Regulating Cyberspace
Can It Be Done?

Amado Jr M Mendoza

Touted for the most part as a revolutionary development with beneficial effects on the way people live, work and communicate, cyberspace has given rise to new and more complex types of legal issues. States are now confronted with the question of whether or not to govern cyberspace. This presupposes the question of whether cyberspace is governable to begin with, and if so, how. This essay notes that although technological advances may seem to render it ungovernable, cyberspace, like real world markets, will require regulation if it is to remain relatively free to spur innovation and creativity.

THE NATURE OF THE BEAST

CYBERSPACE IS AN OXYMORON. IT IS BOTH THERE AND NOT there. The cyberworld is a virtual world; it does not really occupy space nor does it have mass. But it 'exists' because physical infrastructure (computers, telephone lines, modems, etc.) undergird it. And real world transactions—personal, intellectual, commercial, diplomatic, and many others—are initiated and perfected in it.

The cyberworld is a world of networks made possible by the creation of the Internet or, simply the Net. According to its creators, '[T]he Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location' (Leiner et al. 2000). The network society, however, is real. It is a creation of networked communications media (of which the Internet is the most prominent) and it stands for new organizational formations and patterns that are characteristic of the most ad-

AMADO JR M MENDOZA is Assistant Professor at the Department of Science of the University of the Philippines in Diliman.

vanced economic sectors, highly competitive business firms, communities and social movements (Castells 1996; Stalder 1998).

Networks are reshaping the way people live, communicate and work. The technological changes that are transforming the business world (e-commerce, e-biz, B2B, B2C, etc.) and civil society will also revolutionize the way government operates and the very nature of public life in the near future. The digital revolution will remake the two distinct yet intertwined relationships between people and their governments: the one between the government and the citizen as 'customer' or 'consumer' of public goods and services, and the other between government and the citizen as 'owner' or 'shareholder'. These transformations will most likely be felt in countries where citizens are formally recognized as stakeholders of the polity.

Observers have argued that the growth of networked societies represent the emergence of a new society: 'A new society emerges when and if a structural transformation can be observed in the relationships of production, in the relationships of power, and in the relationships of experience' (Castells 1998). Social development is inseparable from technological change 'since technology *is* society and society cannot be understood or represented without its technological tools' (Castells 1996).[1]

To the extent that cyber-transactions are instantaneous and the Net enables long-term relationships, its multinational character makes it possible for users to engage in regulatory arbitrage, which is defined as choosing 'to evade disliked domestic regulations by communicating/transacting under regulatory regimes with different rules'.

The Internet is undoubtedly an international and global phenomenon. As Froomkin (1996) observes, Net users are largely indifferent to the physical location of their interlocutors as long as they understand each other and connection is established rather rapidly. To the extent that cyber-transactions are instantaneous and the Net enables long-term relationships, its multinational character makes it possible for users to engage in regulatory arbitrage, which is defined as choosing 'to evade disliked domestic regulations by communicating/transacting under regulatory regimes

with different rules. Sometimes this will mean gravitating to jurisdictions with more lenient rules, or perhaps no rules at all; sometimes it will mean choosing more stringent foreign regimes (for example, those with strong consumer protection laws), where stricter rules are more congenial' (Froomkin 1996).

CAN THE CYBERWORLD BE GOVERNED?

THEORETICALLY, the Net is the perfect Hobbesian world. In fact, that was how it was before big business realized its commercial potential. The designers of the Net wanted it to be as unrestricted as possible in order that research and intellectual exchange could proceed apace. But various social actors believe that the Net needs regulation given the volume of commercial transactions, both domestic and international, done through it. The most important regulatory issue is the protection and enforcement of property rights.

In the literature, there are two views regarding the governability of the Internet and other information-communications networks. An earlier trend considered the Net to be beyond regulation and argued that government should not regulate it. Former Grateful Dead lyricist and co-founder and vice chairman of the Electronic Frontier Foundation John Perry Barlow earlier wrote that copyright is dead, killed by the new technology. He claimed that 'everything we think we know about intellectual property is wrong' (Barlow 1994 quoted in Fujita 1996).

This view has long since been abandoned. A newer view regarding regulation and cyberspace has emerged. Its leading proponent, Harvard law professor Lawrence Lessig, asserts that code (the underlying architecture of the Net) regulates cyberspace (Lessig 1999a). In his works (Lessig 1999a, 1999b), Lessig acknowledges his debts to two academics—Joel Reidenberg of Fordham and Pamela Samuelson of Pittsburgh University and to two science-fiction writers, Vernor Vinge and Tom Maddox. Vinge reportedly warned at the 1996 conference on 'Computers, Freedom, and Privacy' about 'ubiquitous law enforcement,' made possible through computer chips linked by the Net to every part of social life. It would be a matter of time, Vinge warned, before government would and could claim its fair share of control and that each new generation of code would increase this power of government. For

Maddox, controls will be spawned by an alliance between government and business. In his view, business, like government, fares better in a regulated world—i.e., property is more secure, data are more easily captured, and disruption is less likely.

Reidenberg claims that life in cyberspace, like other forms of life, is regulated. This regulation, which he called *lex informatica*, is built into the code and determines what behavior is possible in cyberspace. A clear example is offered by the communications protocol used within the Net: no site in the Web can be accessed without the ubiquitous 'http' prefix. However, *lex informatica* is not a fixed law since it is dependent on code: when code is changed, *lex informatica* is likewise changed. For this reason, governments will try to regulate cyberspace not by directly regulating human behavior in cyberspace, but by regulating the code that regulates the behavior of people in cyberspace.

