

CHAPTER 1

TOWARDS THE FURTHER LEGALIZATION OF GLOBAL INFORMATION LAW

Stephen C. Hicks and Michael L. Rustad
Suffolk University Law School
Boston, Massachusetts, United States

*Such is the unity of all history that any one who endeavors to tell a piece
of it must feel that his first sentence tears a seamless web.*

*Frederic William Maitland*¹

1.01 Introduction

The reader should be aware that the first few sentences in this chapter may well do just that to Maitland's observation. The Internet signifies a wholesale transformation in the way people and communities are formed and interact. The network of networks is a global medium that connects the home pages of every person and every nation in the world into a different kind of "seamless web". The Internet's "virtual" world not only changes one's primary medium of communication, and thus any model we may be using of human communication, but it allows an online business to sell goods and render services in any country connected to the web that comprises the Internet.

This changes the perception of the world as a place we inhabit, and it creates new worlds that need ordering through law. While the Internet is still a two-dimensional space, as seen externally as a platform for users in real space and time, it "shrinks distances" so that "the provider and consumer need not share the same geographic space".² It also "flattens time" so that communication may be

1 Maitland, "A Prologue to a History of English Law", 14 *Law Quarterly Review* 13 (1898).

2 Jenson and de Sousa Santos, *Globalizing Institutions: Case Studies in Regulation and Innovations* (2000), at p. 10.

instantaneous and across many different avenues, as if everyone were in the same place at the same time. The discontinuity of our normal experience of time in which we may live in the moment of excitement or endure days of boredom in an hour or two is leveled into a virtual and global instantaneity.³

Finally, one may say that it also renders everything uniform, in that the same website information appears for everything, regardless of its magnitude or importance, and hugely complex devices of bionic, computing, transmitting, and creative power utilize the same technologies and are, therefore, vulnerable to the same problems which may previously have only arisen in one dimension of time and space, but which now exist in virtual reality and which, therefore, the law must solve.

It follows from this uniformity, instantaneity, and placelessness that the “seamless web” of history must be torn asunder to grasp the importance of the changes that the seamless web of the Internet and cyberspace make in our lives. It marks a new stage in human history, one that may, as time unfolds, come to be seen as great a change in our way of living as was industrialization, the printing press, the emergence of the organized state, and even the appearance of a codified system of law itself, as one looks back over two thousand years of history.⁴

At all of these times in history, the law has lagged behind changes in technology, and so it is now. Still, there have been a number of myths constructed about Internet time and how it has transformed society. The unsupported mantra through the 1990s that Internet traffic was doubling every 100 days fuelled much of the excitement about what the technological revolution — that famous “paradigm shift” — would mean for telecoms, dot-coms, and other technology companies.⁵ What is different, however, is that Internet commerce takes place in a virtual world, not that of live interaction or voice to voice distant communication. Legal solutions, as a result, must be accommodated to the new problems of this new reality of the Internet and cyberspace.

For example, the growth of electronic commerce raises a great potential for litigation over the validity of:

1. Contracts by electronic agents;⁶

3 Hillis, *Digital Sensations* (1999), at pp. 79 and 80.

4 Hewitt de Alcantara, “The Development Divide in a Global Age”, 5 *Technology, Business, and Society*, United Nations Research Institute for Social Development Program, Paper Number 4 (August 2001).

5 Wahl, “The Superhighway to Hell”, *Canadian Business* (28 March/10 April 2005), at p. 19.

6 The electronic contracting provisions of article 2 of the United States Uniform Commercial Code (UCC) include definitions of “electronic”, “electronic agent”, “record”, “electronic record”, and “information processing system”, and certain electronic aspects of “receive” closely parallel those of the Uniform Electronic Transactions Act and the federal Electronic Signatures in Global and National Commerce Act. Sales contracts may be made by the interaction of electronic agents. Proposed Comment to Uniform Commercial Code, revised section 2-103(g) (Proposed 2002 Amendments to article 2 of the Uniform Commercial Code).

2. Mass-market license agreements;⁷
3. Digital signatures;⁸
4. Validity of e-contracts;⁹
5. Choice of law, and forum clauses;¹⁰ and
6. Use of disabling devices in software.¹¹

These are new problems for the law. The purpose of this chapter is to provide a context for understanding the subsequent chapters concerning the progress the law has made towards solving these problems.

The chapters in this volume reflect the problems of adapting diverse substantive fields of law to the new technologies and point towards the need for a global legal order. The World Summit on the Information Society (WSIS) is a step in the direction of coming to grips with the problems of a global legal

-
- 7 The first case in which a shrink-wrap software license agreement was enforced even though the terms were not disclosed prior to purchase. *ProCD, Inc. v. Zeidenberg*, 86 F3d 1447 (7th Cir., 1996). The *ProCD* court held that the licensee was bound to the terms of the license agreement for a software package called SelectPhone because he had an opportunity to review the restrictive license term prior to being bound. In that case, the licensee was found to be infringing the copyright in disseminating the licensed software on the Internet.
 - 8 Internet Law and Policy Forum, *Survey of State Electronic and Digital Signature Legislative Initiatives* (compiled by Perkins, Coie LLP) (visited 22 February 2005), at <http://www.ilpf.org/groups/update.htm> (surveying state digital laws).
 - 9 Uniform Commercial Code, revised section 2-103(h) (Proposed 2002 Amendments) (defining “electronic agent” to mean “a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual”). See also Uniform Commercial Code, revised section 2-105(o) (defining “record” to mean “information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form”). National Conference of Commissioners on Uniform State Laws, Revision of Uniform Commercial Code, article 2 — Sales (2002 Annual Meeting, 26 July/2 August 2002).
 - 10 *In re America Online Version 5.0 Software Litig.*, 168 F. Supp. 2d 1359 S.D. Fla., 2001); *Williams v. America Online, Inc.*, 2001 Mass. Super. Lexis 11 (Mass. Super. Ct., 8 February 2001) (refusing to dismiss claim and enforce AOL’s choice-of-forum clause in cause of action arising out of claim that personal computers were damaged by America Online Version 5.0 software).
 - 11 The 2002 Amendments to UCITA prohibit the use of disabling devices or remote shut-offs by licensors. Section 816(b) prohibits electronic repossession in all mass-market transactions. If the parties agree to permit electronic self-help in non-mass market licenses, the licensee must separately manifest assent to a term authorizing use of electronic self-help. See section 816(c). Detailed procedures for executing electronic self-help are found in section 816(c) and (d), National Conference of Commissioners on Uniform State Laws, Amendments to Uniform Computer Information Transactions Act, Meeting in its One-Hundred-and-Eleventh Year, Tucson Arizona, 26 July/2 August 2002 (2002 UCITA Amendments).

order in the information age and an emerging knowledge economy. In Geneva, in 2003, certain themes emerged from the Roundtable Discussions which will be followed up in Tunis in 2005. The themes were “access”, “diversity”, and “development”.

The primary concern voiced by all at the Geneva Summit was the appearance of a “digital divide” between the “haves” and the “have-nots”. This obviously speaks equally loudly of an “economic development divide” which transcends digital access, diversity, and development as such.¹²

To the extent that nations can create their own “e-strategies” and initiatives for entrepreneurship, investment, and subsequent regulation, which simultaneously preserve local culture and heritages within the trend towards globalization, the barriers of education and skills and of the cost and availability of the hardware to connect with the “seamless web” of global networking might be overcome. In the first phase of the World Summit on the Information Society, the conferees declared that the first principle was the:

. . . development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights.¹³

An abyss exists between the principle of equal access to information and the empirical reality of a world system trifurcated into “core”,¹⁴ “semi-periphery”,¹⁵

12 Hewitt de Alcantara, “The Development Divide in a Global Age”, *5 Technology, Business, and Society*, United Nations Research Institute for Social Development Program, Paper Number 4 (August 2001).

13 World Summit on the Information Society: Geneva 2003, Tunis 2005, Declaration of Principles, Building the Information Society: A Global Challenge in the New Millennium (visited 1 May 2005), at <http://www.itu.int/wsis/docs/geneva/official/dop.html>.

14 The first core nations to develop were England, France, and Holland in northwestern Europe, between 1300–1450. *Modern History Sourcebook: Summary of Wallerstein on World System Theory* (visited 13 February 2005), at <http://www.fordham.edu/halsall/mod/wallerstein.html>.

15 The semi-periphery regions were in the borderland between core and periphery countries in terms of stages of developments. The semi-periphery consists of countries in decline or peripheral countries “attempting to improve their relative position in the world economic systems”, *Modern History Sourcebook: Summary of Wallerstein on World System Theory* (visited 13 February 2005), at <http://www.fordham.edu/halsall/mod/wallerstein.html>.

and “periphery”¹⁶ nations. The worldwide trade framework of the World Trade Organization, including China, Russia, the former Soviet Republics, Taiwan, and Saudi Arabia, has spearheaded the development of a world system.¹⁷

The “Action Plan” for the Tunis Summit aims at 2015 as the target date for reducing measurable income disparities in economic growth, which have hitherto been exacerbated by technology. An obstacle to this is that one of the themes found in many of the chapters in this book is the degree to which major powers, such as the United States, are attempting to impose their legal norms on less-developed countries.¹⁸ In this respect, one may consider the “open source” movement, or the distribution of “free software”, as mechanisms that may offer ways around the direct confrontation between investment/profit and access/innovation to the benefit of developing nations entering the Information Age.

The creation of civil society for the digital age depends on an engineered consensus based on participation in the constitution of norms rather than the command and control of rules and regulation.¹⁹ Radically different cultures and legal systems are placed into conflict with the rise of the Internet. The

16 The countries of the periphery were at the opposite end of the economic development continuum. During early capitalism, the less-developed regions were Eastern Europe and Latin America. *Modern History Sourcebook: Summary of Wallerstein on World System Theory* (visited 13 February 2005), at <http://www.fordham.edu/halsall/mod/wallerstein.html>. Wallerstein argued that the core countries “expropriated much of the capital surplus generated by the periphery through unequal trade relations”. *Modern History Sourcebook: Summary of Wallerstein on World System Theory* (visited 13 February 2005), at <http://www.fordham.edu/halsall/mod/wallerstein.html>. Today, there is a new global system applicable to the Internet. In the new knowledge-based economy, the United States is the core hegemonic power seeking to impose its sovereignty on less-developed countries (semi-periphery and periphery). The problem for periphery and semi-periphery countries is that the core powers make the rules and control the markets. The United States has spearheaded a new system of global intellectual property rights. To date, much of the controversy over “global intellectual property rules” stems from the ability of the United States and other core powers to “ratchet up intellectual property standards”. Drahos and Mayne (eds.), *Global Intellectual Property Rights: Knowledge, Access, and Development* (2002) (arguing that the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) is an “extension of monopoly by these rules allow[ing] powerful Northern-based companies to extend control over markets and raise the price of vital technology goods”).

17 King, “The WTO: What It Does and Doesn’t Do, How it Affects U.S. Business”, 22 *Middle East Exec. Rep.* 8 (October 1999). The World Trade Organization that developed TRIPS now has 145 members as of 5 February 2005. World Trade Organization, Documents on Line (visited 28 February 2005), “WTO Membership Rises to 145”, (visited 1 April 2005), at http://www.wto.org/english/news_e/news_e.htm#armenia145.

18 Müller, “Who Owns the Internet? Ownership as a Legal Basis for American Control of the Internet” (21 March 2004) (visited 11 May 2005), at <http://ssrn.com/abstract=520682>.

