1997

Law and Order in Cyberspace

Nick Allard
Brooklyn Law School, nick.allard@brooklaw.edu

David A. Kass

Recommended Citation
19 Hastings Communications and Entertainment Law Journal 563 (1997)

Law and Order in Cyberspace: Washington Report†

by
NICHOLAS W. ALLARD*
&
DAVID A. KASS**

Table of Contents

---

† An earlier version of this Article was presented at the *Hastings Communications and Entertainment Law Journal*'s Ninth Annual Computer Law Symposium, University of California, Hastings College of the Law, February 1, 1997. The views expressed in this review are those of the authors and do not necessarily represent those of any client or any other party.

* Latham & Watkins, Washington, D.C. J.D., Yale University, 1979; B.A., Oxford University, 1976; A.B., Princeton University, 1974. Mr. Allard is a member of the *Comm/Ent* Advisory Committee and is a frequent contributor to *Hastings Comm/Ent.* He is especially grateful for the friendship and tireless efforts of his co-author.

** House Government Reform and Oversight Committee. J.D., Duke University, 1995; A.B., Duke University, 1992. Mr. Kass participated in the Computer Law Symposium and co-authored this article while an attorney at Latham & Watkins, Washington, D.C.

Introduction

Our subject, Law and Order in Cyberspace, grows each day as policymakers, legislators, judges, and prosecutors scramble to address an explosion of legal issues presented by advanced communications and information technology. When you conduct business or interact with people using 19th and 20th century lines of communication, the activity is governed by an array of civil and criminal laws. But if you slip through a wormhole into the parallel world of cyberspace,[1] it is not

1. The term "cyberspace," a word which did not appear in dictionaries less than a decade ago, is not nearly as hackneyed as the mother of all modern metaphors, "Information Superhighway." Cyberspace is a term, however, of varying and sometimes elusive meaning. "Cyber" now serves as the prefix for anything modern and computerized, from "cybersurfing" to "cybergadgets." In fact, a brief NEXIS search for words with the prefix "cyber" revealed cyberwords ranging from the mundane (cyberland, cybertypes, cyberpunk) to the absurd (cybersax, cyberhell, cyberhip, cyberbask).

Author William Gibson is widely credited with coining the term cyberspace in his 1986 novel *Neuromancer.* However, the meanings of the word remain unsettled. Some commentators have thought of cyberspace as a compilation of wires, fiber-optic cables, telephones, satellites, and antennae. However, this view ignores the information, the substance that makes up cyberspace. Others see cyberspace as a "virtual space" where certain activities occur. One commentator in this school sees cyberspace as:

> a completely spatialized visualization of all information in global information processing systems, along pathways provided by present and future communications networks, enabling full copresence and interaction of multiple users, allowing input and output from and to the full human sensorium, permitting simulations of real and virtual realities, remote data collection and control through telepresence, and total integration and intercommunication with a full range of intelligent products and environments in real space.

Dan L. Burk, *Patents in Cyberspace: Territoriality and Infringement on Global Computer Networks,* 68 TUL. L. REV. 1, 3 n.9 (1993) (quoting Marcus Novak, *Liquid Architectures in Cyberspace, in* CYBERSPACE—FIRST STEPS 225 (Michael Benedict ed., 1991)).

Other commentators view cyberspace as a "marketplace for virtually all goods and services." Stephen P. Johnson, *Planning for the Next Century in the California Courts,* 66 S. CAL. L. REV. 1751, 1751 (1993). Still others define cyberspace as including "all electronic messaging and information systems [and] research data networks." Anne M. Fulton, *Cyberspace and the Internet: Who Will Be the Privacy Police?,* 3 COMMLAW CONSPECTUS 63, 63 (1995)(footnotes omitted).

John Deutch, the former Director of Central Intelligence, has weighed in on this issue as well. According to Deutch, research performed by the Central Intelligence Agency (CIA) has:

> revealed that the term "cybernetics" was coined by the Father of Cybernetics, Norbert Wiener, in 1948. In Mr. Weiner's words, "we have decided to call the entire field of control and communication theory, whether in the machine or the animal, by the name cybernetics, which we form from the Greek *kyberneies* or 'steersman.'"