Samuelson, in response to the claim that cyberspace cannot be regulated by government, observes that several laws, especially those protecting intellectual property rights, are already changing the architecture of cyberspace (Lessig 1999b). In one of his works, Samuelson criticizes the anti-circumvention measures of the Digital Millennium Copyright Act of 1998 (DCMA) as being 'unpredictable, overbroad, inconsistent, and complex' and 'harmful to innovation and competition in the digital economy sector, and harmful to the public's broader interests in being able to make fair and noninfringing uses of copyrighted works' (Samuelson 1999).[2]

It is apparently the desire of copyright owners that their copyrighted products be distributed with built-in technical protection systems, as in the case of the SDMI format in lieu of the unprotected MP3 music format (discussed below), so that no unauthorized uses can ever be made of them. But the deployment and restrictiveness of built-in protection systems will largely depend on consumer response. The economists Carl Shapiro and Hal Varian (quoted in Samuelson 1999) warn that:

> The more liberal you make the terms under which customers can have access to your product, the more valuable it is to them. A product that can be shared with friends, loaned out and rented, repeatedly accessed, or sold in a resale market is obviously more

> valuable to a potential user than one that can be accessed only once, under controlled conditions, by only a single party.

In addition, competition may affect the successful deployment of technical protection systems. If one provider tightly locks up his product, a competing provider may see a business opportunity in selling a less restrictive good to customers who might otherwise buy from the first provider.

'The more liberal you make the terms under which customers can have access to your product, the more valuable it is to them.'

Apart from these mundane observations, it is the nature of the code, cyberspace's architecture, that defines the limits on its regulability. If governments will indeed try to regulate cyberspace by regulating code, then the question, according to Lessig (1999b), has to do with the regulability of code. The answer to this question depends on the openness of the code. If the code is closed (e.g., controlled by private for-profit organizations), then it is possible for government to exert more control. However, if the code is open (e.g., non-proprietary and outside the control of any particular economic actor), then governmental control is more difficult to impose. Why is this so?

> The reason is straightforward. Open code is software in plain view. It is software that comes bundled with its source code as well as its object code. Object code is the code that the computer reads. If you display it on your machine, it will appear as gibberish. But source code is the code that programmers can read. It is this code that allows a programmer to open an open source software project and see what makes it tick. By being able to see what makes it tick, open source software makes transparent any control that the code might carry. For example, if the code carries a government-mandated encryption routine, that routine will be apparent to open source coders. And because it is apparent, open source coders can then choose whether or not to adopt that portion of an open code project. For by its nature, and by the promises that it comes bundled with in the form of licenses, any open code software project remains available for adopters to modify or improve, however the adopters think best.
>
> Closed code functions differently. It does not come bundled with its source, which means that its code is hidden under a hood

> that won't open. Thus adopters or users of closed code cannot as easily detect what makes closed code tick. They can't as easily see whether it carries within it a given encryption routine or systems for collecting private data or technologies for monitoring and reporting usage. Clever adopters can try to work it out through reverse engineering or hacking. But no matter how clever the adopter, closed code will be harder to monitor, and harder to change than open code. An adopter of open source code who doesn't like a module can simply substitute another; an adopter of closed code has no equivalently simple choice (Lessig 1999b).

THE BIG BROTHER SYNDROME

A development fearfully forecasted by Vinge is the Federal Bureau of Investigation's (FBI) newfound ability to accurately monitor e-mail through a network snooping scheme known as Carnivore, so named because of its supposed ability to get to 'the meat' of what would otherwise be an enormous mass of electronic data. The Carnivore system may be used as a surveillance mechanism in investigations as it makes possible the interception of packets of data sent over the Net, including private e-mail between unsuspecting criminals.[3]

To be effective, the Carnivore system must be hooked directly to the computer networks of Internet service providers. That would give the government, at least theoretically, the ability to eavesdrop on all customers' digital communications, from e-mail to online banking and Web surfing. The FBI defends Carnivore as more precise than the wiretap methods used in the past since it allows investigators to tailor an intercept operation so they can pluck only the digital traffic of one person from among a stream of millions of other messages. An earlier version, code named Omnivore, could suck in as much as six gigabytes of data per hour, but in a less discriminating manner.

Still, critics contend that Carnivore is open to abuse. Mark Rasch, a former federal computer crimes prosecutor, said the nature of the surveillance made possible by Carnivore raises important privacy questions since it analyzes every snippet of data traffic that flows past, if only to determine whether to record it for the police. He likened it to listening to everybody's phone calls to identify which phone call one should be monitoring.

The extant Electronic Communications Privacy Act of 1986 allowed, with the proper court order, real-time interception of wired communications. Noting that there is no law that clearly allows or prohibits the use of Carnivore, the American Civil Liberties Union (ACLU) has asked the US Congress to amend outdated electronic privacy laws accordingly so that clear limits on what law enforcers can and cannot do are set unambiguously.

Carnivore can be stymied by encrypted electronic data, which could be expected of criminal traffic. These messages can be captured but law officers can read them only to the extent that they are decrypted. The electronic correspondence of law-abiding citizens will most likely be clear-text and it is their privacy that is theoretically subject to abuse.

The electronic correspondence of law-abiding citizens will most likely be clear-text and it is their privacy that is theoretically subject to abuse.

There is a similar debate on the other side of the Atlantic. The British spy agency MI5 recently announced plans to construct a million-dollar center to monitor e-mail and other online activity. The center, code named GTAC (Government Technical Assistance Centre), will give the British Security Service the power to monitor electronic and online activity under the new Regulation of Investigatory Powers (RIP) Bill. Officers will need a warrant to snoop into e-mail but do not need one to monitor the Internet (News in brief, *International Internet Law Review*, June 2000).

