuitable for the country’s citizens, such as information considered sensitive for political or religious reasons, pornographic sites, and the like. According to a report in *The New York Times* on November 19, 2001, over 7,000 sites are



added to the blacklist monthly and the control center receives more than 100 requests a day to remove specific sites from the blacklist-many because they have been wrongfully characterized by the US commercial blocking software used.

The Singapore Broadcasting Authority (SBA) has regulated Internet content as a broadcasting service since July 1996. Under a Class Licence Scheme, Internet Content Providers and ISPs are deemed automatically licensed. Licensees are required to comply with the Class Licence Conditions and the Internet Code of Practice, which includes the definition of "prohibited material". Briefly, "prohibited material" is that which is deemed "objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws." The SBA has the power to impose sanctions, including fines, on licensees who contravene the Code of Practice.

The SBA takes a light-touch approach in regulating services on the Internet. For example, licensees found to be in breach of regulations will be given a chance to rectify the breach before the Authority takes action. Users in Singapore have access to all material available on the Internet, with the exception of a few high impact illegal Web sites, and Internet content is not pre-censored by SBA; nor are ISPs required to monitor the Internet. SBA is concerned primarily with pornography, violence, and incitement of racial or religious hatred. SBA's purview covers only the provision of material to the public. Private communications, such as email and Internet Relay Chat between two individuals or parties, are not covered.

Are there countries that do not regulate content?

In August 1998, the Canadian Radio-Television and Telecommunications Commission (CRTC) called for public discussion on what role-if any-it should have in regulating matters such as online pornography, hate speech, and "Canadian content" on the Web. Subsequently, in May 1999, the CRTC issued a media release titled "CRTC Won't Regulate the Internet". It states, among others, that "[a]fter conducting an in-depth review, the CRTC has concluded that the new media on the Internet are achieving the goals of the Broadcasting Act and are vibrant, highly competitive and successful without regulation. The CRTC is concerned that any attempt to regulate Canadian new media might put the industry at a competitive disadvantage in the global marketplace."

Likewise, as of this writing, Denmark has no law making it a criminal offense to make material unsuitable for minors available on the Internet. Nor is there any proposal to create such a law. Discussion regarding protection of minors is unfolding primarily around the issue of filtering at public libraries.

Similarly, the "new media" (Internet) in Norway is not regulated by law. Instead the efforts are toward informing the public of the developments in the Internet through the Norwegian Board of Film Classification, which every now and then publishes reports concerning technological advancements and their social impact.

Is regulating the Net similar to regulating the telephone, radio or TV?

No. Government involvement in radio and television is based on the “scarcity” doctrine, which holds that government censorship of content is justified by the government’s role in assigning broadcast frequencies on a scarce spectrum. The Internet, on the other hand, is not a “scarce” resource as anyone can attach a computer to it without the government’s permission. Nor is it a government-licensed common carrier like a phone company. Moreover, the regulations that have been held constitutional for telephone, radio and TV merely seek to shift (“channel”) explicit speech to a time or place where children cannot access it, but not to ban such speech entirely.

Is censorship of the Internet the answer?

The Internet is the fastest growing and largest tool for mass communication and information distribution in the world. It can be used to distribute large amounts of information anywhere in the world at a minimal cost. The problem is that information may be “good” or “bad.” In the last 10 years, there has been increasing concern about damaging Internet content, including violence and sexual content, bomb-making instructions, terrorist activity, and child pornography.

What then? Should governments step in to filter information? Or should individuals be allowed to determine for themselves what is harmful? The question is not easily answered as it involves striking a delicate balance between the individual’s freedom of expression and information and a State’s right to prevent what it considers harmful to its subjects.

Table 2 sums up the two positions on censorship of the Internet.

What about self-regulation?

Self-regulation is less costly than traditional command-and-control regulation. First, command-and-control rules are unsuited to the rapid changes of technology in the innovation age. Second, with self-regulation authorities need not drastically expand their enforcement mechanisms. From the standpoint of participants in markets, whether industry or consumers, self-regulation might arise as a natural outgrowth of consumer demand. This “bottom-up” process is voluntary and likely to be highly decentralized.

How can self-regulation be made effective?

Codes of conduct should be adopted to ensure that Internet content and service providers act in accordance with principles of social responsibility. These codes should meet community concerns and operate as an accountability system that guarantees a high level of credibility and quality. For instance, as part of codes of conduct, Internet providers hosting content have an obligation to remove illegal content when they are informed that such content exists. The procedure for giving notice and take-down should be indicated.