19 Crawford, “Cyberspace: Defining a Right to Internet Access through Public Accommodation Law”, 76 *Temple L. Rev.* 225 (2003); Benoliel, “Technological Standards Inc: Rethinking Cyberspace Regulative Epistemology”, 92 *Cal. L. Rev.* 176 (2004).

forces dictating convergence represent those of the economically powerful, while the forces resisting are those of the groups and institutions and interests of civil society which know from history the important difference between a top-down system of authority, such as the *ecclesia*, or body of the church, and a bottom-up system, such as that of a *mund*, the quasi-representative body of a pre-feudal Germanic village.²⁰ Medieval history is instructive regarding the analogy between the divine right of a king, representing the “aristocratic” wealth of major corporations, and the sacred power of an emperor or a pope, representing the natural order of the “given world” and the real world of the people, who need representation, as they did before modern times.

The United Nations Project on the Information Society recognizes the need for greater legalization to achieve the promise of the interconnected digital world.

Nevertheless, a premise of the Geneva Summit, one that has since been affirmed, is that one cannot challenge the private/corporate leadership and/or domination of the information technology revolution. The role of governments is to educate their populations about this reality, and the role of civil society is to work within this from the bottom up. Therefore, a global world of Internet users is not going to resemble a homogenous group like the followers of a charismatic leader, members of a nation state, or believers in a true faith. Rather, they will look and act like members of a corporation who also are consumers of its products.

Even so, this does not mean that the United States controls the Internet. The Internet is no longer the exclusive province of the United States Department of Defense. The Internet is gaining a foothold on every continent. Internet usage is growing rapidly in China, which was expected to surpass Japan in late 2003.²¹

By December of 2002, the number of mobile phone subscribers in China was more than 200-million.²² Asia alone (with the exceptions of Japan and the Republic of Korea) added 21-million new users to the Internet in a single year.²³ The globalization of the information society is occurring at a rapid rate. Asian and Pacific countries are harnessing the power of e-commerce to

20 Ullman, “Juristic Obstacles to the Emergence of the State in the Middle Ages”, *The Church and State in the Earlier Middle Ages* (1975), at p. 264.

21 PTI, “Asia-Pacific Nations Pledge to Promote E-Commerce”, *Economic Times* (visited 22 February 2005), at <http://economictimes.indiatimes.com/cms.dll/xml/comp/articleshow?artid=29089893>.

22 NUA Internet Survey, December 2002 (visited 2 February 2005), at http://www.nua.com/surveys/?f=VSandart_id=905358668andrel=true (citing *ZD Net Report*; released by The Ministry of Information Industries).

23 Greenspan, “The Web Continues to Spread” (visited 20 January 2005), at http://cyberatlas.internet.com/big_picture/geographics/article/0,5911_1556641,00.html.

accelerate development.²⁴ In China, Malaysia, Indonesia, and East Asia, where software piracy is rampant, authorities are responding to outside pressure to restrain the online trading of software, music, and movies.²⁵ Broadband technology poses the greatest threat to copyright, as it shortens the download time for pirated media.²⁶

However, the point is that formation technology resists state control, whether it be taxation, censorship, or channeling through legalization. Civil society pushes back to be open, free, voluntary and, above all, uncoerced.

However, there still remains the reality of the digital divide and the economics of overcoming it, as the following chart demonstrates.

Chart I: The Internet as a Modern World System²⁷

Ideal Type	Core	Semi-Periphery	Periphery
Characteristics	Large numbers of Internet users, hosts; high proportion of personal computer ownership. ²⁸	Distribution networks not as seamless as core countries (lack of local warehouses, unable to compute price, delivery, taxes, or tariffs accurately). ²⁹	Low level of Internet users (10 per cent or less of population), low percentages of personal computer owners, low number of host servers, relatively few servers.

24 TI, "Asia-Pacific Nations Pledge to Promote E-Commerce" (visited 12 March 2005), at <http://economictimes.indiatimes.com/cms.dll/xml/comp/articleshow?artid=29089893>.

25 McCullagh, "Mexico Summit Urges Anti-Piracy Action" (visited 12 March 2005), at <http://news.com.com/2100-1023-963538.html>.

26 NAs *Internet Law News* (ILN) (8 October 2002) (visited 1 March 2005), at <http://www.online.wsj.com/article/0,SB1034042124444014600,00.html> (reporting an article in *Wall Street Journal*).

27 The authors wish to acknowledge the research assistance of Tracey Tom, who constructed this chart and assisted with the reconceptualization of the world system analogy for the World Wide Web.

28 The rise of the World Wide Web may be signaling a paradigm shift but, today, only approximately 14 per cent of the world's population is connected (888,681,131 out of 6,412,067,185 (13.9 per cent). Africa, for example, has achieved an Internet penetration of only 1.5 per cent (13,468,600 out of 900,465,411). Only 7.5 per cent of the population of the Middle Eastern countries is connected to the Internet (19,370,700 out of 259,499,772). In the Asian countries, Internet users total 302,257,003 out of 3,612,363,165. Latin America fares only slightly better with 10.3 per cent of the population connected to the Internet (56,224,957 out of 546,917,192). Australia/Oceania has 48.6 per cent of its population connected to the Internet (16,269,080 out of 33,443,448). Slightly greater than one-third of Europeans (35.5 per cent) are connected to the Internet (259,653,144 out of 730,991,138). North America leads the world with 220,437,647 out of 328,387,059 connected to the Internet. "Internet Usage Statistics — The Big Picture", *World Internet Users and Population Stats 2005* (visited 28 April 2005).

29 Forrester Report, "Mastering Commerce Logistics" (August 1999), reprinted as Tariff Product Fact Sheet (visited 22 February 2005), at <http://tariffic.com/Docs/Newsroom/mediakit1.htm>.

Country Policies	Focus on facilitating e-commerce, such as the United States moratorium on Internet taxes and new, multiple, and discriminatory taxes on e-commerce.	Primary focus on protecting intellectual property rights and enacting telecommunications laws: greater likelihood of government censorship or regulation.	Internet is often very strictly monitored in these countries.
Implication for Exporters	Large, sophisticated markets for all types of e-commerce activities. Likely targets for most e-business activities.	Lower percentage of Internet users and relatively low level of e-commerce in contrast to core countries.	Very low percentage of Internet users and very low level of e-commerce, particularly because of strict monitoring.
Exemplars	Australia, Canada, England, France, Japan, The Netherlands, New Zealand, United States. ³⁰	Argentina, Brazil, Chile, China, ³¹ India, Indonesia, Malaysia, Mexico, Philippines, Portugal, South Korea, Spain.	Cambodia, Cameroon, Central African Republic, Chad, Myanmar, Nepal, Rwanda, South Africa, Tunisia, Vietnam.

The contributors to this volume shed light on the barriers to an achievable information-based society. Each of the chapters in this volume confirms the rapid internationalization of information law that stems from a rapidly evolving global information society.³² While each contributor to this volume

30 The United States also is core of the top domains in the new economy. For example, the most popular websites visited by UK Internet users were predominately American sites: (1) Yahoo; (2) Freeserve; (3) MSN; (4) Microsoft; (5) AOL; (6) GeoCities; (7) Demon; (8) Amazon; (9) Excite; and (10) BBC. Cyberatlas, "Geographics: European Internet Audience Data" (visited 3 March 2005), at <http://cyberatlas.internet.com>.

31 By September 2002, China had more than 54-million Internet users among its population of 1.3-billion, the third largest Internet user-base after the United States and Japan. However, due to its monitoring of Internet use and still-developing distribution networks, the country remains for now in the semi-periphery category. PTI, "China Has World's Third Largest Internet User Base" (visited 12 February 2005), at <http://economictimes.indiatimes.com/cms.dll/xml/comp/articleshow?articid=29435857>. UNCTAD, *Annual Report*, AFP, "Internet Users to Reach 655 Million by Year-End" (visited 14 February 2005), at <http://www.smh.com.au/articles/2002/11/19/1037599406943.html>, which states that China's Internet user base is 56.6-million, the second largest Internet population in the world.

32 Goldstein, "Introduction: Legalization and World Politics", in Goldstein, *et. al.*, *Legalization and World Politics* 3 (2001) (defining key qualities of legalization as "[i]nternational institutions-enduring sets of rules, norms, and decision-making procedures that shape the expectations, interests, and behavior of actors but which vary on many dimensions").

has a slightly different perspective on global information law, each raises serious legal and policy issues necessary for further legalization of the information society. Each chapter raises a panoply of legal issues that need to be addressed by international treaties or conventions.

Legalization, the process of developing international legal constraints on nation-states, can be seen in many of the legal developments discussed in this volume as responses to changing information technologies, such as:

1. The Cybercrime Convention;
2. The World Intellectual Property Organization (WIPO) Uniform Dispute Resolution Proceedings for Resolving Domain Name Conflicts; and
3. European Union (EU) Directives Governing jurisdiction, electronic commerce, privacy, and the regulation of the information society.³³

The United Nations Project on Information Technology is a first step to achieving a transborder legal order where there is democratic participation. At present, there is disagreement among the participants at the open consultations on the form of Internet governance arrangements.³⁴ The principal fissure at the open consultations has been between those who seek Internet governance based on a United Nations framework versus those seeking a market-based private sector approach.³⁵

In an interesting way, this mirrors two different metaphors for conceiving of the Internet, namely, as the mythic open frontier for unfettered exploration or as a feudal society of mutually indebted and integrated levels of different stakeholders.³⁶

At present, the patchwork of disparate attempts to regulate the Internet signals the failure of civil society to govern the virtual world. Further harmonization is

33 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 *Official Journal* (L281) 31 (visited 1 March 2005), at <http://europa.eu.int/eur-lex/en/lif/date/1995/en395L0046.html>.

34 "UN E-Governance Panel Focuses on Spam, Web Governance", *DMEurope* (21 April 2005).

35 "UN E-Governance Panel Focuses on Spam, Web Governance", *DMEurope* (21 April 2005).

36 Yen, "Western Frontier or Feudal Society: Metaphors and Perceptions of Cyberspace", 17 *Berkeley Tech. L.J.* 1207 (2002).

needed to solve the growing substantive and procedural problems³⁷ of crossborder Internet-related litigation.³⁸

Just as the leading Western nations cooperated to create a unified law of the sea, advances in cyberspace technology are creating international problems that need to be addressed through a consistent cross-national legal regime. It is the form that this will take that remains uncertain at present. This provides the big picture context for considering both the problems and legal solutions of the global information society.

1.02 Electronic Contracting Issues

(a) The Law of E-Contracting in the World System

In a *New Yorker* cartoon, two dogs are seated in front of a computer. The caption reads:

On the Internet, nobody knows you're a dog.

Buying online is one important step removed from buying from a catalogue. Computer-to-computer contracts require a reworking of traditional contract law. A Clinton White House Report on Electronic Commerce contends that we “are on the verge of a revolution that is just as profound as the change in the economy that came with the Industrial Revolution”.³⁹ Since society is at every point changing, global commercial law also must change. The law lags behind social and technological change, and it must be continually updated. The Clinton Administration’s concept of the Global Information Infrastructure included wired and wireless networks, information appliances, and a global matrix of interconnected computer networks.⁴⁰

37 For example, the Anti-Cybersquatting Consumer Protection Act recognizes an *in rem* remedy useful in obtaining jurisdiction over foreign defendants. The United States Court of Appeal for the Fourth Circuit affirmed the lower court’s dismissal of the automobile manufacturer’s *in rem* action in *Porsche Cars N. Am, Inc. v. Porsche.net* 302 F.3d 248 (4th Cir., 2002).