Two opposing court decisions on both sides of the Atlantic may likewise have far-reaching implications on free cyberspace speech. On 11 June 1996, a three-judge panel of the Eastern District of Pennsylvania granted a motion for preliminary injunction and suspended enforcement of the Communications Decency Act of 1996 (CDA), which it found to be in violation of the First Amendment. On 16 April 1997, across the Atlantic in Munich, Germany, Bavarian prosecutors announced the indictment of the senior manager of the German branch of the CompuServe Information Service, asserting that CompuServe should be held liable for offensive material posted on the Net that is accessible through CompuServe to its customers in Germany.[4]

The CDA represents the US Congress' first foray into regulating the content of online communication. It is designed to regulate obscenity, child pornography and 'indecency' on the Net and other interactive computer services (including even firm Intranets). The Philadelphia court panel noted that the Internet is as diverse as human thought and though sexually-oriented material exists online, the court found no evidence that this was the primary type of content on the Net. It likewise noted that nobody encountered sexually-oriented material on the Net by accident, unlike on radio and television.[5]

In the Bavarian case, Felix Somm, general manager of CompuServe GmbH, CompuServe's German affiliate, was charged with being an accessory in the dissemination of pornography, including child pornography, because CompuServe subscribers are able to access such material through Internet newsgroups. German authorities initially searched CompuServe's offices in 1995, and CompuServe blocked access to some 200 Internet newsgroups but later restored access to newsgroups that did not clearly contain illegal material such as child pornography. Somm's defense centered around the technical and practical realities of the Internet—i.e., the difficulty of controlling Internet newsgroup content, which consists of thousands of discussion threads participated in by countless individuals worldwide, and which changes constantly and cannot be monitored in advance in any meaningful way.

The Net is not national; it is not even international since it covers not only transactions between nations but all digital transactions within and between nations and non-state actors.

Two days after the Somm indictment, the German government proposed even more far-reaching regulation of the Internet. In its Information and Communications Services Bill, it proposed to regulate content on what is termed the 'German Internet', which is defined as any network or server within Germany and any network or server outside Germany to which someone inside Germany can post content. If enacted, the proposal would effectively seek to regulate content on the entire Net since German residents can obviously post content on networks or servers outside Germany. (At best, the proposal exhibits the German legis-

lators' lack of technical understanding of the Net. The Net is not national; it is not even international since it covers not only transactions between nations but all digital transactions within and between nations and non-state actors.)

THE QUESTION OF INTELLECTUAL PROPERTY RIGHTS

CAPITAL mobility in an increasingly globalized economy and the changed nature of on-the-cutting-edge products (being more a bundle of ideas rather than a package of tangible or material inputs) make property rights even more important today than ever before (Evans 1997). This is so because knowledge products (for example, software, movies, books, songs, etc.) are more susceptible to copying or replication. The open and replicative nature of contemporary technologies makes the enforcement of property rights over these same products difficult. Consequently, the key area of property rights enforcement and protection is the realm of intellectual products.

A recent case involving www.napster.com, a popular song-swapper on the Internet, is a case in point.[6] The Recording Industry Association of America (RIIA) asked the US federal courts to shut down the Internet site on the grounds of 'massive copyright infringement'. To date, Napster already has 22 million users who use the site to download music files (in the MP3 format), free of charge.[7]

Earlier, the RIIA had filed suit and gotten a favorable decision for copyright infringement against an older venture, MP3.com, at the Southern District Court of New York. The recording industry association claimed that the defendant's practices were promoting copyright infringement and therefore, music piracy. It contended that although any musical format (such as cassette tapes and CDs) can be bought or sold, the musical content belongs to the artist and should not be copied and stored for free. What apparently won the case for RIIA was the fact that although it is legal in the US to make copies of CDs and other music formats, it is illegal to allow an intermediary body to do so. According to one senior lawyer, the US has the court-made doctrine of "contributory infringement" that enables courts to enjoin third parties who "knowingly participate" in another's direct infringement. Particularly egregious direct infringers may be hauled to court to make "examples"

and raise awareness' (Discord in the online music industry, *International Internet Law Review*, No. 5, June 2000.)

Despite its defeat in court, MP3.com maintains that it did not interfere with recording industry copyright and revenue because its system can use only CDs that are already owned by the consumer. Although consumers can load CDs at will, MP3.com does not allow the resulting files to be shared between users. MP3.com opted to settle individually with the recording studios. The latest settlement was with Sony Music Entertainment, which MP3.com paid an undisclosed amount. It also signed a non-exclusive, North American licensing agreement with Sony (MP3 settles lawsuit, *Philippine Daily Inquirer*, 23 August 2000).

The case versus Napster is more interesting since it allows file sharing among its subscribers. Napster does not store digital MP3 files or makes them directly available to its subscribers. Although it supplies the software that allows users to download them from the Net, it is not technically violating copyright. However, it is under obligation to remove known pirates from its site. Thus, when the rock band Metallica personally delivered to Napster 13 boxes containing 335,435 names of specific Napster subscribers who, Metallica alleged, had illegally downloaded its music, Napster went ahead to block these subscribers from its site. (Discord...)

Asian entrepreneurs have apparently walked the proverbial extra mile to put one over copyright owners and enforcers. They download the MP3 files from the Net themselves and transfer them onto discs that are then sold to consumers who need not visit any Internet site. These discs also contain the software that consumers need to be able to play MP3 files on their personal computers. Making the disks an even better bargain is the fact that they are so cheap. At the Greenhills shopping mall in Metro Manila a disc costs only PhP 80.00. On the average, each disc carries 150 songs or an incredible PhP 0.53 per song; this means that a song is cheaper than the shortest jeepney trip or a bottle of softdrink. For consumers without personal computers, Greenhills vendors also sell a desktop MP3 player (manufactured in China and shamelessly carrying the famous Sony brand) which can play audio CDs, video CDs and MP3 discs, at the outrageous price of three thousand pesos

(PhP 3,000.00). These MP3 players can be hooked up to existing television and audio systems for the purpose of viewing VCDs or listening to audio CDs and MP3 discs.