The Department of State concurred with CIA's findings but wished to point out that the Greek *kybernetes* is related to the Latin *gubernator*, meaning "steersman" or "governor." The Defense Intelligence Agency is not yet ready to make a judgment and is exploring the possibility that "cyber" may have come from the Greek *kybisterer* or "diver," from which we also derive the

so clear what rules do or ought to apply. The relatively legally unfettered frontier of cyberspace is showing the strains of a commercial gold rush.[2] It often resembles wild west boomtowns, populated with earnest PC pioneers and homestead users, Internet preachers, copyright rustlers, perverts, scam artists, and plain old crooks. There also will be some ghost towns if any of the early goldmines go bust, or if entrepreneurial prospectors continue to lose their shirts on attempts to make anything other than e-mail and entertainment pan out. And as in the old west territories, the first outpost of law and order is the federal judge, whose episodic justice sometimes encourages the bad guys because it reminds them of the infrequency of hangings. In the 104th Congress, there were several relatively minor initiatives designed to deal with this phenomenon. For

---

work "cybister" or "a genus of large diving beetles." Letter from John Deutch to Sen. Sam Nunn, June 22, 1996, *reprinted in* S. Hrg. 14-701, at 511.

Perhaps the best, and simplest, definition for cyberspace views it as a place where information exists accessible to electronic transmission. This definition includes more than just the wires and circuits of communication and conveys that cyberspace is at its essence information that is accessible by special means. At present, there is no generally applicable federal statutory definition of the Internet. KEVIN WERBACH, FCC OFFICE OF PLANS AND POLICY, DIGITAL TORNADO: THE INTERNET AND TELECOMMUNICATIONS POLICY 12 (1997). Werbach's paper, which is part of the OPP's working paper series, discusses the history of the Internet and makes tentative conclusions about the FCC and government roles in regulating it.

2. Microchips, unknown to the vacuum tube days of ENIAC, the first modern general purpose computer, power an almost trillion dollar computer industry today. In the United States alone, 40% of households own a PC, 20% have access to the Internet, and consumers now spend more on computers than televisions. Andrea Stone, *Life Begins to Compute*, USA TODAY, Feb. 14, 1996, at 2A. By the end of 1995, there were more than 152,000 registered commercial web sites, and new sites have been added at the rate of 2,000 per week, suggesting that today there are more than 250,000 sites. Richard Harwood, *Speculating in Cyberspace: Will it Pay Off*, WASH. POST, Jan. 23, 1997, at A17. A year later, Network Solutions, Inc., the government authorized private registry of e-mail and World Wide Web addresses, which planned to handle 10,000 registrations a month, is now registering above 85,000 new addresses per month—and losing money in the crush! David S. Hilzenrath, *Masters of Internet Domains Says it Loses at Monopoly*, WASH. POST, Jan. 24, 1997, at D1. In finance, digital communications networks move more than $2 trillion a day. Andrea Stone, *Life Begins to Compute*, USA TODAY, Feb. 14, 1996, at 2A. In the recent 1996 elections, more than six percent of the general population signed on to political web sites, and one percent of the population said that they rely on the Internet as their main source of election coverage. While these numbers may seen small, considering the relative infancy of the Internet and related technologies, they represent substantial inroads into the traditional media. According to the FCC, as of January 1997, there were more than sixteen million host computers on the Internet, more than ten times the number of hosts in January, 1992, and more than three thousand Internet access providers in the United States. Several studies cited by the FCC calculate the numbers of Internet subscribers ranging from 47 million to more than 50 million adults in the United States and Canada alone, compared with less than 18 million in the Spring of 1996, indicating rapid growth. Over 175 countries are now connected to the Internet. WERBACH, *supra* note 1, at 21-22.

example, the landmark Telecommunications Act of 1996 contains controversial provisions designed to prevent children from being exposed to pornography and indecent material over the Internet.[3] Although the cyberporn law was struck down as unconstitutional, and is currently before the Supreme Court,[4] other bills introduced to deal with computer crime portend broader efforts by the new 105th Congress to extend law and order into cyberspace. As they relate to electronic commerce, these upcoming policy debates can be grouped into four main categories: (I) security and privacy; (II) intellectual property, especially copyright;[5] (III) regulation of commerce; and (IV) distributional and participatory democracy issues.

This Article focuses on legal changes emanating from the federal government, with a nod to some, but not all, of the related international legal developments, and with some mention of judicial decisions that are breaking new ground. We will concentrate on commercial and business issues and largely steer clear of the array of criminal and moral issues that have received so much attention elsewhere.[6] This focus will help us to explore the virtual vacuum of a

3. Communications Decency Act of 1996, *in* Telecommunications Act of 1996, §§ 230, 501-561, Pub. L. No. 104-104, 110 Stat. 56, 133-43 (1996)(to be codified as amended in scattered sections of 18 U.S.C. and 47 U.S.C.)[hereinafter the CDA]. *See generally* William Keane, *Impact of the Communications Decency Act of 1996 on Federal Prosecutions of Computer Dissemination of Obscenity, Indecency, and Child Pornography*, 18 HASTINGS COMM/ENT L.J. 853 (1996). Elsewhere, the CDA adheres to the policy of limited government intervention in the Internet. The CDA states that it is the policy of the United States to "preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation." CDA, § 230(b)(2). *See* A Framework for Global Electronic Commerce (visited Jan. 10, 1997)<http://www.iitfinist.gov/electronic.commerce.htm>.