38 In *Int’l Bancorp, LLC v. Société Des Bains De Mer Et Du Cercle Des Etrangers a Monaco*, 192 F. Supp. 2d 467 (E.D. Va., 2002), a trade mark infringement action involved the plaintiff Casino de Monte Carlo against off-shore defendants who had registered 53 “.com” and “.net” domain names that incorporated, in various ways, the name “Casino de Monte Carlo”. The plaintiff claimed that the companies’ use in United States commerce of the term “Casino de Monte Carlo” in the disputed domain names and on various websites constituted trade mark infringement in violation of the Lanham Act. The court concluded that the companies’ use of 43 domain names created a likelihood of confusion because the plaintiff’s mark had secondary meaning.

39 White House, “A Framework for Global Electronic Commerce”, 1 July 1997, at p. 1 (quoting Vice-President Albert Gore, Jr.).

40 White House, “A Framework for Global Electronic Commerce”, 1 July 1997, at p. 6.

Since article 2 of the Uniform Commercial Code was drafted more than a half century before the emergence of Internet contracts, it is not surprising that sales law is out of step with electronic commerce.⁴¹ The article 2 now in effect was a product of the 1940s and 1950s, long before the rise of the Internet. The revised article 2 will permit parties to sign sales contracts by executing a digital signature.⁴² The exchange of paper forms by humans is increasingly being replaced by contracts conducted by electronic means.

The licensing of Internet-related software, for example, requires licensors to comply with United States law as well as the law of every foreign nation where software is licensed.⁴³ The economies of the advanced industrial states are being broadly impacted by e-commerce, an entirely new mode of delivering goods and services in a networked world. The past decade witnessed the formation of “thousands of new ventures based largely on new business models”.⁴⁴

“The Internet is turning the process of contracting on its head. More and more, ordinary people enter into contracts electronically, over the Internet, through electronic mail, and by installing software”.⁴⁵ In 2003, the business-to-business Internet commerce “market will increase to US \$3.6-trillion, and at the end of 2004, worldwide business-to-business Internet sales transactions are forecast to reach US \$6-trillion”.⁴⁶ Direct marketers spent US \$217-billion in 2004 — half of all advertising — and the business-to-business market segment accounted for US \$114.7-billion.⁴⁷ Global electronic commerce creates an array of legal questions on what contract regime will facilitate business while at the same time honor the law of contract.

41 The revision of article 2 is a joint project of the American Law Institute (ALI) and the National Conference of Commissioners on Uniform State Law (NCCUSL).

42 Section 2-102(1) of the proposed draft will permit parties “to sign, or to execute or adopt a symbol or sound, or encrypt a record in whole or in part” as a functional equivalent to the paper-based signature; revised article 2 (Proposed Draft, 1 March 1998).

43 One of the greatest difficulties is that “some foreign jurisdiction may apply its laws . . . in an inconsistent or unpredictable way”. Twiddy, “United States: International Licensing: A Guide to Entering the Foreign Marketplace”, Mondaq’s Article Service: Kilpatrick, Stockton LLP, 26 February 2005 (visited 2 March 2005), at <http://www.mondaq.com/article.asp?articleid=2045>.

44 Bagby, “Cyberlaw: A Forward”, 39 *Am. Bus. L.J.* 521 (2002).

45 Hillman and Rachlinski, “Standard-Form Contracting in the Electronic Age”, 77 *N.Y.U.L. Rev.* 429 (2002).

46 Gartner Group, “Worldwide Business-to-Business Internet Commerce to Reach US \$8.5 trillion in 2005” (visited 3 February 2005), at http://www4.gartner.com/5_about/press_room/pr20010313a.html.

47 “U.S. Direct Industry Boosts Revenues to US \$2.3 Trillion”, *Precision Marketing* (1 April 2005), at p. 9.

(b) E-Contract Rules: Substantive and Procedural Issues

E-contract law makes it possible to make agreements to order goods or render services by any reasonable method, including the exchange of electronic records. Every web-based business must enter into a large number of online contracts to be competitive. Karen Mills addresses the question of the formation of contracts transacted through electronic means in a crossborder legal environment. The validity of electronic contracts will be determined on not only the facts and intentions of the parties, but how the contract will be interpreted, governed, and enforced. Her thesis is that an innovative contract law paradigm must evolve to accommodate to the “new e-economy”.

The critical question is whether the parties in an electronic transaction have reached an agreement and how the terms of the agreement will be interpreted. Mills reminds us that the substantive provisions of commercial law as well as the transactions have not fundamentally changed. What has changed is the means of purchasing goods and services, the financing of assets and projects, the issuance and transfer of stocks and bonds, the perfection of security interests, and cross-border transfers of commercial paper. In the Internet environment, contracts may be entered into through “click-wrap” or “browse-wrap” contracts or by simply downloading software with universal terms of service. However, she notes that negotiated contracts also may be entered into through electronic means where the language is dickered over in e-mail.

In her chapter, she compares contract formation rules in Common Law and Civil Law systems. Under the Common Law of contracts, formation occurs when the parties manifest a desire to be bound. She notes how normally this process is memorialized by an offer and acceptance. Common law contract, according to Mills, is based on a mutual declaration of an intention to be bound. The Civil Law paradigm of contracting rests on a bedrock of formal requirements. Once the formal requirements are met, the inquiry shifts to whether parties voluntarily intended to adhere to specific terms. She notes that individual Civil Law jurisdictions have their own formal requirements that address the question of when the parties are bound. Civil law countries do not require consideration, which is a requirement of the Common Law contract.

Given the significant differences in Civil Law and Common Law jurisdictions on the basic issue of contract formation, there will be prickly issues when parties are from entirely different legal traditions.

She next examines the different types of e-contracting practices that have evolved over the past decade. The simplest form of sales contract is the “click-wrap” agreement where the buyer clicks a box signifying that they agree with the terms set by the seller. While millions of click-wrap agreements are entered into each day, it is unsettled as to what constitutes an offer or acceptance.

Mills notes how questions arise as to exactly when contract formation has occurred. She notes that the so-called “browse-wrap” contracts used by websites are even more problematic. United States courts will be more inclined to enforce mass-market license agreements so long as the licensee has notice of terms and an opportunity to manifest assent. However, she questions whether courts outside the United States will find electronic formation for many of these mass-market agreements. European consumers, unlike American consumers, have an absolute right to file suit against sellers or suppliers if they pursue commercial or professional activities in the member state of the consumer’s domicile.⁴⁸

In the United States, consumers may waive their right to rights and remedies including the choice of law and forum.⁴⁹

This means that a United States business that directs its consumer transactions to Europe can be sued in the consumer’s home court.⁵⁰ It is quite likely that a website with different languages and accepting the Euro as a currency is directing its activities to member states.⁵¹

An American website that does not wish to be subject to the home court rule for jurisdiction over consumer contracts needs to employ blocking software or implement other techniques for “red flagging” European consumer

48 Brussels Regulation, article 15.1(c).

49 Compulsory arbitration clauses in mass-market license agreements have been enforced by a number of United States courts. *Westendorft v. Gateway 2000, Inc.*, 2000 Del. Ch. LEXIS 54 (Del. Ch. Ct., 16 March 2000); *Brower v. Gateway 2000, Inc.*, 676 N.Y.S. 2d 569 (1998); *Lieschke v. RealNetworks, Inc.*, 2000 U.S. Dist. LEXIS 1683 (N.D., 2000) (enforcing arbitration clauses in mass market licenses); *America Online, Inc. v. Booker*, 781 So. 2d 423, at p. 425 (Fla. Dist. Ct. App., 2001) (upholding forum selection clause in “freely negotiated agreement” and holding that the unavailability of a class action procedure in Virginia was not a sufficient basis for striking down a forum selection clause); *Caspi v. Microsoft Network, LLC*, 323 N.J. Super. 118, 732 A2d 528, at pp. 530, 532, and 533 (N.J. Super. Ct. App. Div., 1999) (upholding forum selection clause where subscribers to online software were required to review license terms in a scrollable window and to click “I Agree” or “I Don’t Agree”); *Barnett v. Network Solutions, Inc.*, 38 S.W. 3d 200, at pp. 203 and 204 (Tex. App., 2001) (upholding forum selection clause in online contract for registering Internet domain names that required users to scroll through terms before accepting or rejecting them); *Specht v. Netscape Commun. Corp.*, 306 F3d 17 (2d Cir., 2002) (holding that user’s downloading software where the terms were submerged did not manifest assent to arbitration clause); *Klocek v. Gateway, Inc.*, 104 F. Supp.2d 1332 (D. Kan., 2000) (declining to enforce arbitration clause on grounds that user did not agree to standard terms mailed inside computer box).

50 Article 15(1)(c) extends the consumer home forum rule to entities that direct activities to member states. Brussels Regulation, article 15(1)(c).

51 Article 6.1 of the Brussels Regulation provides that a company may be subject to jurisdiction if a co-defendant is domiciled in one of the member states. Brussels Regulation, article 6.

transactions. The European Court of Justice ruled that the Brussels Convention⁵² applied to a Canadian company in a contract action brought in a French court.⁵³

She notes how it is easy to electronically construct letterhead and difficult to determine the originator of documents. Cybercriminals, for example, use pseudonyms, false identities, and forged e-mail addresses to swindle consumers.⁵⁴ Internet fraudsters seamlessly transmit Internet fraud artists, for example, use auto-dialer programs to commit financial crimes. “The auto-dialer programs change Internet users’ dial-up settings to call an international number without their knowledge.”

To paraphrase Gertrude Stein, as far as the Internet is concerned, not only is there perhaps “no there there”, the “there” is everywhere there is Internet access.⁵⁵ There is no physical object for the subject to control in space; nor is it the subject which controls through time. Interaction is dispersed and not experienced as such. Contracting parties may fraudulently transmit electronic messages using any letterhead they wish. Documents may be copied, morphed, or transformed at a click of the mouse. Just as people invent identities in chat-rooms, so too are parties to contracts created in cyberspace, as well as their contracts. The immateriality of the Internet is a challenge for law.⁵⁶

Mills argues that the key question is to determine whose rules and what terms dictate contract law in this seamless and borderless contracting environment. She notes how the fundamentals of contract formation are so unsettled in the borderless electronic environment. The primary issue of open advertisements as an “offer to treat” or an “invitation to make an offer” is decided differently in Common Law than in Civil Law jurisdictions. She points to the language of article 14 of the Convention for the International Sales of Goods as a possible uniform view.

Legalization must begin with a clear cut methodology for entering into a legal, binding, and enforceable contract. The author practices in Indonesia and the contracting rules evolved out of Dutch law, which has norms which

52 The 1968 Brussels Convention was replaced by the Brussels Regulation in March 2002.

53 Gulland, “All the World’s a Forum: Businesses That Benefit from the Increased Globalization of Commerce Also Face Increased Risks of Liability Abroad”, *New Jersey Law Journal* (29 April 2002) (discussing *Group Josi Reinsurance Co. SA v. Universal General Insurance Co.*, 2000 E.C.R. I-5925).

54 *Zixit Corp. v. VISA USA, Inc.*, 2002 W.L. 3219734 (Tex. Dist., 31 July 2002) (reporting defamation lawsuit against VISA based on more than 400 anonymous messages on an Internet message board).

55 *Digital Equip. Corp. v. Altavista Technology, Inc.*, 960 F. Supp. 456, at p. 462 (D. Mass., 1997) (J. Gertner).

56 Poster, *What Is the Matter with the Internet?* (2001), at p. 17.

vary substantially from the Anglo-American law of contracts. All systems of contract law must answer as to who can be parties to contracts, as well as when, where, what, and why. Despite these differences, the Indonesian concepts of legal capacity, certainty of obligations, contractual purpose, and consent share much common ground with the Common Law.