Table 2. Censorship vs. No Censorship

Censorship	No Censorship
<p>Despite the generally prevailing principle of freedom of speech in democratic countries, it is widely accepted that certain types of speech are not given protection as they are deemed to be of insufficient value compared to the harm they cause. Child pornography in the print or broadcast media, for instance, is never tolerated. The Internet should be no exception to these basic standards. Truly offensive material such as hardcore pornography and extreme racial hatred are no different simply because they are published on the World Wide Web as opposed to a book or video.</p>	<p>Censorship is generally an evil and should be avoided wherever possible. Child pornography is an extreme example and there is already sufficient legislation to deal with those who attempt to produce, distribute or view such material. Other forms of speech may well be truly offensive but the only way a society can deal with them is by being exposed to them and combating them. Otherwise, these groups will merely go underground.</p>
<p>Censorship is tailored to the power of the medium. Accordingly, there is a higher level of censorship attached to television, films and video than to newspapers and books. This is due to the recognition that moving pictures and sound are more graphic and powerful than text and photographs or illustrations. There is also normally more regulation of videos than cinema films because the viewer of a video is a captive audience with the power to rewind, view again, and distribute more widely. The Internet, which increasingly uses video and sound, should be attached the same level of power and regulated accordingly.</p>	<p>The distinction between censorship of the print and broadcast media is becoming increasingly irrelevant. It is quite possible that in 10 years time people will be entirely reliant on the Internet for news and entertainment. The reason why the print media is comparatively unregulated is that medium is the primary means of distributing information in society. For this reason, the Internet must be granted the same protection. When the founding fathers of the US constitution spoke of the freedom of the press, they were concerned about the primary and most powerful organ of the media at that time, the print press. Nowadays they would more likely be concerned with preventing censorship of the broadcast media and the Internet, which are our prime means of distributing information.</p>
<p>That it is hard to censor the Internet does not mean we should not seek to do so, it is extremely difficult already to prevent the sale of snuff movies or hard core pornography but governments do so because it is deemed to be of societal importance. A more relevant difficulty is the anonymity provided by the Internet, which gives pornographers and criminals the opportunity to abuse the medium. Asian countries have experimented with requiring citizens to provide identification before posting content on to the Internet. Such a system, if universally adopted, could be a relatively simple way of enforcing laws against truly offensive and harmful content.</p>	<p>Even allowing for the extreme problems surrounding freedom of speech, Internet censorship would be more or less impossible. Governments can attempt to regulate what is produced in their own country but it would be impossible to regulate material from abroad. What is the point in removing all domestic reference to hardcore pornography in the USA when it is possible to access such material from the United Kingdom or Sweden? It is also possible for citizens to produce material and store it in an overseas domain, further complicating the issue. True freedom of speech requires anonymity in some cases to protect the author. The governments that have introduced ID requirements for Internet use also deny many basic rights to their citizens. The Internet allows citizens to criticize their government and distribute news and information without reprisal from the State. Such a system clearly could not survive with ID requirements.</p>

<p>In many countries there are multiple liabilities for production of slanderous material and material that incites racial hatred. Where the author or publisher cannot be traced or are insolvent the printers can be sued or prosecuted in some circumstances. The relatively small number of ISPs should be made liable if they assist in the provision of dangerous and harmful information such as bomb making instructions, hard core pornography, and the like.</p>	<p>ISPs are certainly the wrong people to decide what can and cannot be placed on the Internet. There is already far too much control of this new technology by big business without also making them judge and jury of all Internet content. In any case, the sheer bulk of information ISPs allow to be published is such that vetting would be more or less impossible. Were there is liability for allowing such material to be displayed, ISPs would inevitably err on the side of caution to protect their financial interests. This would result in a much more heavily censored Internet.</p>
<p>The issues at stake in this debate-protection of children, terrorist activity, crime, racial hatred, etc.-are all international problems. If a global solution is required, then it can be achieved by international cooperation and treaties. It is acknowledged that it is justifiable to censor where harm is caused to others by the speech, words or art of an author. All the examples cited above are clearly causing harm to various groups in society. By a combination of the initiatives listed above, it is possible to limit that harm.</p>	<p>Many ISPs have shown themselves to be responsible in immediately removing truly offensive content where they have been alerted to it. What is required is self-regulation by the industry recognizing their responsibility to Internet users but not imposing arbitrary and draconian restrictions upon its use. It is already possible for parents to use "Net nanny" browsers that will edit out offensive and inappropriate material for younger users.</p>

Source: Matt Butt, "Summary: Should governments censor material on the World Wide Web?" (November 3, 2000); available from IDEA Debatatabase <http://www.debatatabase.org/debatatabase/details.asp?topicID=83>

A service provider may include in its contracts with users and content providers terms that allow it to comply with its legal obligations and protect it from liability. It is in the best interest of industry to take on such responsibility since it enhances consumer confidence and is ultimately good for business.