These developments should not surprise knowledgeable observers since Asian (particularly South Korean) techies and indies have produced the world's first mass-produced portable MP3 player—the Rio. Korean engineer Hwang Jung Ha walked out of a lucrative job at Microsoft Korea to do so. Currently, two-thirds of all portable MP3 players sold around the world are Rios, now manufactured by the US-based digital media group, S3. The Singaporean group, Creative Laboratories, makes and sells the Nomad MP3 player which is gaining followers. The rest of the demand is met by no-name indies like Unitech, HanGo and Genica, many of them based in Korea. Over 200 firms—most of them financed by shoestring budgets—make MP3 players in Korea alone (Little Acorns, *Far Eastern Economic Review*, 17 August 2000).

The picture is a mixed one for the region. Smarting from their earlier error of ignoring the dotcoms offering free online music, the major recording companies believe that Asia may offer them a second chance to make handsome profits online. According to Michael Smellie, Tokyo-based senior vice president for BMG Entertainment, which carries a vast stable of artists, including Elvis Presley and Santana, they 'have something of a window here' but they 'need to move quickly' (Behind the Beat, *Far Eastern Economic Review*, 17 August 2000).

Learning from the Napster experience, every major recording company has announced plans to enter the online music world by selling or providing previews of recordings from second-tier artists. However, the recording industry has decided to use a standard other than MP3 because it lacks copyright protection and because it supposedly produces technically inferior sound quality—the Secure Digital Music Initiative (SDMI). This standard file format encrypts music files with a digital 'watermark' that can supposedly control how music is copied or on what devices it can be played, and even how many times or for how long it can be heard. For instance, the record company EMI recently released an online mix of over 100 albums. Sony Music Entertainment and the Universal Music Group have joined forces to explore selling music online on a subscription basis through PCs, wireless Internet and TV

set-top boxes (Behind...). Other Asian entrepreneurs, such as the Singaporean soundbuzz.com and Xudio.com and Hongkong's gogo.com, have joined the fray. The hope is that piracy-rife Asia will mend its ways.

The hope is that piracy-rife Asia will mend its ways. However, the end to what established industry calls 'cyberpiracy' is not in sight.

However, the end to what established industry calls 'cyberpiracy' is not in sight. Movie makers are the next 'victims' of Net-enabled piracy as new technology enables consumers to download full-length copies of high quality digital movies on to a regular compact disc or a personal computer hard disk from a number of illicit Web sites, as well as view them on their personal computer systems. The movie industry, especially the Hollywood studios, earlier assumed that it would take years before they would face the sort of digital piracy that is giving ulcers to the recording industry because digital video disk (DVD) movie files are extremely large compared to MP3 files and require many hours, even days, to download. However, new software can now store DVD movie files in 10-20 percent of the space required six months earlier. In addition, PC users can access the Internet faster with cable modem connections so that a full-length movie can be downloaded in an hour or two.[8]

A 16-year-old member of a Norwegian group calling itself Masters of Reverse Engineering (MORE), Jon Johansen, was arrested in January 2000 for helping to distribute over the Net the software program that enables users to make unauthorized copies of DVD movies. The teenager refuted the charges, stressing that he and others on the Internet created the software for playing DVDs on computers running the Linux operating system. Previously, when the movie industry contacted him and asked him to remove the source code, he complied so as to avoid a lawsuit. But the movie industry is suing anyway (DVD hacker arrested in Norway, *ZDNet News*, 25 January 2000).

Major Hollywood studios use an encryption scheme, the CSS or Content Scrambling System, on their DVDs to prevent unauthorized copying. Johansen's program, known as DECSS, is thought to have been the first program posted to the Internet that resulted from reverse en-

gineering the DVD copy protection system. The major studios scored a legal victory on 16 August 2000 when a US federal judge in New York ordered the hacker-zine 2600 Magazine to remove DECSS from its website. The ruling prevents 2600 from not only distributing copies of DECSS but also linking to Web pages or areas of a website where it resides. The decision, if upheld on appeal, could affect not only websites distributing DECSS—and there are thousands of them—but also efforts of the Linux users community to develop an open source DVD player.

DEADLY VIRII AND CYBERCRIME

IN May 2000, a computer virus allegedly written and spread by a young Filipino computing student wreaked havoc on e-mail systems around the world. The virus, innocuously named 'Love Bug', rapidly replicated itself via e-mail, overloading corporate and government e-mail systems in many countries and causing as much as $15 billion in damages.[9] While the virus caused a lot of actual damage, this was not the first time that the world's computers systems were tweaked and whacked by virii. Last year, a similar though largely harmless virus called Melissa spread around the globe.

The alleged author and unleasher of the deadly 'Love Bug' was identified as one Onel de Guzman, assisted by his equally young friends and fellow computing students. He was charged by Philippine government authorities but the lack of applicable laws in the Philippines forced prosecutors to dismiss all charges against him. A new law covering electronic commerce and cybercrime was passed in June 2000 in the aftermath of the Love Bug but it could not be used retroactively in de Guzman's case. He was charged with traditional crimes such as theft[10] and violation of a law that normally covered credit card fraud. However, the Department of Justice (DOJ) ruled that the credit card fraud law does not cover computer hacking and that investigators did not present adequate evidence to support the theft charge. Instead, the young man apparently got rewarded for his misdemeanor. Unconfirmed reports have it that he was hired by a British computer security firm for a handsome fee.