One of the critical questions is whether an international regime of contract law will be the legal recognition of electronic signatures. Mills begins her survey of electronic signatures with a discussion of the United Nations International Trade Law Commission (UNCITRAL) Model Law on Electronic Signatures (2001). UNCITRAL's Model Law provides the basic concepts and methods for cross-border electronic contracting rules. She documents how electronic signatures are gaining acceptance in the United States (with the enactment of the E-Sign Act of 2000) and around the globe. She notes how software firms are offering sophisticated encryption products that permit authentication of signatures. The cross-border practitioner needs a globalized paradigm of electronic commerce law to facilitate commercial transactions in cyberspace.

(c) Cryptography and E-Signatures

The use of encryption as a means of protecting the global communications infrastructure raises difficult legal and political questions. Cryptography or the science of secret writing is a “science that has roots stretching back hundreds and perhaps thousands of years”.⁵⁷ Encryption runs readable messages called plaintext through a computer which in turn translates the message according to an algorithm into unreadable cipher text. Decryption then translates cipher text back to plaintext. Encryption methods are either conventional or symmetric and public-key or asymmetric cryptography.⁵⁸ Public-key cryptography is based on algorithms such as RSA and DSA, which are well-explained by Maury Shenk, Stewart Baker, and Winnie Chang in their chapter, “Cryptography and Electronic Signatures”.

The authors explain that AES, DES, and Blowfish are symmetric algorithms that permit the exchange of confidential communications through the use of a shared key. Symmetrical cryptography employs a single key to encrypt and decrypt messages, whereas public-key cryptography employs a pair of complementary keys: a private and public key. Asymmetrical algorithms, in contrast, such as RSA, employ a two-key system, one of which is usually public.

57 *Bernstein v. United States Department of Justice*, 176 F3d 1132 (9th Cir., 1999).

58 Oei, “Primer on Cryptography”, in Smedinghoff, ed., *Online Law: The Software Publishing Association's Legal Guide to Doing Business on the Internet* (1996), at p. 497 (describing the two generic types of cryptography).

The chapter by Shenk and his colleagues discusses the regulation of the export, import, and use of products and technology involving use of cryptography. In the United States, government control over encrypted communications has been the subject of great controversy. The Federal Bureau of Investigation implemented the Carnivore system to intercept electronic mail and instant messaging information pertaining to suspects from Internet Service Providers (ISPs).⁵⁹ The USA Patriot Act gives law enforcement the authority “to collect addressing information of electronic communications (e.g., e-mail) without a warrant”.⁶⁰ Encryption makes it possible to conduct electronic commerce safely. However, the seamy side of encryption is that it can be used by terrorists to conceal their communications.

Shenk, Baker, and Chang describe the types of encryption regulations, as well as the Wassenaar Arrangement (adopted by 33 countries) that sets the floorboards but not the ceiling tiles for export regulations, including mass market software. The Wassenaar Agreement is a transnational regime that seeks to increase the transparency of global transfer of conventional arms and dual-use goods, such as encrypted software products.) They note how the United States approach to encryption controls is functionally equivalent to the Wassenaar rules. Australia, Canada, the European Union (EU), and Japan have implemented export controls closely tracking Wassenaar controls. While Hong Kong and Singapore are not signatories to the Wassenaar Arrangement, they have policies that also track Wassenaar guidelines. However, not all countries follow this model, with China, Israel, and Kazakhstan applying various *ad hoc* controls.

In general, the United States reserves the most rigorous restrictions on encryption technology, proprietary source code, and open cryptographic interfaces (OCIs) exported to countries which do not qualify as favored countries. The authors note that the favored countries include the member states of EU, Australia, Japan, New Zealand, Norway, and Switzerland. However, the overall picture suggests the eventual deregulation of encryption products.

The authors’ global survey of export rules reveals a lack of harmony between Europe and the rest of the world. Throughout Europe, there are no meaningful controls on mass-market encryption products, regardless of key length. These products may be freely exported outside the EU. There also is no restriction on encryption used for scientific research. In addition to European Community-wide regulations, individual countries such as France may their own controls which are quite restrictive.

59 Lemley, *Software and Internet Law* (2003), at p. 911.

60 Lemley, *Software and Internet Law* (2003), at pp. 911 and 912.

Prior to 11 September 2001, the path of encryption controls was to gradually deregulate these products. In the post-911 period, this trend has been reversed. The authors note that there is little agreement as to the best approach to encryption regulation. In general, the core countries or those with advanced encryption industries have a stronger basis for implementing export controls. However, the authors doubt whether there is any realistic way of enforcing controls on the exporting of strong encryption products.

A digital signature is defined as an electronic signature “created and verified by means of cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again”.⁶¹ The purpose of a digital signature is to protect the integrity and authenticity of electronic messages. The first wave of electronic signature statutes enacted in several states of the United States adopted a prescriptive approach marked by inflexibility. More recently, an enabling approach is becoming popular, exemplified by the Uniform Electronic Transaction Act (UETA). However, most countries still adopt a hybrid solution, such as the EU’s Electronic Signature Directive. The final section of the Shenk, Baker, and Chang chapter explores the thorny issue of regulating digital signatures that employ public key cryptography. The authors call for a globalized regime for encryption controls in a crossborder environment.

1.03 Torts, Delicts, and Contractually-Based Remedies for Defective Software

Sakari Aalto, Lauri Mertala, and Leena Kerppilä examine the “Vendor’s Liability for Defective Software”. They conclude that the law of software has yet to develop an internationally accepted regime outside the field of intellectual property protection. Software law has been slow to develop because the courts tend to enforce one-sided software industry contracts that disclaim responsibility for defects in the United States, as well as in France, Germany, and Finland.

Legal remedies for software failure must be addressed in an international legal regime. Increasingly, the global infrastructure, from the “electronic power grid to air traffic control, is migrating to the Internet”.⁶² Hospitals and other health care providers are increasingly using the Internet to transmit

61 This definition was devised by the Information Security Committee, American Bar Association, Committee on Science and Technology, Digital Signature Guidelines with Model Legislation (1995).

62 Landau, “Sun Microsystems Inc., The Internet, Security, and Politics” (visited 16 November 2004), at <https://your.trash.net/pipermail/siug-discuss/2001-October/001829.html>.

medical images or provide medical consultations,⁶³ a process that has the potential of producing a large amount of tort litigation.

Aalto, Mertala, and Kerppilä describe a software industry too willing to race to market before adequately testing products and services. They argue that the industry releases products with serious defects or bugs relying on its customers to discover problems long after the release of software. The practice of testing products in the marketplace rather than the laboratory may make software more affordable, but not more secure. The authors argue that the allocations of liability in the delivery chain are inadequate from their multi-national survey of applicable regimes of substantive law. It may be cheaper not to fix known software defects where there is, in effect, a liability-free zone.

The authors' survey of software contracting law in the United States, Germany, France, and Finland reveals that freedom of contract is moderated by provisions in the law that protect software licensees. Under French law, the vendor is accountable for the consequences of software defects despite exculpatory language. The Finnish Sale of Goods Act also places the burden of proof on the vendor as under German law. Throughout Europe, unlike the United States, there are meaningful consumer protections and other mandated terms in business-to-consumer software contracts.

Under French law, even business licensees may be entitled to mandatory terms, such as non-disclaimable warranties and limits on the ability of the seller to disclaim liability. The French recognize the concept of a minimum adequate remedy that limits the power of the vendor to reallocate all of the costs of defective software. The authors note how the concept of "professional of the same specialty" (*professionnel de la même spécialité*) applies to French business-to-business software transactions.

In the United States, Maryland and Virginia have enacted the pro-licensor Uniform Computer Information Transactions Act (UCITA). UCITA permits software vendors to disclaim all warranties and limit vendors' remedies to a refund. UNCITRAL's Convention for the International Sale of Goods (CISG) is more user friendly, but it does not explicitly govern software. The authors note that the applicability of CISG continues to be an unsettled issue.

The information-based world system needs a harmonized software law that balances the interests of licensors and licensees. Aalto and his colleagues have documented the need for a new cross-border law governing vendors' liability for bad software. We have entered a new information-based

63 Telemedicine may involve a physician answering a question on a website, or it may take a more complex form, such as having an emergency room physician in Milwaukee consult with a colleague in New York. The Internet makes it possible for a cardiologist in Miami to assess sounds of the heart and lung of a patient located in a small hospital in the Red River Valley of Northwest Minnesota.

economy based on software and other transfers of information. There is an urgent need for harmonizing the rights and remedies for the victims of defective software.

Next, the authors examine the problem of defining defects in performance or the quality of software. Apart from security problems, software may have design defects that cause problems with formatting, processing speeds, the amount of data that could be handled, and problems of system integration with other software components or users.⁶⁴ However, the authors note that software failure may be a problem of compatibility with hardware or other software. Products liability has yet to be extended to the worldwide software industry that has evolved in less than a quarter century.

The authors contend that product liability cannot develop until there is widespread agreement on what constitutes a defect. The law of software warranties has evolved faster than the theory of strict products liability. A defect is a predicate to a products liability action. Products liability is a branch of tort law concerned with “the bases for, defenses to, and scope of liability of manufacturers and others who are in the business of selling or supplying goods for harms caused by defective tangible products”.⁶⁵

The authors document that the law of software in France, Germany, and Finland is primarily based on contract rather than tort, as in the United States. The principal obligation of a software vendor is to deliver products that perform in conformity with product specifications. The authors argue that meaningful remedies are needed for the licensees of software as liability serves the reparative function of compensating the victim of defective software. In addition, software liability also serves a preventative function in leading to more careful software design and testing. If licensors are permitted to disclaim any of the consequences of failed software, they will have an insufficient incentive to take remedial steps to improve their products and services.

Cybercriminals routinely exploit software holes or defects to launch denial of service attacks, to crash servers, disable anti-virus protection, conduct script insertion attacks, execute arbitrary code, bypass firewalls, alter e-mail headers, and obtain elevated privileges on computer networks. Security holes on Internet Explorer, for example, permit junk to be “installed on a user’s PC by merely visiting a single site”,⁶⁶ The number of malicious code reports skyrocketed from “just eight in 1988 to almost 53,000 in 2001”, and

64 Rustad, “Making UCITA More Consumer-Friendly”, 18 *J. Marshall J. Computer and Info. L.* 547, at p. 574 (1999) (citing survey of Computer Law Association members conducted by Michael Rustad and Cynthia Anthony).

65 Dobbs, *The Law of Torts* (2000), at p. 970.

66 Edelman, “Who Profits from Security Holes?” (visited 26 November 2004), at http://www.benedelman.org/news/111804_1.html.

the spread of viruses is not trending downward.⁶⁷ At present, software licensees are left without a meaningful remedy for the consequences of defective software that enables cybercrime. The authors note that the purchaser's contributory actions may exacerbate software failure.

One of the difficulties in developing software law with teeth is that this intangible is neither a product nor goods. Software is licensed, not sold like other products. "Software licenses do not transfer title and only the right to use information. Software contracts, access contracts, multimedia contracts, anti-viral products and services, and a multitude of other products are licensed."⁶⁸ The installation of network security may involve the sale of goods, the licensing of software, and the expert services of computer engineers.

The present legal environment does not make vendors accountable for the consequences of marketing defective software. In business-to-business transactions freedom of contract is the prevailing ideology. However, apart from the United States, many countries place limits on the vendor's power to limit or exclude warranties or remedies. The authors discuss possible warranty remedies for off-the-shelf (mass-market) software as well as products for the business-to-business marketplace. The Finnish attorneys draw on developments from Finland, France, Germany, and the United States in concluding that vendors' liability for software is undeveloped, outside of the law of warranties.

At present, vendors have no tort liability for marketing products with known vulnerabilities. Each system surveyed provides contractually based remedies for defective software. However, the content of the protection offered licensees is not uniform. The authors call for an international treaty to harmonize remedies for defective software.