To be effective, codes of conduct must be the product of and be enforced by self-regulatory agencies. Such agencies must be broadly representative and accessible to all relevant parties. Subject to a process of acquiescence by public authorities, they should enjoy certain legal privileges enhancing their functions. Effective self-regulation requires active consumer and citizen consultation by such agencies. Without user involvement, a self-regulatory mechanism will not accurately reflect user needs, will not be effective in delivering the standards it promotes, and will fail to create confidence.

Is there a role for government under a regime of self-regulation?

Self-regulation cannot function without the support of public authorities. The support can be in the form of simply not interfering with the self-regulatory process, or endorsing or ratifying self-regulatory codes and giving support through enforcement.

There are clearly limits to what can be achieved by self-regulation. It alone cannot guarantee that child pornographers are caught and punished. However, self-regu-



latory mechanisms can help ensure that criminals do not use the Internet with impunity. Governments should, through education and public information, raise awareness among users about self-regulatory mechanisms such as the means to filter and block content and to communicate complaints about Internet content through hotlines.

For governments, the emphasis should be on achieving regulatory efficiency by allowing business to take on as much of the task as possible. After all, business has a strong interest in creating trust across the whole spectrum of users and providers of services.

But where should the dividing line between business self-regulation and government regulation be drawn? Clearly, governments must ensure that the law is respected in cyberspace, to protect intellectual property and stop criminal abuse, for example. Business accepts the key role of governments in establishing Internet policy and is no less determined that the Internet should not become a free-for-all. In general terms, business urges governments to leave untouched those areas where there is no clear evidence that business conduct will have a negative effect on society or on the fundamental rights of individuals.

What about empowering the end-users?

Filtering technology can empower users by allowing them to select the kinds of content they and their children are exposed to. Used wisely, this technology can help shift control of and responsibility for harmful content from governments, regulatory agencies, and supervisory bodies to individuals. Thus, there is need for an improved architecture for the rating and filtering of Internet content. An independent organization that will provide a basic vocabulary for rating and oversee updates to the system at periodic intervals is needed.

A good filtering system realizes several important values: end user autonomy, respect for freedom of expression, ideological diversity, transparency, respect for privacy, interoperability and compatibility. Moreover, the system must feature a user-friendly interface that encourages actual use of its features and makes choice a real possibility for the vast majority of end users. Third parties should be encouraged to develop and provide free filters. Industry should promote the availability and use of filtering systems, educating consumers about how to filter and making it easy for parents, teachers, and other concerned adults to choose, install and adapt filters to their set of values. Regulatory requirements for service providers to screen or filter content should be avoided. Government or regulatory agencies may supply filters but should not mandate their use.

Likewise, there is a need for technical and organizational communication devices to ensure that users can respond to content on the Internet that they find to be of substantial concern. These “hotlines” ensure that, where necessary and appropriate, effective action can be taken to remedy such concerns. The task of evaluating the legality or illegality of specific data is difficult for Internet providers and should,

therefore, be integrated into the work of hotlines. In order to function, hotlines need an environment and operational rules that honor their specific task of handling problematic-and perhaps illegal-content. Legislators should formulate minimum requirements regarding the organizational setup and procedures of hotlines and, in turn, shield them from criminal or civil liability incurred in the proper conduct of their business (“safe harbor”).

What should be considered when choosing a particular regulatory mechanism?

Whatever the approach to content regulation, the important consideration is that regulation must not stifle innovation. It would seem that a hybrid between a government-regulated regime and an industry-regulated regime may be the right combination when dealing with censorship in the information age.