As things stand, computer attack, unlike murder or robbery, is still not universally recognized as a crime. Many countries do not have com-

puter hacking laws and are potentially safe havens for would-be attackers. Alarums have been raised by the DOJ's exoneration of de Guzman. Susan Brenner, a cybercrime professor at the University of Dayton School of Law in Ohio, said that if the DOJ's decision was widely publicized, it would have an effect 'opposite of deterrence'. She added: 'It makes it clear [that] if your country doesn't have a cybercrime law, you're not going to be prosecuted in that country' (Lack of law...).

There is in fact widespread ambivalence over computer hacking. In a manner similar to distinctions made between white and black magic, 'hacking' is differentiated from 'cracking' (de la Cruz 2000). The hacker is celebrated as an apostle of freedom and knowledge since he, being a programmer with advanced knowledge of computer operating systems and programming languages, constantly seeks further knowledge and freely shares with others what he has discovered. Much admired real life hackers include Richard Stallman of the MIT Artificial Intelligence Laboratories, who received the McArthur Genius Award for creating hundreds of freely distributable software for Unix (a computer operating system), and Linus Torvald, the creator of the LINUX operating system.

In a manner similar to distinctions made between white and black magic, 'hacking' is differentiated from 'cracking'. The hacker is celebrated as an apostle of freedom and knowledge...

On the other hand, the most celebrated cracker is Kevin Mitnick, a.k.a. Condor (after his role model, the character played by Robert Redford in the movie 'Three Days of the Condor': a CIA employee who uses his knowledge of the telephone network to avoid capture by sinister forces in the US government). As a teenager, Mitnick broke into the computers of the North American Air Defense Command (NORAD), foreshadowing the 1983 movie 'War Games'. He allegedly cracked every manner of secure site imaginable—including military and financial sites. Arrested and detained for minor crimes since his teens, Mitnick was imprisoned and held without trial since February 1995 and was conditionally released only last January 2000 (he will be freed from this conditional state on January 2003). If we are to believe Mitnick's supporters, the US prosecutors did not have much against him, being un-

able to compute exactly the losses allegedly sustained by businesses because of his cracking activities.[11]

Other prominent crackers include Kevin Poulsen and Justin Peterson. Poulsen alegedly seized control of the Pacific Bell Phone system and used his cracking talents to win a radio contest (with a Porsche as the prize) by manipulating the phone lines so that his call would be declared the winning one. Peterson meanwhile cracked a consumer credit agency, obtained a deal with the FBI to work undercover against other crackers, but went on another crime spree that ended in a failed attempt to secure a six-figure fraudulent wire transfer (de la Cruz 2000).

The latest darling is Jon Johansen of DECSS fame. His fate is again symptomatic of international ambivalence over cracking. When he helped write the DECSS software, he was only 15 and he did it with the full knowledge of his father who agreed that the program be posted in his father's website. Although he was brought in for questioning by the Norwegian police in January 2000, Johansen was never imprisoned.

INTERNATIONAL LAW AND CYBERSPACE REGULATION

SINCE cyberspace is a new phenomenon, one cannot expect international law to have been able to keep up with it, much less be able to formulate appropriate jurisprudence to regulate the various activities undertaken within cyberspace. The situation apparently is one where the pioneering efforts are essayed within municipal jurisdictions so that adequate experience may be accumulated as basis for international jurisprudence. Comparatively, the international law regime on intellectual property is relatively well-developed. The international law regime on intellectual property is built on the following international treaties and/or conventions to which the Philippines is a signatory party:

- the Berne Convention for the Protection of Literary and Artistic Works (Paris Act of 24 July 1971) as amended on 28 September 1971
- the Paris Convention for the Protection of Industrial Property (patent, trademarks, service marks and tradenames, industrial designs and layout, utility models, indicators of source and repression of unfair competition)

- the International Convention for the Protection of Performers, Production of Phonograms and broadcasting Organizations (Rome, 25 September 1984)
- the World Intellectual Property Organization (WIPO) Copyright Treaty adopted by the Diplomatic Conference on September 1996. This treaty includes databases, computer programs and photographic works. The convention establishing the WIPO was signed in Stockholm, Sweden on 14 July 1997
- the Trade Related Aspects of Intellectual Property Rights (TRIPS) agreement under the Uruguay Round of the General Agreement on Tariffs and Trade (GATT) of 1984
- the Treaty on Intellectual Property in Respect of Integrated Circuits (the Philippines is not a signatory to this treaty)

However, even with international issue-area regimes in place (such as the GATT-Uruguay Round Treaty with its TRIPS, TRIMS, etc), nation-states are still tasked with the enforcement and protection of intellectual property rights (Evans 1997). American copyright lawyers agree that the GATT and WIPO Treaties are potentially beneficial but there are caveats. Under GATT, member countries are required to adopt and enforce minimum standards of copyright protection. However, political realities have given rise to in a somewhat Faustian bargain. France, which is culturally protectionist, preserves its right to impose local quotas. Canada has imposed 'Canadian content' requirements in radio for many years. They complain that the discriminatory practices tolerated by GATT represent a potential threat to the growth of American content industries.[12]

A principal motivation for the two treaties adopted by the WIPO in December 1996 was to bolster copyright in the context of e-commerce. In addition to recognizing a specific right of online distribution, the Treaty on Copyright Law was the first international expression of the right to be protected against circumvention of technological measures intended to prevent unlawful replication. The Treaty on Performances and Phonograms established the rights of performers and producers of sound recordings. In addition, there was an 'agreed statement,' not incorporated into the treaty, that made clear that the right of re-

production under the Berne Convention included the right to make digital copies (Biederman 1999; Goldberg 1997).