1.04 Harmonized Intellectual Property

(a) Protecting Digital Content in the Global Information Economy

Dana Beldiman raises the difficult policy issue of how to protect digital property rights on the Internet. The threat of the uncontrolled dissemination of copyrighted material led the information industries to lobby Congress for stronger intellectual property protection. Congress has enacted several

67 Gelbstein and Kamal (United Nations ICT Task Force), "Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security" (2002) (visited 24 November 2004), at http://www.itu.int/wsis/docs/background/themes/security/information_insecurity_2ed.pdf.

68 A license is permission to use information under restricted conditions, such as the software, in only one single-user computer. A sale, in contrast, involves the passage of title to goods for a price. Software does not require a fixed inventory or even raw materials. There is an infinite supply of "1s" and "0s", and they may be delivered without passing title. Licenses are based on the number of copies licensed, the method of distribution, the type of end user, and the form of the license agreement.

statutes increasing the power of the “haves” in cyberspace.⁶⁹ *America Online*,⁷⁰ *Playboy Enterprises*,⁷¹ *Verizon*,⁷² *Universal Studios*,⁷³ and *Microsoft*⁷⁴ are typical of large Internet stakeholders that have litigated aggressively to solidify their market position in cyberspace.⁷⁵ Beldiman’s chapter surveys the legal and technological measures developed to protect copyrighted content on the Internet and how this affects the interests of powerful media.

She examines three means of protection of digital information, namely:

1. Copyright law;
2. The technology itself; and
3. Other legal responses.

69 The only significant consumer victories have been cases where the government was the prevailing plaintiff, not individuals. *Time Warner Entertainment Co. v. FCC*, 2001 U.S. App. LEXIS 3102 (D.C. Cir., 2001) (ruling in favor of the FCC imposing limits on cable system and channel capacity). *Ford Motor Co. v. Texas DOT*, 106 F. Supp. 2d 905 (W.D. Tex., 2000) (ruling in favor of Texas state governmental unity in cases involving the sale of used automobiles on the Internet); *State of Missouri ex rel. Nixon v. Beer Nuts Ltd.*, 29 SW3d 828 (Mo. Ct. App., 2000) (upholding Missouri ban on the online sale of beer to Missouri residents); *FTC v. Dell Computer and Micron Electronics*, FTC File Number 982 3563; FTC File Number 982 3565 (1999) (entering consent order against computer companies).

70 *America Online, Inc. v. Huang*, 106 F. Supp.2d 848 (E.D. Va., 2000); *America Online, Inc. v. IMS*, 24 F.Supp.2d 548 (E.D. Va., 1998); *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp.2d 444 (E.D. Va., 1998); *America Online, Inc. v. National Health Care Discount, Inc.*, 174 F. Supp.2d 890 (N.D. Iowa, 2001); *America Online, Inc. v. Prime Data Systems, Inc.* 1998 W.L. 334016692 (E.D. Va., 1998); *America Online, Inc. v. Superior Court*, 108 Cal. Rptr. 2d 699 (Cal. App., 1 Dist., 2001).

71 *Playboy Enterprises, Inc. v. Asiafocus Intern., Inc.*, 1998 W.L. 724000 (E.D. Va., 1998); *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla., 1993); *Playboy Enterprises v. Netscape Communications Corp.*, 55 F. Supp.2d 1070 (C.D. Cal., 1999); *Playboy Enterprises v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503 (N.D. Ohio, 1997); *Playboy Enterprises v. Terri Welles Inc.*, 78 F. Supp. 2d 1066 (S.D. Tex., 1997); *Playboy Enterprises, Inc. v. Webworld, Inc.*, 991 F. Supp. 543 (N.D. Tex., 1997).

72 *RIAA v. Verizon Internet Services*, 2003 U.S. App., Lexis 25735; C.A. 2-MS-0323 (D.D.C., 2002).

73 *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211 (S.D.N.Y., 2000); *RIAA v. MP3.com*, 2000 US. Dist. LEXIS 5761 (S.D.N.Y., 2000).

74 Microsoft is a frequent defendant as well as plaintiff in Internet-related cases. *United States v. Microsoft Corp.*, 253 F3d 34 (D.C. Cir., 2001); “Microsoft Sues Online Pirates”, *Wired News* (8 December 1999), with “Priceline.com Files Suit against Microsoft”, *CNET.com* (visited 11 October 2004), at <http://news.com.com/2100-1001-231384.html?legacy=cnet>.

75 Fortune 500 bricks-and-mortar companies also have been active in cyberspace litigation. *Ford Motor Co. v. Lane*, 67 F. Supp. 2d 745 (E.D. Mich., 1999); *Sony Computer Entertainment v. Connectix Corp.*, 48 F. Supp. 2d 1212 (N.D., 1999); *Sega Entertainment, Ltd. v. Maphia*, 857 F. Supp. 679 (N.D. Cal., 1994), modified, 948 F. Supp. 923 (N.D. Cal., 1996); *Mattel, Inc. v. Adventure Apparel*, 2001 U.S. Dist. LEXIS 13885 (S.D.N.Y., 2001); *Mattel, Inc. v. barbie-club.com*, 2001 US. Dist. LEXIS 5262 (S.D.N.Y., 2001); *Cable News Network LP, LLLP v. cnnnews.com*, 162 F. Supp. 2d 484 (E.D. Va., 2001); *Lockheed Martin v. Network Solutions*, 141 F. Supp. 2d 648 (N.D. Tex., 2001); *E and J Gallo Winery v. Spider Webs LTD, et al.*, 129 F. Supp. 2d 1033 (S.D. Tex., 2001); *Fleet Boston Financial Corp. v. fleetbostonfinancial.com*, 138 F. Supp. 2d 121 (D. Mass., 2001); *Harrods Limited v. Sixty Internet Domain Names*, 110 F. Supp. 2d 420 (E.D. Va., 2000); *Caesars World, Inc. v. Caesars-Palace.com et al*, 2000 U.S. Dist. LEXIS 2671 (E.D. Va., 3 March 2000).

The Digital Millennium Copyright Act (DMCA) is an example of a third tier response. It provides Hollywood with new weapons to battle the downloading of copyrighted music and images by college students.⁷⁶

So too, the Anti-Cybersquatting Consumer Protection Act of 1999 (ACPA) was enacted to deter the unauthorized registration or use of trade marks as Internet domain names.⁷⁷ The ACPA addressed the problem of dot.com startups and cyberpirates who registered domain names that were confusingly similar or identical to well-known marks. In addition to domestic statutes, stakeholders are protected by World Intellectual Property Organization (WIPO) treaties.

Civil code countries such as France, Germany, and The Netherlands are pursuing a different legal path forging a different balance between intellectual property stakeholders and the public interest, the trend of United States copyright law. The Dutch, for example, generally regard online music swapping as non-infringing. The networked world is causing a clash between litigants from radically different legal traditions. A French court ruled that radio stations may not stream musical extracts on their websites without the express permission of music producers. This producers' right to control communications to the public was decided under the French Intellectual Property Code.⁷⁸ On the other hand, a United Kingdom court held that a British Internet café chain infringed United Kingdom copyright law by providing a commercial service for downloading music onto recordable CDs for customers.⁷⁹

The Internet will increasingly involve crossborder contractual disputes, such as in *Profile Publ'g and Mgmt. Corp. APS v. Musicmaker.com*,⁸⁰ which pitted the Danish owner of musical recordings by the musical group The Who against a website providing consumers with custom disc compilation services. Musicmaker, which owned and operated an Internet website, had no permission to copy digital musical recordings on compact discs. When threatened with a lawsuit, Musicmaker.com entered into an agreement to

76 The DMCA arms the entertainment industry with new remedies against using circumvention devices designed to decrypt the contents of DVDS that are cosseted by a Content Scramble System (CSS). The peer-to-peer file sharing movement on the Internet pits the movie, record, and film industry against Internet users. In *A and M Records, Inc. v. Napster, Inc.*, 239 F3d 1005 (9th Cir. 2001), the Ninth Circuit upheld a federal court order enjoining Napster for facilitating the wholesale copying of music on its service. *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp.2d 211 (S.D.N.Y., 2000) (enjoining websites from posting the Decks software which circumvents software controls on DVDs).

77 15 United States Code, section 1125(d) (2004).

78 *Société des Producteurs de Phonogrammes en France Union des Producteurs Phonographiques Francais Independants, Tribunal de Grande Instance de Paris* (15 May 2002), reported in 2002 ILRWeb PandF 1713 (2002).

79 *Sony Music Entertainment (UK) Ltd. v. Easyinternetcafe Ltd.*, H.C. 2 C01798 (High Court of Justice, Chancery Division, 30 January 2005), reprinted at 2005 ILRWeb (PandF) 1055 (2005).

80 *Profile Publ'g and Mgmt. Corp. APS v. Musicmaker.comProfile*, 2005 U.S. Dist. LEXIS 991 (S.D.N.Y., 24 January 2005).

pay royalties. After Musicmaker.com shut down its website, it failed to pay the full amount of royalties due. The court ordered them to honor their installment contract and assessed sanctions against the company and its attorneys for frivolous counterclaims and defenses.

Courts outside the United States may not be as receptive by attempts by large corporations to “push the envelope” by asserting an ever-expanding array of intellectual property rights. Beldiman’s chapter begins with a lucid discussion of the United States approach to digital rights protection. Powerful United States copyright owners seek to “keep the cat in the bag” and yet participate in the new networked economy where information is transferred seamlessly at the click of a mouse. Beldiman argues that it is difficult to protect digital content while permitting the unfettered distribution of content. She argues that copyright law provides a strong, but not an absolute protection in the digital world. The critics of the United States approach argue that the copyright moguls such as Hollywood and the recording industry are “pushing the envelope” on protecting content, which critics describe as “simple overreaching”. Beldiman explains the opposing views in copyright law as part of the growing pains of a new emergent copyright paradigm.

Beldiman’s chapter clearly explains content protection technologies, privacy enhancing technologies, payment mechanisms, and other rights management that depends on legal norms against anti-circumvention. The entertainment industry has pressed for increasing civil and criminal penalties for those seeking to circumvent digital rights management software. She reviews the Digital Millennium Copyright Act or the DMCA, which was a byproduct of the 1996 WIPO Copyright Treaties. Movie producers, for example, lobbied for the passage of the Digital Millennium Copyright Act,⁸¹ providing remedies against circumventing copyright protection software used in distributing Digital Versatile Discs (DVDs).⁸² Next follows a discussion of the logic and the limits of the DMCA comparing United States law to the EU Copyright Directive.

The Beldiman chapter concludes with a synoptic survey of other law governing digital content as well as a discussion of emergent business models which will likely reshape global copyright law. The global rules for streaming media broadcast and entertainment transmitted digitally over the Internet are presently being negotiated between stakeholders and the government. He hypothesizes that the DMCA and other copyright law will become less important as new technologies evolve, such as the globalized “pay per use” system of commercializing and protecting digital content.

81 Pub. L. Number 105-305, 112 Stat. 2860 (1998).

82 “On 12 October 1998, Congress passed the Digital Millennium Copyright Act (DMCA), a complex piece of legislation which makes major changes in United States copyright law to address the digitally networked environment”. Band, “The Digital Millennium Copyright Act” (visited 11 May 2005), at <http://www.arl.org/info/frn/copy/band.html>.

(b) Towards a Globalized Fair Use Standard

Jon Grossman and Elizabeth Parsons examine the problem of developing an international fair use standard. Their chapter pays particular attention to the path of United States copyright law focusing on the difficult topic of fair use. The chapter surveys governmental as well as industry approaches to fair use for digital information. Finally, the chapter suggests the need for a new international standard for copyright protection and identifies factors that should comprise the cross-border fair use rules.