4. *See* ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa.), *prob. juris. noted*, 117 S. Ct. 554 (1996)(oral arguments March 19, 1997, decision pending).

5. More than twenty-five pending bills relate to the Internet, which is "more than double the number introduced during the entire 104th Congress." The bicameral Congressional Internet Caucus has grown from twenty to ninety-seven members. Barbara J. Saffir, *Bit by Bit, Congress Is Opening Up to the Information Age*, WASH. POST, June 2, 1997, at A17.

For a discussion of patentability of software, see Nancy J. Linck and Karen A. Buchanan, *Patent Protection for Computer-Related Inventions: The Past, The Present and The Future*, 18 HASTINGS COMM/ENT L.J. 659 (1996).

6. For example, an inordinate amount of public attention accompanying the enactment of the Telecommunications Act of 1996 focused on the so-called V-Chip and cyberporn provisions. If the truth be told, these were two small amendments added relatively late in the legislative history of the Act and were unrelated to what amounted to a complete overhaul of more than six decades of laws governing communications that Congress labored over for several years. An outstanding and useful survey of the Telecommunications Act of 1996 was recently authored by William & Mary College of Law Dean Tom Krattenmaker. *See* Thomas G. Krattenmaker, *The Telecommunications Act of 1996*, 49 FED. COMM. L.J. 1 (1996). For an assessment of the impact of the 1996 Act on its first anniversary, see, for example, FCC Chairman Reed Hundt, Remarks

coherent framework for cyberpolicy which, in the absence of leadership in Washington, will be filled in on a piecemeal basis by ad hoc judicial decisions, state attorneys general and other local regulators, and limitations imposed on the United States from abroad. While we will cover a number of different issues, we hope to develop three major themes.

First, the federal government and Congress in particular are far behind the curve in balancing the competing, legitimate interests that are at stake in developing the new rules needed for cyberspace.

Second, when the federal government and Congress eventually get around to addressing an issue of cyberlaw, lawmakers skip over the threshold issue of whether or not to fashion new legal approaches that best fit the reality of new technology for the 21st Century. Instead, they proceed immediately to debate ways to tinker with and patch existing law originally developed for earlier technology.

Third, although lawmakers are lagging behind on issues raised by new technology, there is time and ample reason to do the job of writing new rules well, whether the legal change be comprehensive and new, or merely a revision of existing legal rules.

It is worth noting, as we recently celebrated the 50th birthday of ENIAC, the first electronic computer, and as we marvel at the advanced state of computer technology in which an inexpensive, common pocket calculator has more brains than that first ENIAC, that today we are only somewhere in the middle ages of computer technology.[7] Updating laws for cyberspace might be somewhat behind schedule, but the dust has hardly settled on the latest innovations, and there are decades more of computer improvements and new uses for technology. So while lawmakers are at it, it is worth developing rules that are flexible and will fit technology as well tomorrow as they might today.

Moreover, while technology is developing at a staggering pace, the human perspectives associated with the technology often remain the same through the years, centuries, and millennia. The policy fights and consensus-building that lies ahead over the uses of new technology, especially those that center on moral choices and values, are the same as those society has often encountered in the past. In a

---

Before the Freedom Forum and Georgetown University (Feb. 7, 1997), and Neil Hickery, *So Big, The Telecommunications Act at Year One*, COLUM. JOURNALISM REV., Jan./Feb. 1997, at 23.

7. Andrea Stone, *We Are in the Middle Ages of Computers*, USA TODAY, Feb. 14, 1996, at 1A.

column, Meg Greenfield said, "[m]y seemingly quaint, flapper-age parents, once they got the hang of the gadgetry, would be as at home in this world as we all would be in the super-duper one about to come. So far as its human inhabitants are concerned, we would have seen it all before."[8]