Other observers have likewise argued that actors in the global economy need a public agency—i.e., the state—that can regulate the business environment even with respect to old-fashioned products, and that economic actors are necessarily embedded in national economic systems. Hirst and Thompson (1995) state that:

> Calculable trade rules, settled and internationally common property rights, and exchange-rate stability are a level of elementary security that companies need to plan ahead and, therefore, a condition of continued investment and growth.... Companies may want free trade and common regimes of trade standards, but they can only have them if states work together to achieve common international regulation.... Companies benefit from being enmeshed in networks of relations with central and local governments, with trade associations, with organized labour, with specifically national systems of skill formation and labour motivation. These networks provide information, they are a means to co-operation and co-ordination between firms to secure common objectives, and they help make the business environment less uncertain and stable—a national economic system provides forms of reassurance to firms against shocks and the risks of the international economy.

A number of cases can be cited to illustrate the international law dimensions associated with the protection and enforcement of intellectual property rights in cyberspace. Consider OLGA (the OnLine Guitar Archive), which flourished as an Internet site before representatives of the American recording industry succeeded in cutting it down to size. Contending that OLGA 'was nothing more than a compendium of illegal derivative works' (Biederman 1999), its opponents convinced many of the state universities whose websites were used by OLGA (the latter noting that certain court decisions in the US held that state governments and therefore state universities were immune from copyright infringement suits) to turn OLGA off for ethical and moral considerations. Following the closure of OLGA, the International Lyric Server (ILS) based in Switzerland uploaded thousands of song lyrics and distributed them throughout the world. When rebuffed by the ILS in a conciliatory first approach, the National Music Publishers Association (NMPA) of the US obtained a temporary restraining order against ILS, who ignored the

same. The Swiss authorities thereupon seized ILS's servers. The parties reportedly reached a settlement and the NMPA is working with the former proprietors to reconfigure ILS and restart it as a legitimate enterprise.

The regulatory arbitrage problem alluded to by Froomkin (1996) gives rise to international jurisdiction problems. A good illustration is a US District Court decision in Quantitative Fin. Software Ltd. V. Infinity Fin. Tech. Inc., where the court held that neither the Berne Convention nor its implementing legislation (the Digital Millennium Copyright Act) confers subject matter jurisdiction in the US for copyright infringement outside the States. If, for example, the ILS posts lyrics unlawfully in Switzerland and a US resident accesses it on his computer, where does the infringement occur?[13] If gambling is prohibited in a municipal jurisdiction but a domestic resident has accessed online gambling facilities, is he guilty of breaking his country's anti-gambling laws? In the case of copyrights, the contending positions are to apply either *lex protectionis* (the law of the country where the damage manifest itself) or the country-of-origin rule.

CONCLUSION

THE international law regime for the regulation of cyberspace remains underdeveloped. It cannot but be so since municipal law regimes are not well developed. That violations and violators are lightly punished or not even penalized at all is symptomatic of this underdevelopment.

...while technological advance may seem to render cyberspace ungovernable, cyberspace, like real world markets, will require regulation if it is to remain relatively free to spur innovation and creativity.

Despite some progress in the international protection of intellectual property rights, domestic and international jurists still have to fully recognize and deal with two incontrovertible facts about cyberspace. First, while cyberspace is virtual or spaceless space, it has real world infrastructures to support it, and real world transactions involving real people and organizations happen there in increasingly large volumes. Second, while technological advance may

seem to render cyberspace ungovernable, cyberspace, like real world markets, will require regulation if it is to remain relatively free to spur innovation and creativity.

Will governments insist on closed code as the underlying architecture of cyberspace? Or will there be a healthy mixture of open and closed code that will serve as cyberspace's *lex informatica*?

Only if and when these issues are faced squarely will regulation enable humankind to realize the full positive potential of cyberspace. As Lessig (2000) wisely puts it: 'We have the opportunity to preserve the original principles of the Internet's architecture and the chance to preserve the innovation that those principles made possible. But that opportunity will require a commitment by us, and by government, to defend what has worked and to keep the Net open to change—a regulation to preserve innovation.'

NOTES

1. Nonetheless, it is a simplistic error to argue that the character of a social formation is determined by technology. The present capitalist society is driven by private capital's competitive drive for profit. On the other hand, technological innovations evolve according to a different logic; they do not respond mechanically to economic reasons or profit motivations, and they are not automatically tapped by economic actors for their purposes (Stalder 1998). These views are contrary to those held by other observers of today's information society, notably Webster (1995) and Smith and Marx (1994). A more nuanced theory is offered by the social informatics school represented by Kling (2000). It recognizes that the impacts of information technology are socially shaped. In this view, technology-in-use and the social world are not separate; they co-constitute each other. Social relationships shape the kind of technological artifacts selected, their configuration and their typical modes of use. Technological artifacts are not seen as separable from social relationships and as mere engineering products. The use of new technology is moderated not only by the physical availability of suitable equipment. In truth, it is more often determined by 'social access'—or the mix of professional knowledge, economic resources and technical skills for using technologies in ways that enhance professional work and social life. Concretely, social access includes various social resources—skilled technical installers, trainers, consultants, and the like. Consideration of social access issues may help understand why there are digital divides in prosperous economies like the United States.

2. The DCMA prohibits the circumvention of technological protection measures used by copyright owners to control access to their works.

3. Information on the Carnivore system is culled from the following sources: Bolmer 2000; King and Bridis 2000; and Oakes 2000.

4. Information about these two cases is taken from Ennis, Kappler and Morris 1997.

5. An earlier decision, FCC v. Pacifica Foundation, ruled as indecent communications radio and TV messages that contain the 'seven dirty words' (Ennis, Kappler and Morris 1997).