In December 2002, WIPO released a report, “Intellectual Property on the Internet: A Survey of Issues”, that examines the impact of the globalization of the Internet on intellectual property rights. WIPO argues for expanded protection for digital technologies in rights to “copyrights, trade marks and patents, as well as domain names. The WIPO report explores the particular concerns that face developing countries in e-development, and outlines the ways in which WIPO is addressing these various issues”.⁸³

The advanced industrial nations control many of the digital technologies, and WIPO’s proposed treaty process is a tool for extending intellectual property rights of the cyberspace core⁸⁴ into the semi-periphery and periphery.⁸⁵

83 World Intellectual Property Organization, *Intellectual Property on the Internet: A Survey of Issues* (December 2002) (visited 28 January 2005), at <http://ecommerce.wipo.int/survey>.

84 Sociologist Immanuel Wallerstein conceptualized the “world system” to explain why European countries arose to world dominance in the period 1300–1450. Wallerstein, *The Modern World System I: Capitalist Agriculture and the Origins of The European World Economy in the Sixteenth Century* (1974). Wallerstein’s model defined the first core nations as England, France, and Holland in northwestern Europe. Core countries have a lasting advantage because they develop the new technologies first and use their expertise to dominate periphery and semi-periphery countries economically, militarily, and culturally. In the 16th Century, the core states “developed strong central governments, extensive bureaucracies, and large mercenary armies”. *Modern History Sourcebook: Summary of Wallerstein on World System Theory* (13 June 2001) (visited 2 February 2005), at <http://www.fordham.edu/halsall/mod/wallerstein.html>. The core countries used their technological superiority to expropriate the resources of the less-developed countries. Nations with sufficient expertise and other resources to partially resist appropriation are defined as satellite or semi-periphery countries. By the 16th Century, the semi-periphery included declining core nations, such as Spain and Portugal as well as Italy, southern Germany, and southern France, which had yet to attain core status. Finally, the 16th century periphery consisted of nations in Eastern Europe, Africa, and Latin Africa, which had little or no ability to resist the demands of the core states. Today, the core nations of the networked world are the United States, Canada, the countries of Western Europe, Japan, South Korea, Australia, and New Zealand. This core of Internet-user nations have a significant advantage over less-developed countries with low numbers of Internet users and hosts, low percentage of personal computers, and poorly developed cyber-infrastructure.

85 The United States sought to negotiate a 20-year copyright term extension with Taiwan which would bring the total copyright term to 70 years, but Taiwan has yet to accede to this request. Reuters, “Taiwan Rejects U.S. Copyright Demands” (visited 17 February 2005), at <http://www.siliconvalley.com/mld/siliconvalley/news/editorial/4260499.htm>.

The policy concern is that too much control would stifle the creative commons. Grossman and Parsons compare the United States doctrine of fair use to approaches found in European countries. The creation of an international “fair use” standard is needed in an age of seamless access to digital copies. The challenge in developing this new standard is to appropriately balance the rights of digital intellectual property owners with the rights of other stakeholders.

(c) Towards a Globalized Regime for Domain Names

Frederick Roos proposes the further legalization of domain names. Roos begins his chapter with a discussion of how domain names clash with the trade marks of powerful corporations. In the early 1990s, cyberspace was referred to as the Wild West because predatory entrepreneurs staked out the domain names containing trade marks of distinctive or internationally known companies and held them for ransom. Roos discusses the unsavory practices of cybersquatting, warehousing, and misspellings, as well as the misuse and abuse of “expired” domain names.

According to Roos, cyberpirates warehoused thousands of domain names with no intention of ever launching a website. The business of warehousing domain names was to place the domain name on the market for the highest bidder or to extort a multi-million dollar settlement from a national company. In addition, the author discusses the difficult problem of “gripe-sites”, which is an issue that places trade mark rights in conflict with the right of expression.

In the United States, information age moguls convinced the United States Congress to fortify the rights and remedies of famous and distinctive trade mark owners. Domain name defendants have responded by becoming more creative in misusing and abusing domain names. In a recent case, an adult entertainment company modified a domain address to “surreptitiously . . . re-direct traffic” for www.sexnet.com to its address — a practice known as “domain name hijacking”,⁸⁶ Internet predators make profits from their callous calculation that many Internet surfers will mistype domain name addresses. These “entrepreneurs” register the most common misspellings of well-known trade marks to divert unwary users to their nefarious sites.

Roos discusses how “mouse trapping” involves capturing the careless typist to the website of a competitor or to a pornography haven with no exit. Like

86 *Telemedia Network v. Sunshine Films Inc.*, 2002 Cal. App. unpub. LEXIS 10369 (Ct. of App. Ca., 13 November 2002) (describing hijacking “as the defendant surreptitiously . . . re-directing traffic” for www.sexnet.com to Sunshine’s address — in effect “hijacking” the [sexnet.com](http://www.sexnet.com) domain name using the Sexnet mark. As a result, any customer attempting to access Sexnet would be sent automatically to a website operated by Sunshine but with no content).

the Roach Motel, entrance into these unsavory sites is easy, but escaping them is made all but impossible by resourceful programmers. Attempts to leave are thwarted by software commands that control the computer's back browser and enmesh the victim ever more deeply into a web of pop-up advertising.

He describes how European courts, as well as those in China, are devising different solutions to the problem of domain names. He surveys alternative dispute resolution systems, such as the ICANN system as well as new legislation and rules for resolving domain name disputes. Sweden, for example, has recently abandoned its domain name registration system based on entitlements to a more modern system.

Roos critiques the Swedish domain name registration system that was based on "prior assessment". The author next turns to the domain name registration systems of individual countries that have led to a balkanization of country-wide registrations. A strong convergence between the United States and European law of domain names has resulted from the internationalization of dispute resolution.

The author next critiques the role of the ICANN and UDRP dispute resolution system that has evolved since the late 1990s. The Internet Corporation for Assigned Names and numbers (ICANN), created in 1998, has responsibility for technical functions of the Internet. ICANN coordinates the assignment of IP address numbers, protocol parameter and port numbers, and the stable operation of the Internet's root server systems.⁸⁷ ICANN states that it:

... is the global forum for developing policies for coordination of some of the Internet's core technical elements, including the domain-name system (DNS). ICANN operates on the basis of consensus, with affected stakeholders coming together to formulate coordination policies for the Internet's core technical elements in the public interest.⁸⁸

The Internet Assigned Numbers Authority (IANA) delegates or redelegates top-level domains and manages the domain-name system root.⁸⁹ The registration of domain names within two-letter country code top-level domains (CCTLDS), such as ".uk" (United Kingdom), ".se" (Sweden), or ".au" (Australia), are administered by country-code managers.⁹⁰

87 Internet Corporation for Assigned Names and Numbers, "Introduction to ICANN" (visited 2 February 2005), at <http://www.icann.org/>.

88 Internet Corporation for Assigned Names and Numbers, "ccTLD Resource Materials" (2 February 2005), at <http://www.icann.org/cctlds/>.

89 Internet Assigned Names Authority, "IANA Report on Redlegation of the la Top-Level Domain" (visited 2 February 2005), at <http://www.iana.org/reports/la-report-11dec02.htm>.

90 Internet Corporation for Assigned Names and Numbers, "ccTLD Resource Materials" (2 February 2005), at <http://www.icann.org/cctlds/>.

The Internet domain name system consists of a directory, organized hierarchically, of all the domain names and their corresponding computers registered to a particular com. All accredited domain-name registrars for domain names ending in “. com”, “.net”, and “.org” are required to adhere to the Uniform Dispute Resolution Policy (UDRP). The UDRP is a good example of legalization. The UDRP’s crossborder dispute resolution system offers a cost-effective solution for resolving cybersquatting or cyberpiracy claims. When a United States company applies for a domain name (or renews it), they are asked to represent that the registration of the domain name will not infringe the intellectual property rights of others.⁹¹ All domain name registrants, wherever they are located, submit to the virtual UDRP dispute resolution system.

The Max-Planck Institute completed a content analysis of the first generation of cases decided under the UDRP procedure between 1999 and 2001.⁹² The researchers found that UDRP panels ordered transfers of domain names in 76.7 per cent of the cases and cancellations in 1.4 per cent of the cases. Complaints were dismissed in only approximately 21 per cent of the cases. Results varied significantly by provider. Complainants prevailed 82 per cent in decisions rendered by WIPO panels in contrast to only 59 per cent before the now defunct eResolutions. Eighty-four percent of the complaints were filed by registered trade mark owners.

The Max Planck study confirms the Swedish author’s thesis that further legalization is required. A globalized solution to domain names must successfully balance intellectual property rights against the right of expression. The lack of predictability, legitimacy, freedom of speech, and conflicting norms in different countries remain obstacles in arriving at a global solution. The author surveys ways that domain name governance is being deployed in the battle against crossborder spam.

91 “By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that (a) the statements that you made in your Registration Agreement are complete and accurate; (b) to your knowledge, the registration of the domain name will not infringe on or otherwise violate the rights of any third party; (c) you are not registering the domain name for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable laws or regulations. It is your responsibility to determine whether your domain name registration infringes or violates someone else’s rights.” ICANN, Uniform Dispute Resolution Policy (visited 17 December 2004), at <http://www.icann.org/dndr/udrp/policy.htm>.

92 Kur, Max Planck-Institute, Munich, “UDRP: A Study by the Max-Planck-Institute for Foreign and International Patent, Copyright, and Competition Law” (in cooperation with the Institute for Intellectual Property Law and Market Law, University of Stockholm and Institute for Information Law and Technical University of Karlsruhe (Germany) (visited 18 December 2005), at <http://www.intellecprop.mpg.de/Online-Publikationen/2002/UDRP-study-final-02.pdf>.

The author's magisterial survey confirms that we are a long way to developing an effective global regime for domain names. Any solution to the domain name problem will need to consider radically different cultures and norms as well as the semantic meaning of trade marks in different languages. Participants in the WSIS consultation process "agreed that spam unsolicited or 'junk' e-mail while not yet officially on the international agenda, must be discussed as a matter of priority".⁹³ The battle to restrain spam and online pornography is leading to greater international cooperation in the field of domain names.

(d) Patent Law for a Global Information Age

David Simonelli examines the difficult problem of internationalizing patent law. He begins by comparing patent protection to that of copyright and trade mark law. Every introductory patent textbook begins with the aphorism that a patent is a monopoly granted for a limited period. The United States law of patents began in 1790 when the United States Secretary of State Thomas Jefferson granted the first United States patent for a method of making potash, which is an ingredient for soap. Simonelli questions whether Jefferson had a monopoly in mind in his concept of patent law.

In fact, Simonelli quotes Jefferson who hoped that the United States' capitalist system would soon rid the economy of all forms of monopolies. Simonelli also dismantles the conventional wisdom that patents should give patent holders a monopoly. He notes how patent law's "monopoly" is subject to doctrines such as the compulsory licenses. Patent law, like every other branch of intellectual property, balances the public's rights against the owner of the intellectual property right.

With copyright law, the exclusive rights of the owner are moderated by the doctrine of fair use. Trade mark owner's rights are subject to the doctrine of parody and fair use, among other limitations. Each branch of intellectual property in the information-based world system must balance the need to protect proprietary rights against the public interest in access to information.

Simonelli suggests that the United States-style patent monopoly places less developed countries at a disadvantage. He suggests ways to protect patent rights while permitting pharmaceuticals and other patents to be used in Third World countries. He proposes a new institution that balances patent owners' rights with the rights of the periphery and semi-periphery countries to have access to medical products and processes, and suggests that an international entity be formulated that would certify Third World entity status.