Because the Internet is global, there is a need for an international network of hotlines governed by a framework agreement containing minimum standards on the handling of content concerns and stipulating mutual notification between hotlines. The hotline in the country where the content is located is asked to evaluate it and to take action. This mechanism results in content providers being acted against only if the material is illegal in the host country. The mechanism also overcomes difficulties in the complex diplomatic procedures necessary for cross-border cooperation of law enforcement authorities.

In the final analysis, no regulatory mechanism can work independently of an education and awareness campaign. The Internet industry should have a continuous online and offline program to develop general awareness of self-regulatory mechanisms such as filtering systems and hotlines. Schools should provide the necessary skills for children to understand the benefits and limitations of online information and to exercise self-control over problematic Internet content. The Internet is itself a process, an enormous system for change and response, feedback and transformation. Like the Internet, the legal system and regulatory mechanisms around it must incorporate similar practices of learning and changing.³⁵



FOR FURTHER READING

- Baumer, David and J. Carl Poindexter. 2001. *Cyberlaw and e-commerce*. McGraw-Hill/Irwin.
- Berners-Lee, Tim. 1999. *Weaving the Web: the original design and ultimate destiny of the World Wide Web by its inventor*. Harper San Francisco.
- Black, Sharon K. 2001. *Telecommunications law in the Internet age*. 1st edition. Morgan Kaufmann.
- Casey, Eoghan. 2000. *Digital evidence and computer crime*. Academic Press.
- Ferrera, Gerald R. et al. 2000. *Cyberlaw: text and cases*. 1st edition. South-Western College Pub.
- Girasa, Rosario. *Cyberlaw: National and International Perspectives*.
- Hiller, Janine and Ronnie Cohen. 2002. *Internet Law and Policy*. 1st edition. Prentice Hall.
- Hitcock, David. *Patent searching made easy: how to do patent searching on the Internet and in the library*. 2nd edition. Nolo Press.
- Isenberg, Doug. 2002. *GigaLaw guide to Internet law*. Random House.
- Lessig, Lawrence. 1999. *Code and other laws of cyberspace*. New York: Basic Books.
- Lessig, Lawrence. 2001. *The future of ideas: the fate of the commons in a connected world*. New York: Random House.
- Litman, Jessica. 2001. *Digital copyright*. Amherst, NY: Prometheus Books.
- Rosenberg, Donald K. (2000). *Open source: the unauthorized white papers*. John Wiley & Sons.
- Stallman, Richard, Lawrence, Lessig and Joshua Gay. (2002). *Free software, free society: Selected essays of Richard Stallman*. Free Software Foundation.
- Vaidhyathan, Siva. 2001. *Copyrights and copywrongs: the rise of IP and how it threatens creativity*. New York University Press.