6. Napster is an Internet site that provides its users software that enables them to download MP3 files free of charge from one another when they are logged on simultaneously. The site was founded in late 1999 by 19 year-old Shawn Fanning. Napster is not the only site offering this kind of service. MP3.com is an older company that promotes and distributes MP3 files to enable consumers an ever-expanding, world-wide catalogue. User's CDs are loaded onto the computer hard drive, either by being 'beamed' by MP3.com proprietary software, or ordered and purchased via the company's recommended online retailers. The reason behind Napster's greater popularity is its free service. Anticipating Napster's closure due to the federal court order, similar sites like Gnutella.com. Gigabeat.com, Myplay.com, and Scour.com have started operations and have bitten into Napster's user base.

7. An MP3 or MPEG-Audio Layer III file is a compression system for digitally formatted music that shrinks a song to a smaller size (by a factor of 10 to 14), making it easier to move and store on the Internet or a personal computer. To convert songs from traditional sources such as compact discs (CDs), cassette tapes or vinyl records into MP3 files, users can employ 'ripper' and 'encoder' software (the downloading of a song to play or encode it as an MP3 file is called ripping). Ripper software copies the song's file from the source onto a user's computer hard disk; encoder software compresses the song into MP3 format, with great fidelity (Discord in the online music industry, *International Internet Law Review*, Issue No. 5, June 2000, p.2).

8. A DVD typically stores up to five gigabytes of data, and many movies are easily that long. New compression software enables making a high-quality copy of DVD files at smaller sizes—close to the 650-megabyte capacity of ordinary CDs. For more information on these new technologies, see DivX Augurs the Arrival of a Napster for Movies, *The Asian Wall Street Journal*, 18 July 2000, p. 8. Other sources on DVD hacking include King 2000; McCullagh 2000a, 2000b, 2000c; Oakes 1999, and Patrizio 2000.

9. Information about the Love Bug is culled from the following sources: Cohen 2000; Hacked off in the Philippines, *The Economist*, 13 May 2000, p. 29; Return to sender, *The Economist*, 13 May 2000, p.

86; and Lack of law let hacker free, *Philippine Daily Inquirer*, 23 August 2000, p. 5.

10. In a very candid admission of the purpose of his proposed thesis, de Guzman said he wanted to write a program to 'steal and retrieve Internet accounts of the victim's computer,' allowing others to use these stolen log-ins to access the Internet free of charge. (Cohen 2000)

11. Information about Mitnick is culled from the following sources: de la Cruz 2000; Markoff 1995; and No Experts. No Evidence. No Justice, from *www.freekevin.com*. The latter is a website of Mitnick's supporters.

12. According to a statement by the International Intellectual Property Association released on 7 May 1998, US core copyright industries accounted for 3.6 percent of the country's GDP in 1996, amounting to $278 billion and representing 3.5 million jobs (Biederman 1999).

13. A legal query can be raised: Does the deed in fact happen in Switzerland? ILS is based in Switzerland. The lyrics are posted in cyberspace by operators in Switzerland. These same lyrics are accessed in cyberspace by an American resident in the US.

REFERENCES

Barlow, JP. 1994. The Economy of Ideas: A Framework for Rethinking Patents and Copyrights in the Digital Age (Everything You Know About Intellectual Property is Wrong). *Wired*, March.

Beiderman, D. 1999. Copyright Trends: With Friends Like These... *http://eon.law.harvard.edu/property/MP3/biederman.html.* (23 August 2000).

Bolmer, N. 2000. Carnivore Takes a Bite Out of Privacy. The Internet Law Journal, 5 August. *http://www.tilj.com/content/litigationheadline0803000I.htm.* (25 August 2000).

Castells, M. 1998. The Information Age: Economy, Society and Culture, Vol. III. *The End of the Millennium.* Cambridge and Oxford: Blackwell.

Castells, M. 1997. The Information Age: Economy, Society and Culture, Vol. II. *The Power of Identity.* Cambridge and Oxford: Blackwell.

Castells, M. 1996. The Information Age: Economy, Society and Culture, Vol. I. *The Rise of Network Society.* Cambridge and Oxford: Blackwell.

Cohen, A. 2000. School for Hackers. *Time*, 22 May, pp. 20-21.

Cruz, E. 2000. Framework: RP Universities and the New Economy. *BusinessWorld*, 11 July.

Dabeau, J and W Fisher. 2000. MP3. *http://eon.law.harvard.edu/h20/property/MP3 /main.html.* (23 August).

Davidson, S and N Engisch. 1996. Applying the Trademark Misuse Doctrine to Domain Name Disputes. *http://www.cla.org/Publications/MembersArticles/T-MISUSE.htm.* (21 August 2000).

de la Cruz, A. 2000. Internet Crimes. Multi-media presentation at the E-Commerce Legal Forum, Makati, 8 June.

Disini, J. 2000a. The Rule of Law in Cyberspace. Multi-media presentation at the E-Commerce Legal Forum, Makati, 8 June.

Disini, J. 2000b. Private Property in Cyberspace. Multi-media presentation at the E-Commerce Legal Forum, Makati, 8 June.

DVD Hacker Arrested in Norway. 2000. ZDNet News, 25 January. *http://www.zdnet.com/zdnn/stories/news/0,4586,2427192,00.html.* (25 August 2000).

Ennis, B, A Kappler, and J Morris. 1997. Governmental Attempts to Regulate Speech in Cyberspace: From Philadelphia to Bavaria and Back. *http://www.cla.org/Publications/MembersArticles/speech.htm.* (21 August 2000).

Evans, P. 1997. The Eclipse of the State? Reflections on Stateness in an Era of Globalization. *World Politics* 50(1): 62-87.

Friedman, M and K Bissinger. 1998. Infojacking: Crimes on the Information Superhighway. *http://www.cla.org/Publications/MemberArticles/infocrimeREV2-98.html.* (21 August 2000).

Froomkin, AM. 1999. Of Governments and Governance. Berkeley Technology Law Journal 14(2). *http://www.law.berkeley.edu/journals/btlj/articles/14_2/Froomkin/html/text.html.* (24 August 2000).