93 "UN E-Governance Panel Focuses on Spam, Web Governance", *D.M. Europe* (21 April 2005).

Another possibility would be to mandate compulsory licenses for Third World entities. He uses the concept of “permissive infringement” to recognize the need for Third World countries to innovate and grow. Simonelli’s proposal recognizes the responsibility of core countries to periphery and semi-periphery countries. Nevertheless, his proposal is only the first step in developing a global regime.

United States patent law conflicts with many of the basic features of the law of patents found in the rest of the world. The United States Patent and Trade Mark Office grants patents to the first person to invent, whereas the rest of the world awards patents to the “first to file” the patent application.⁹⁴ To date, WIPO has been unable to negotiate a treaty to harmonize these divergent patent laws.⁹⁵ The United States has recently become a member of the Patent Cooperation Treaty (PCT) that permits the filing of a single international patent application. The PCT permits individuals and companies within member countries or regional patent systems to file a single patent application in one member country and then file a second patent application in a second country, within the first year of filing, and have the benefit of priority.⁹⁶

The European system of patents not only recognized national patents, but a relatively new European patent granted by the European Patent Office in Munich. The European patent system was created by article 237 of the EC Treaty.⁹⁷ The European Patent Convention provides protection to patent holders in member states for a term of 20 years.

The Europeans have lagged behind the United States in developing patents for e-commerce. In contrast, e-commerce patents have skyrocketed since the United States federal court decision in *State Street Bank and Trust Co. v. Signature Financial Group, Inc.*⁹⁸ The United States was the first country to recognize e-commerce or business methods patents which are not yet recognized in Europe. No European country has yet to issue patents for Internet-related business methods.

94 International Chamber of Commerce, “Current and Emerging Issues Relating to Specific Intellectual Property Rights” (visited 3 March 2005), at http://www.iccwbo.org/hom/intellectual_property/current-emerging/roadmap.asp.

95 International Chamber of Commerce, “Current and Emerging Issues Relating to Specific Intellectual Property Rights” (visited 3 March 2005), at http://www.iccwbo.org/hom/intellectual_property/current-emerging/roadmap.asp.

96 Kirsch, “Strategies for the Use of Patents by Start-Up Internet Companies”, *Gigalaw.com* (visited 3 March 2005), at <http://www.gigalaw.com/articles/kirsch-2000-07-p5.html>.

97 The European Commission, Internal Market, Patents-Commission Approves Green Paper (25 June 1997 (visited 3 March 2005), at http://europa.eu.int/comm/internal_market/introp/indprop/558.ht.

98 *State Street Bank and Trust Co. v. Signature Financial Group, Inc* 149 F3d 1368 (Fed. Cir., 1998) (ruling that a mathematical algorithm used in a mutual fund hub and spoke business method for computing interest in mutual funds produced “a useful, concrete and tangible result”).

Software patents are not well-established in some countries. The United Kingdom's Patent Office issued a report rejecting patent protection for computer software as well as for methods of doing business.⁹⁹

A proposed European Directive would “harmonize the conditions for the patentability of inventions related to computer programs”.¹⁰⁰ Recently, the European Commission has suspended further development of the new Directive on software patents. Although European patent protection for software or methods of doing business is not well-established, enforcement of patent rights is robust.

In a United Kingdom case, the High Court rejected an argument that British bookmakers were not infringing a gaming system patent simply because their host computers were in the Netherlands Antilles.¹⁰¹ Patent litigation rules vary significantly across European countries. In Germany, there is no discovery but, in France and Italy, the court can order the inspection of the premises in a patent case.¹⁰²

The underlying jurisprudence behind patent law varies. In France and England, the theory is that a patent represents a contract between society and the inventor.¹⁰³ The German view, in contrast, is paternalistic and “[p]atents are granted because the state has decided, in its wisdom and part of the exercise of its power as *parens patriae*”.¹⁰⁴ Simonelli's chapter signals the need for a harmonized patent law for the global information society.

(e) Resolving Disputes over Information Transfers

Mark Nadeau's survey of the law of technology transfers suggests the need for further legalization of the information-based world system. Increasingly, information and communication technologies (ICTs) are becoming the

99 The United Kingdom Patent Office, “Should Patents Be Granted for Computer Software or Ways of Doing Business: The Government's Conclusions” (visited 3 March 2005), at <http://www.patent.gov.uk/about/consultations/conclusions.htm>.

100 World Intellectual Property Organization, “What Is the PCT” (visited 3 March 2005), at <http://www.wipodot.org/pct/guide/en/gdvo11-01.htm>.

101 “British High Court Rules in Jurisdictional Dispute over Game System Patent”, 4 *Mealey's Litigation Report: Cyber Tech and E-Commerce* (April 2002).

102 Ladas and Perry, “Ladas and Perry Guide to European Patent Office Practice, Post-Grant Issues” (visited 3 March 2005), at <http://www.ladas.com/GUIDES/PATEN/EPOPractice/EOPractGuide-8.html>.

103 Ladas and Perry, “Ladas and Perry Guide to European Patent Office Practice, Post-Grant Issues” (visited 3 March 2005), at <http://www.ladas.com/GUIDES/PATEN/EPOPractice/EOPractGuide-8.html>.

104 Ladas and Perry, “Ladas and Perry Guide to European Patent Office Practice, Post-Grant Issues” (visited 3 March 2005), at <http://www.ladas.com/GUIDES/PATEN/EPOPractice/EOPractGuide-8.html>.

subject of crossborder disputes in the information age. This is because of the proliferation of online contracts, software licenses and other virtual practices over the Internet, which have a global reach. Without a reliable means to enforce rights and seek remedies, intellectual property rights will disappear with a click of the mouse.

Nadeau lays out the fundamental concepts underlying the resolution of intellectual property disputes and considers the various methods available for parties. He argues in favor of a less adversarial process than is found in most legal systems at present. As a result, he calls for a new international forum, created by international treaty, as many of the contributors also do for their respective areas of interest. This treaty would encompass a consistent set of rules for choice of law, enforcement of foreign judgments, and alternative modes of settlement for the parties to choose from prior to suit. Nevertheless, there are dimensions to this project that involve very real differences, in addition to those imposed by cyberspace.¹⁰⁵

(f) Data Base Protection and Privacy Regulation in a Global Economy

David Gryce and Roxanne A. Esche make it plain that any transborder legal regime governing databases also must protect privacy. Gryce and Esche review the concepts and methods of the Database Directive expertly describing key questions such as what protected data is and who can claim rights. They argue that intellectual property right holders need protection since they have invested significant resources in collecting information that they then store in electronic databases. Information must be protected to return value to the intellectual property right holder.

Gryce and Esche next review the legislative regimes that apply to protecting databases or proprietary data. Civil Law jurisdictions generally accord greater protection of personal data than the Common Law countries.¹⁰⁶ Finally, the authors propose specific database protection that will harmonize the law of databases. They endorse further international efforts to protect databases and privacy and see this balance as the key to seamless transborder data flows.

The balance between database protection and the free exchange of scientific or other data has yet to be achieved in many countries. In the United States, there is no copyright protection for databases that are mere compilations

105 Renteln, "Cross-Cultural Dispute Resolution: the Consequences of Conflicting Cultural Norms", 10 *Willamette. J. Int'l and Dispute Res.* 103 (2002).

106 Whitman, "The Two Western Cultures of Privacy: Dignity v. Liberty", *Yale Law School Public Law and Legal Theory Research Paper Series Number 64* (2004).

because they lack originality.¹⁰⁷ The information industry proposed database protection in the Conference Report for the Digital Millennium Copyright Act of 1998.¹⁰⁸

In contrast, the EU's 1996 Database Directive provides copyright protection for databases meeting the originality standard as well as a *sui generis* protection for non-original databases.¹⁰⁹ Copyright protection applies if the selection and arrangement of the data or contents' qualities as an original intellectual creation. In contrast, a *sui generis* term of protection for 15 years is granted to databases where there has been a substantial investment in obtaining, verifying, or presenting contents.

Europeans endorse the "sweat of the brow" theory, which is an approach not followed in the United States. In *British Horseracing Board Ltd., v. William Hill Organization Ltd.*,¹¹⁰ the court held that racing information compiled by a governing body of horseracing violated a horseracing body's *sui generis* database rights under EU law. The plaintiff maintained an extensive database of information on races, jockeys, owners, and other information that it supplied to the defendant. The defendant then began to use the horseracing body's database rights on its website. Absent a license agreement, there would be no cause of action in the United States for a similar usage. The radically different concepts of data protection found in the United States and Europe are a case in point for greater harmonization. It is instructive to note that the different approaches do not merely mirror the Common Law and Civil Law divide.

Another major difference between the United States and Europe is in data collection of personally identifiable information. The Europeans treat privacy as a fundamental human right versus the weak tradition of privacy protection in the United States. The United States approach to privacy has

107 Under United States copyright law, a work needs some minimum modicum of originality to qualify for copyright protection and a work is original if it was independently created by the author and possesses a minimum level of creativity. The United States Supreme Court ruled, in *Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 United States 340 (1991), that a telephone directory consisting of white and yellow pages lacked the minimum originality to receive copyright protection. The Court rejected a "sweat of the brow" theory that the time and effort in compiling and organizing a database satisfied the originality requirement.

108 Band, "Digital Millennium Copyright Act" (visited 3 March 2002), at <http://www.drfdot.org/issues/graphic/2281/JB-Index?JB-Memo/jb-memo.html>.

109 Directive 96/9/EC of the European Parliament and of the Council of March 1996 on the legal protection of databases: *Official Journal* L j077 of 27 March 1996 (396L009 (Database Directive)).

110 *British Horseracing Board Ltd., v. William Hill Organization Ltd.*, H.C. 2000 1335 (High Court of Justice, Chancery Division, 9 February 2001), reported in 8 *I.L.R.* (P and F 629 (2001)).

focused on a self-regulatory or market-driven approach¹¹¹ supplemented by statutory protection in sectors such as health care¹¹² and financial service.¹¹³

Since October 1998, the European member states have been implementing the Directive by enacting national legislation. The European approach to Internet privacy is a command and control model with precise rules governing the handling of personal information, in contrast to the United States which relies largely on a market-based solution to privacy.

In contrast, the purpose of the European Data Protective Directive is to create uniformity in the processing of personal information across member states.¹¹⁴ The Data Protection Directive gives data subjects control over the collection, transmission, or use of personal information. The data subject has the right to be notified of all uses and disclosures about data collection and processing.

Gryce and Esche examine the role of the Organization for Economic Cooperation and Development (OECD) in formulating guidelines for the protection of privacy in the context of transborder flows of personal data. Under the OECD principles, a company, for example, is required to obtain explicit consent as to the collection of data on race and ethnicity, political opinions, union membership, physical and mental health, sex life, and criminal records.

The EU's Data Protection Directive requires that personal information be protected by adequate security. Data subjects have the right to obtain copies of information collected as well as the right to correct or delete personal data. It is important that consent be obtained from the data subject prior to entering in to the contract.¹¹⁵ Data may not be transferred to other countries without an "adequate level of protection".¹¹⁶ EU member states are required

111 The authors' analysis of Federal Trade Commission cases shows that the Commission is stepping up its enforcement of online privacy. If a website has a privacy policy, but its information collection and use practices are inconsistent with that policy, the Commission has authority to investigate and restrain the misrepresentations in the privacy policy as unfair or deceptive trade practices. Nahra, "What Every Insurer Needs to Know About Privacy", *5 Mealey's Litigation Report: Emerging Insurance Disputes* 1 (8 November 2000).