If one looks to history, it might, in fact, seem that man's uneasiness with information technology and society's search for the right response to communication innovations raise questions that are eternal. For example, the invention of writing, perhaps more so than the advent of the Internet in the modern world, created many concerns for ancient society.[9] The first references to writing, found in Homer's eighth century B.C. oral epic, *The Illiad*, demonstrate strong misgivings. The marks made by the illiterate Greek warriors in order to cast their lots for the right to fight the Trojan hero, Hector, are called *semata lugra* by Homer, or "sorrowful signs."[10] Elsewhere in *The Illiad*, the hero Bellerophon is given a tablet containing "murderous symbols" that he must carry to a distant king.[11] The treacherous message in this, and many other narratives, such as the double-double cross of Rosencrantz and Guildenstern in *Hamlet*, is "kill the bearer of this message." The presumption underlying these earliest references to writing in Western literature, that this innovation will be used to nefarious ends by unscrupulous men in power, will be familiar to anyone following the recent "clipper chip" debate in Washington, D.C.[12]

Similarly in the fifth century B.C., when Greek merchants began importing Egyptian paper into Athens, Socrates purportedly condemned the new technology. He was concerned, among other things, that it would disrupt the human ties that formed between philosopher and student, cause the mind and memory to atrophy,

8. Meg Greenfield, *Back to the Future*, WASH. POST, Jan. 20, 1997, at A27.

9. The authors are indebted to S. Georgia Nugent, Professor of Classics, Princeton University, for her many insights into the similarities between information technology in Ancient Greece and our current policy debates on the subject. Recently, Prof. Nugent addressed this subject during a talk: *If Socrates Had Email . . . .* (Mar. 1, 1997, Washington, D.C.)(paper delivered as part of symposium honoring 250th anniversary of Princeton University: *The Transformation of Learning in the Age of Technology*)(text on file with HASTINGS COMM/ENT L.J.). She notes that even communication by speech was somewhat worrisome in classical antiquity for the archaic poets Semonides and Hesiod, the dramatist Euripides, and the historian Thucydides, who were all uneasy about the ability of women to speak. *Id.*

10. *Id.* at 3. *See* HOMER, THE ILLIAD book VII, 175-95.

11. THE ILLIAD, *supra* note 10, at pt.VI, 165-75.

12. Nugent, *supra* note 9.

depersonalize interactions, and replace public discourse with less desirable and potentially dangerous private communication. Sound familiar? Compare Socrates' views to concerns many people have about e-mail and chat groups and talking over the Internet instead of over backyard fences. Later, Socrates' friend and protégé, Plato, attributed to Greek drama all of the criticisms that are today leveled against television: too violent, too much sex, too little educational content, and so on.[13]

Some 2,000 years later, when Gutenberg developed the movable-type printing press, many envisioned a communications revolution—specifically, that the printing press would put knowledge into the hands of the common man. For centuries, however, the benefits of Gutenberg's invention were available mainly to the rich, to academics, and to clerics. It was several hundred more years, with the advent of public libraries and improved printing technology that made books more affordable, before books became widely available to the public. This history reminds us of the current policy debate over expanded universal service and appropriate ways to eliminate gaps between technology haves and have-nots. It suggests at least one great opportunity America has to improve upon the past by finding ways to put the benefits of technology into the hands of the public. Perhaps fortunately, the massively overhyped and still uncertain economic, social, and political ramifications of the Internet will not be felt fully for some time, giving policymakers time to build a consensus and find solutions to both the age-old and novel legal and policy issues.

I
Security and Privacy

Congress will continue to be drawn into the task of striking a balance between the need for the free flow of information and the need to protect privacy, as well as the need to secure the increasingly on-line economy. Congress will also have to balance the need of law enforcement and national security authorities to monitor criminal and terrorist activities. Telephone and computer lines reach into homes and businesses, and it is increasingly easier to intercept and eavesdrop on over-the-air transmissions, so there is great interest in systems that

13. Carol Rigolot, Assistant Director, Program in Humanistic Studies, Princeton University, recently discussed this point, originally made by Alexander Nehamas, Director, Program in Hellenic Studies, Princeton University, in informal remarks at a meeting of Princeton alumni, March 20, 1997, Washington, D.C.

can maintain the privacy of conversations and data transmissions.[14] Databases and personal information of all sorts, including what individual users do on the Internet, are increasingly available and accessible online, raising an array of additional concerns.[15]

The government, on the other hand, has sought to prevent the use of security technologies it cannot pierce to obtain information needed for national security and law enforcement purposes. The Administration has proposed to limit export of strong encryption[16] to those manufacturers that agree to use a "key escrow" system accessible to government agents. This proposal is encountering nearly as much opposition as the so-called "Clipper Chip" did in the recent past, and it reveals the growing rift between the natural course of the Internet's private commercial development and the demands of a government intent on protecting certain public interests. These differences are being played out in a number of legislative proposals, some of which purport to deregulate the Internet, and others which would impose new government controls.[17] The lack of international consensus on the subject complicates the debate. While Great Britain