NOTES

- ¹ Doug Isenberg, *GigaLaw Guide to Internet Law* (Random House, 1985).
- ² *EDIAS Software Intern. V. BAGIS Intern., Ltd.*, 947 F. Supp. 412 (D. Ariz. 1996)
- ³ *DVD Copy Control Association, Inc. v. Andrew Thomas McLaughlin et al.*, Case No. CV 786804 (Superior Court of the State of California, County of Santa Clara).
- ⁴ Richard, Taylor, *The APEC Group and E-commerce Policy: Implications of the U.S. "Framework" for Global Electronic Commerce*; available from <http://www.ist.psu.edu/iip/Publication/Taylor/ITS98rt3.pdf>
- ⁵ *Approaches in Electronic Authentication Legislation*; available from http://rechten.uvt.nl/simone/Ds-art4.htm#_Toc468692769
- ⁶ *Ibid.*
- ⁷ *Ibid.*
- ⁸ *Ibid.*
- ⁹ *Ibid.*
- ¹⁰ Paul Scholtz, "Economics of Personal Information," *First Monday* 5, 9 (September 2000), [e-journal] http://www.firstmonday.dk/issues/issue5_9/sholtz/#s4
- ¹¹ *Ibid.*
- ¹² *Ibid.*
- ¹³ "Trade Secrets"; available from <http://www.cerebalaw.com/tradesec.htm>
- ¹⁴ James Hollander, "Amazon.com and Wal-Mart Settle Explosive E-commerce Lawsuit," *E-Commerce Times* (April 5, 1999), [e-journal] <http://www.ecommercetimes.com/news/articles/990405-1.shtml>
- ¹⁵ "Internet Business Patents," available from Nolo Encyclopedia <http://www.nolo.com/lawcenter/ency/article.cfm/objectID/C2DBFF26-7097-4B7B-AE36DA00499851EE>
- ¹⁶ *State Street Bank & Trust Co. v. Signal Financial Group, Inc.* 149 F.3d 1368 (Fed. Cir. 1998) cert denied 119 S. Ct. 851 (1999); available from <http://www.kuesterlaw.com/saris.htm>
- ¹⁷ Jennifer Hampton, "Hollywood Claims Victory in DVD Piracy Case," *E-Commerce Times* (August 18, 2000), [e-journal] <http://www.ecommercetimes.com/news/articles2000/000818-6.shtml>
- ¹⁸ "Songwriters, Music Publishers and Recording Industry Take Audiogalaxy.com to Court For Wholesale Copyright Infringement," *Recording Industry Association of America Press Releases* (May 24, 2002); available from http://www.riaa.com/PR_story.cfm?id=520
- ¹⁹ Susan Rush, "Audiogalaxy vs. The Music Industry: Case Closed," *Broadbandweek.com* (June 18, 2002); available from http://www.broadbandweek.com/news/020617/020618_content_Agalaxy.htm
- ²⁰ <http://www.dsl.org/copyleft/>
- ²¹ <http://www.gnu.org/philosophy/free-sw.html>
- ²² http://www.evolt.org/article/GNU_GPL/17/137/
- ²³ *Principles for Providing and Using Personal Information*; available from http://iitif.doc.gov/ipc/ipc-ipc-pubs/niiprivprin_final.html
- ²⁴ Irving J. Sloan, *Law of Privacy in a Technological Society* (Oceana Publications, 1986).
- ²⁵ Margaret N. Uy, "Internet Privacy, Are We Prepared For It? (Part 1)", *e-Legal* 1:2.
- ²⁶ "Council Definitively Adopts Directive on Protection of Personal Data", *European Commission Press Release: IP/95/822* (July 25, 1995); available from http://www.privacy.org/pi/intl_orgs/ec/dp_EC_press_release.txt
- ²⁷ OECD, *Guidelines for Consumer Protection in the Context of Electronic Commerce* (2000); available from <http://www1.oecd.org/publications/e-book/9300023E.PDF>
- ²⁸ Janet Reno, 5 April 2000
- ²⁹ Electronic Frontier Foundation, "EFF Analysis Of The Provisions Of The USA PATRIOT Act That Relate To Online Activities" (October 31, 2001); available from http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html



- ³⁰ "Cybercrime," Cyberlaw India FAQs; available from <http://www.cyberlawindia.com/cyberindia/cybfaq.htm#cybercrime>
- ³¹ *US v. Brown*, 925 F.2d 1301, 1308, 10th Circ. 1991
- ³² http://eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_analysis.html
- ³³ Jonathan Wallace, "Protecting the Worldwide Conversation: CDA Decision is a Sweet Victory - Part I;" available from <http://www.spectacle.org/cda/decision.html>
- ³⁴ "Federal Court Rejects Government Censorship in Libraries, Citing Free Speech Rights of Patrons," Press Release (May 31, 2002); available from American Civil Liberties Union online archives <http://www.aclu.org/news/2002/n053102a.html>
- ³⁵ Center for Democracy & Technology, "CDT Principles;" available from <http://www.cdt.org/mission/principles.shtml>

ABOUT THE AUTHOR

Rodolfo Noel S. Quimbo is the chief of staff of Philippine Senator Juan M. Flavier. He received his Bachelor of Arts in English and Law degrees from the University of the Philippines. He has written numerous articles and delivered many lectures on electronic commerce law in the Philippines and in the ASEAN region.



ACKNOWLEDGMENT

I wish to acknowledge the following:

Kimi, for her love, patience, and friendship;

Senator Juan M. Flavier, my boss, for the encouragement, and for generously granting me time to write this;

Romy and Lydia Quimbo, for encouraging me to go back to school;

Emmanuel Lallana and Jaime Faustino, for introducing me to e-commerce policy study;

Ramon J. Navarra Jr. and Renato N. Bantug Jr., able co-researchers and dearest friends;

Greta, whose tail always wags when I arrive home;

Pavan Duggal, Advocate, Supreme Court of India, for patiently reviewing the draft; and

Borro, Bheng, Rommel, Pids, Angie, Percy, Celia, Jean, Winnie, Rene, Didith, Philip, Cynthia, Bong, Perry, and Bats, and Katch, Shelah, Patricia, co-workers and friends.