112 The requirements of the Health Insurance Portability and Accounting Act (HIPPA) apply equally well to the Internet.

113 The requirements of the Gramm-Leach-Bliley Act focus on privacy protection for the individual customers of financial institutions. Nahra, "What Every Insurer Needs to Know About Privacy", *5 Mealey's Litigation Report: Emerging Insurance Disputes* 1 (8 November 2000).

114 The data protection traditions varied significantly across member states. Germany, France, and United Kingdom had a tradition of strong protection of privacy versus non-existent regulation in Greece. Mann and Winn, *Electronic Commerce* (2002), at p. 7.

115 Data Protection Directive, article 7.

116 Data Protection Directive, article 25.

to provide that a transfer of personal data to a third party takes place only if there is assurance of an adequate level of data protection. A company is civilly liable for the unlawful processing of personal data. Damages may be assessed for collection or transmitting information without data subject consent.¹¹⁷

The fundamental principles of United States privacy law are less developed outside the medical, financial services, and a few other sectors. Unlike Europe, there is no real codification of privacy rights in United States law. The Founders of the United States Constitution did not explicitly address privacy as a fundamental right.¹¹⁸ The American law of privacy has evolved in a crazy quilt of piecemeal statutes at the federal and state levels. The path of United States privacy law has been to limit governmental intrusion into a sphere of personal conduct and relations by defining the boundaries between the individual and the government.¹¹⁹

In contrast, the United States prefers that the business community develop industry standards, such as the Better Business Bureau's Online Privacy Seals or other certification programs. The United States seeks to develop a transnational online privacy seal that can be earned by adherence to industry norms.¹²⁰ The EU Data Protection Directive sought to establish a regulatory framework that would guarantee free movement of personal data. However, each individual is guaranteed a basic level of privacy by requiring each provider or transmitter to adhere to a set of guidelines.¹²¹

The Directive stated that organizations were forbidden to transfer personal information of Europeans unless the transferee complied with the notice and choice principles.¹²² Organizations were required to ascertain whether third parties subscribed to the principles of the Directive before transferring information to them. The authors note that, in the interconnected

117 Data Protection Directive, article 23.

118 "Constitutional privacy law has evolved largely from textual and inferential construction of the Bill of Rights; in particular, the First, Fourth, Fifth, and Ninth Amendments, as well as the Fourteenth Amendment." Schacter, *Informational and Decisional Privacy* (2005), at p. 8.

119 Schacter, *Informational and Decisional Privacy* (2005), at p. 25.

120 Rustad and Daftary, *E-Business Legal Handbook: 2003 Edition* (2005), section 8.02[D].

121 The legal grounds defined in the Directive are "consent, contract, legal obligation, vital interest of the data subject, or the balance between the legitimate interests of the people controlling the data and the people on whom data is held (i.e., data subjects)". European Commission Press Release: IP/95/822, Council Definitively Adopts Directive on Protection of Personal Data, 25 July 1995 (visited 3 March 2005), at http://www.privacy.org/pi/intl_orgs/ec/dp_EC_press_release.txt.

122 United States Department of Commerce, "Safe Harbor Privacy Principles" (visited 2 March 2005), at <http://www.export.gov/safeharbor/shprinciplesfinal.htm>.

information-based world economy, there is an increased danger that personal information will be misused or abused. Increasingly, the digital economy poses a risk that personally identifiable information is inaccurate or is intentionally misused by third-party cybercriminals. They note how the private/public split has become a false dichotomy with the distinction between commercial and government uses of personal information becoming blurred, increasing the possibility of the invasion of privacy and the loss of individual rights.

Few sectors of the American economy adhered to the minimum data protection principles which threatened to shut down large portions of the global information economy.¹²³ The United States Commerce Department negotiated a “safe harbor” with the EU by agreeing to adhere to reasonable precautions protecting data integrity.¹²⁴ Europeans generally find American industry offers insufficient protection for personal data.

The authors call for a transborder legal regime of intellectual property that strikes the correct balance between ensuring sufficient private returns on investment in innovations in exchange for the disclosure and diffusion of those new inventions. Without such a balance, there will be interruptions in data flow that will harm the world system.

1.05 Regulating the Global Internet

(a) Technology-Assisted Surveillance

Sajai Singh, Probier Roy Chowdhury, Armut Joshi, and Govind Naidu begin their chapter by introducing the concept of communications surveillance and its close cousin, physical surveillance. To understand the law of surveillance, one must understand cultural as well as technological developments. In the United States, as in Europe, greater surveillance has been justified on the grounds of crime control.

Their chapter examines the various arguments in favor of surveillance and reviews statutes governing surveillance from the United States, the United Kingdom, the EU, Canada, and India. The chapter also examines the objections to surveillance advanced by privacy advocates. Finally, the chapter

123 The Europeans were generally satisfied with privacy protection for the personal information of medical patients.

124 The United States is lobbying international organizations to convince them to adopt America’s self-regulatory approach to privacy. The United States is participating in the Platform for Privacy Protection (P3P), which is an industry standard developed by the World Wide Web Consortium that will enable visitors to express privacy preferences through their browsers; Third Annual Report, United States Government Working Group on Electronic Commerce (2000), at p. 40.

calls for greater balance between the right to conduct surveillance weighed against the individual right to privacy.

(b) Internet Regulation

Julian Ding attempts a global model of Internet regulation to reconcile the difficult problem of clashing regulatory regimes. He begins with the basic question of who should be the sovereign in cyberspace, the reasons for regulation, and the meaning of regulation. Governments race to regulate the Internet because of market failure, political pressure, and national self-interest. It is a consequence of the system of nation-states that individual regulation is often conflicting, overlapping, or leaves gaps. The decision in *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*¹²⁵ highlights the problem of asserting sovereignty in cyberspace.

In that case, Yahoo!, an Internet Service Provider (ISP), convinced a California federal court to declare another Internet-related judgment unenforceable in the United States. Originally, a Paris tribunal directed Yahoo! not to post any items of Nazi memorabilia for sale through its online auction network accessible in France. The United States federal court ruled that the action was not enforceable because it violated public policy protected by the First Amendment. The *Yahoo!* case is perhaps the best-known examples of how the Internet creates the potential for clashing legal norms.

Further international legalization is necessary to facilitate cross-border cooperation, to permit enforceable global jurisdiction, to collect monetary judgments, to enjoin defendants in off-shore havens, to pierce corporate veils designed to frustrate accountability, to harmonize dispute settlement systems, and to generally construct a supranational cyberspace law. The advanced-core industrial nations have entered an information age in which the entertainment and software industries are displacing the durable goods economy as a primary source of wealth and power. Information is the chief commodity of the new economy.

“Digital information can be perfectly copied and instantaneously transmitted around the world, leading many content producers to view the Internet as one giant, out-of-control copy machine.”¹²⁶ The information revolution has helped propel the field of intellectual property from a sleepy backwater of esoteric specialization into the center of public policy debates. The shape of intellectual property law will determine the ultimate winners and losers in

125 *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 169 FSupp. 2d 1181 (N.D. Cal., 2001).

126 Shapiro and Varian, *Information Rules, A Strategic Guide to the Networked Economy* (1998), at p. 4.

the world Internet economy. Global stakeholders are engaged in a protracted conflict over who shall determine the rules, norms, and decision-making processes for extracting value from consumers.

1.06 Conclusion

Internet law does not descend from the cyber heavens in the form of stone tablets.¹²⁷ It is a field more accountable to Darwin than to Newton, in that it is responsive to the felt needs of the networked world and continues to be in the process of becoming, rather than appearing against, a fixed horizon.

This volume confirms that the Internet is in the process of rapid legalization. The choices courts and legislatures make and the future they are forging will determine the path of global Internet law. The external view of the Internet as a network of users, and the internal view of cyberspace as a virtual reality, are competing models that offer insights for legal solutions to new problems. By considering both perspectives, it will be possible to forge new material and metaphoric tools to define the meaning of harm, property, premises, and persons in the information-based world system.¹²⁸

All of the core countries are facing functionally equivalent legal dilemmas: the protection of databases, illegal copying of computer games, software, the deep linking of websites, and the regulation of Internet lotteries, the privacy rights of ordinary citizens, the publicity rights of celebrities on the Internet. Courts throughout the core nations are grappling with the issue of whether mass-market licenses, such as click-wrap or shrink-wrap licenses, should be enforced and under what conditions.

What we know from the chapters in this volume is that no one core country can regulate the Internet or impose its norms on the semi-periphery and the periphery. The unilateral imposition of law will have a short and unhappy life, much like hatching sea turtles are devoured by everything from birds to mammals on shore and fish in the oceans.

The Internet, by its very nature, is multi- and trans- and inter-national, and it will require new global approaches to solutions, like those suggested in many of the chapters in this volume. One-billion Internet users worldwide will be online by the end of 2005, and the value of e-commerce was estimated to reach as high as US \$2.3-billion in 2002 and US \$3.9-billion by the

127 The authors are updating the famous Legal Realist aphorism of Felix Cohen. Cohen, "Transcendental Nonsense and the Functional Approach", 35 *Colum. L. Rev.* 809, at p. 834 (1935).

128 Frischmann, "The Prospect of Reconciling Internet and Cyberspace", 35 *Loyola U. Chicago L.J.* 205 (2003).

end of 2003.¹²⁹ The future path of Internet law will require greater convergence between the law of the core countries and a concerted effort to include the less-developed countries in law formation.

One possibility drawn from history, which would validate Maitland's original insight that we began with, might be to turn to the idea of the informal "law merchant" tradition, as a model of an original source of Internet law from which to analogize solutions on an *ad hoc* basis to particular problems. The law-merchant tradition, or *lex mercatoria*, refers to the customary rules and standards that apply universally to international trade.¹³⁰ The medieval fair was a precursor to the marketplace of towns, which is a precursor to the cross-border and virtual Internet marketplace.

A historical continuity between the medieval piepowder courts and Internet law can be drawn. Just as the law merchant was the source of law for negotiable instruments, bills of lading, warehouse receipts, and other commercial law devices, a new global law merchant must search for solutions for e-commerce, and do so quickly and satisfactorily to all. The advantage of the *lex mercatoria* of the medieval period was its speed, flexibility, and ability to decide disputes that crossed territorial borders. The new *lex mercatoria* of cyberspace must serve the same function for a future model for legalization.

Forging a transnational commercial law for cyberspace is necessary because of the great changes wrought by technology today, and is possible because of the same changes, that is, "practitioners and academics have at their disposal, by means of the internet, a highly accessible online working tool".¹³¹ Indeed, online dispute resolution already exists to meet the needs of parties who cannot have access to the same court.¹³²

The law of cyberspace requires a body of law with instant and easy access to its contents at any time and everywhere over the world.¹³³ The law of the global information economy must not be a treasure trove crammed full of useless legal artifacts preserving the past like a fly in amber.¹³⁴ Global information law must be a living law that takes into account radically different cultures and legal systems, and the radically different medium of the Internet, and the radically different experience offered us by cyberspace.

129 Reuters, "Internet, E-Commerce Boom Despite Slump" (visited 13 February 2005), at <http://economictimes.indiatimes.com/cms.dll/xml/comp/articleshow?artid=28739383>.

130 Trakman, *The Law Merchant: The Evolution of Commercial Law* (1983).

131 Berger, "Lex Mercatoria Online: The Central Transnational Law Database", at <http://www.tldb.de>.

132 Katsch and Rifkin, *Online Dispute Resolution: Resolving Disputes in Cyberspace* (2001); Rule, *Online Dispute Resolution for Business* (2002).

133 Berger, "Lex Mercatoria Online: The Central Transnational Law Database", at <http://www.tldb.de>.

134 Gilmore, "On the Difficulties of Codifying Commercial Law", 57 *Yale L.J.* 1341, at p. 1342 (1948).