Froomkin, AM. 1996. *The Internet as a Source of Regulatory Arbitrage.*

Fujita, A. 1996. The Great Internet Panic: How Digitization is Deforming Copyright Law. Journal of Technology Law and Policy 2(1): Fall. *http://journal.law.ufl.edu/~techlaw/2/fujita.html.* (23 August 2000).

Goldberg, MD. 1997. The New WIPO Treaties A Report on the December 1996 Diplomatic Conference: The WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. *http://www.cla.org/Publications/MembersArticles/mdgcla.htm.* (21 August 2000).

Hirst, P and G Thompson. 1995. Globalization and the Future of the Nation-state. *Economy and Society*, 24: 408-42.

King, B. 2000. Tuning Up Digital Copyright Law. Wired News. 16 May. *http://www.wired.com/news/print/0,1294,36323,00.html.* (25 August 2000).

King, N and T Bridis. 2000. FBI System Covertly Searches E-mail. ZDNet News, 11 July. *http://www.zdnet.com/zdnn/stories/news/0,4586,2601502,00.htm.* (25 August 2000).

Kling, R. 2000. Learning About Information Technologies and Social Change: The Contribution of Social Informatics. The Information Society 16(3). *http://www.slis.indiana.edu/TIS/articles/Kling 16(3).pdf.* (23 August 2000).

Lee, M, S Pak, T Kim, D Lee, A Schapiro, and T Francis. 1999. Electronic Commerce, Hackers, and The Search for Legitimacy: A Regulatory Proposal. Berkeley Technology Law Journal 14(2). *http://www.law.berkeley.edu/journals/btlj/articles/14_2/Lee/html/text.html.* (24 August 2000).

Leiner, B, V Cerf, D Clark, R Kahn, L Kleinrock, D Lynch, J Postel, L Roberts, and S Wolff. 2000. A Brief History of the Internet. *http://www.isoc.org/internet-history/brief.html.* (18 August 2000).

Lessig, L. 1999a. *Code and other Laws of Cyberspace.* New York: Basic Books.

Lessig, L. 1999b. The Limits in Open Code: Regulatory Standards and the Future of the Net. Berkeley Technology Law Journal 14(2). *http://*

www.law.berkeley.edu/journals/btlj/articles/14_2/Lessig/html/text.html. (24 August 2000).

Lessig, L. 2000. Innovation, Regulation, and the Internet. The American Prospect, 11 (10): 27 March-10 April. *http://www.prospect.org?archives/V11-10/lessig-l.html.* (23 August 2000).

Markoff, J. 1995. Cyberspace's Most Wanted: Hacker Eludes FBI Pursuit. New York Times, 4 July 1994. *http://takedown.com/coverage/most-wanted.html.* (21 August 2000).

McCullagh, D. 2000a. Studios Score DeCSS Victory. Wired News, 17 August. *http://www.wired.com/news/print/0,1294,38287,00.html.* (25 August 2000).

McCullagh. 2000b. Teen Hacking Idol Hits Big Apple. Wired News, 20 July. *http://www.wired.com/news/print/0,1294,37650,00.html.* (25 August 2000).

McCullagh. 2000c. Digital Copyright Law on Trial. Wired News, 18 January. *http://www.wired.com/news/print/0,1294,33716,00.html.* (25 August 2000).

Nadel, M. 2000. Computer Code vs. Legal Code: Setting the Rules in Cyberspace. *Federal Communications Law Journal.* 52(3): 821-36.

No Experts. No Evidence. No Justice. 2000. *http://www.freekevin.com/news-052899.html.* 21 August.

Oakes, C. 2000. ACLU: Law Needs 'Carnivore' Fix. Wired News, 12 July. *http://www.wired.com/news/print/0,1294,37470,00.html.* (25 August 2000).

Oakes, C. 1999. DVD Hackers Hit With Lawsuit. Wired News, 28 December. *http://www.wired.com/news/print/0,1294,33303,00.html.* (25 August 2000).

Patrizio, A. 2000. MPAA Sues to Stop DECSS Linking. Wired News, 5 April. *http://www.wired.com/news/print/0,1294,35394,00.html.* (25 August 2000).

Pearson, H. 1997. International IT Law Update: Europe. *http://www.cla.org/Publications/MembersArticles/claeurit.htm.* (21 August 2000).

Quimbo, R. 2000. Legislative Response to Electronic Commerce Issues. Paper presented at the E-Commerce Legal Forum, Makati, 8 June.

Samuelson, P. 1999. Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised. Berkeley Technology Law Journal 14(2). *http://www.law.berkeley.edu/journals/btlj/articles/14_2/Samuelson/html/text.html.* (24 August 2000).

Smith, MR and L Marx. 1994. *Does Technology Drive History?: The Dilemma of Technological Determinism.* Cambridge and London: MIT Press.

Stalder, F. 1998. The Network Paradigm: Social Formations in the Age of Information. The Information Society 14(4). *http://www.slis.indiana.edu/TIS/articles/stlader.htm.* (24 August 2000).

Tricarichi, J. 1999. Hackers Defeat DVD Encryption and Post De-encryption Software on the Web. The Internet Law Journal. *http://www.tilj.com/content/ipheadline02290001.htm..* (21 August 2000).

Turnipseed, D. 2000. Initiative Encourages E-Commerce in the European Union. The Internet Law Journal, 8 March. *http://www.tilj.com/content/ecomarticle03080001.htm.* (24 August 2000).

van Dijk, JAGM. 1999. The One-dimensional Network Society of Manuel Castells. Chronicle World. *http://www.thechronicle.demon.co.uk/archive/castells.htm.* (24 August 2000).

Webster, F. 1995. *Theories of the Information Society.* London and New York: Routledge.