14. Public awareness and interest in this subject is increasing. A small fortune spent on Madison Avenue could not have educated the public more than the media brouhaha in January 1997, over the unauthorized eavesdropping and recording of a conference call involving House Speaker Newt Gingrich about the differences between digital Personal Communications Services (PCS) voice communications, which are currently difficult to intercept, and standard cellular analog mobile phones, which are not. John Markoff, *Team Cracks Part of Digital Cellular Phone's Security Code*, HOUS. CHRON., Mar. 20, 1997, at 3; John Schwartz, *Computer Scientists Break Cellular Phone Privacy Codes: Team's Effort Deals Setback to Industry*, WASH. POST, Mar. 20, 1997, at C1.

15. *See* Nina Bernstein, *On Frontier of Cyberspace, Data Is Money, and a Threat*, N.Y. TIMES, June 12, 1997, at A1, A16-17. For example, the Social Security Administration (SSA) abruptly ended its practice of making employment histories and other information available online when it became known that the SSA could not protect the privacy of individual records. *See* John Schwartz & Barbara J. Saffir, *Privacy Concerns Short-Circuit Social Security's Online Service*, WASH. POST, Apr. 10, 1997, at A23; *Blank Screen at Social Security*, WASH. POST, Apr. 11, 1997, at A26.

Large numbers of IRS employees have been dismissed or otherwise sanctioned for electronically browsing through tax records of celebrities, friends, and family members. *See* Stephen Barr, *IRS Audit Reveals More Tax Browsing*, WASH. POST, Apr. 9, 1997, at A1.

16. Specifically, 56-bit encryption software used to scramble data for protection from hackers and others.

17. *An Act to Extend the Effective Date of Investment Advisors Supervision Coordination Act*, S. 410, 105th Cong. (1997); *Fair Labor Standards Act to be Changed*, H.R.1, 105th Cong. (1997).

and France have been generally supportive of the United States' position, many other countries have not.[18]

A. Encryption

The three-year old policy debate over encryption provides a vivid example of the political tradeoffs presented by the new system of electronic commerce. Widespread use of strong public key encryption is necessary in the United States and abroad if we are to be able to conduct banking, cash transfers, and other commerce over the Internet.[19] However, law enforcement has realized that this same encryption technology can be used to conceal money laundering, other fraudulent or illegal transactions, or even espionage and terrorism.

In the light of the need for encryption, and all of the problems accompanying it, policymakers are faced with three basic choices when regulating encryption technology. First, they can do nothing. If the government did not regulate the sale and export of this technology, software manufacturers would sell whatever products they desired at home and abroad. Although U.S. consumers would have ready access to the latest encryption products, criminals and terrorists would similarly have free access to these products. This technology may give those criminals the ability to avoid government surveillance and detection, making it easier to use computer technology to facilitate money laundering, terrorism, and other crimes.

The second policy choice available to the government is to bar powerful forms of encryption that the government cannot break. As a preliminary matter, such an action by the government may not be constitutional. Even if this action were constitutional, however, the government would be forcing private parties to use weaker forms of

18. Recently, for example, the Organization for Economic Coordination and Development rejected the United States' proposal to permit the world's law enforcement authorities to eavesdrop on computer transmissions. John Markoff, *U.S. Rebuffed in Global Proposal for Eavesdropping on the Internet*, N.Y. TIMES, Mar. 27, 1997, at A1.

19. Public key encryption is a system of encryption where every individual has two keys; one public key to encrypt messages, and a second, private key used to decrypt messages. This is in contrast to a system of private key encryption, where the same key is used to lock and unlock messages. In a system of public key encryption, strangers can send encrypted messages without agreeing beforehand on the key to unlock the messages. In a private key system, parties can send and read encrypted messages only if they already know the other parties' secret key. Because electronic commerce requires large-scale communications between strangers, a system of public key encryption is vital. *See* Don Clark, *Security Dynamics Unit and Cylink End Patent Row*, WALL ST. J., Jan. 7, 1997, at B6; Don Clark, *Bizdos is Holding the Key to Guard Internet Secrets*, ASIAN WALL ST. J., Apr. 17, 1996, at 12.

encryption that could be broken easily by other private parties. Such a lack of security would compromise the utility of Internet for business transactions and would very likely stunt the growth of electronic commerce.

The third option is a middle path between banning and deregulating strong encryption, and this appears to be the choice of the Clinton Administration. The administration is allowing private parties to use and export strong encryption, as long as the government has access to the keys necessary to break the code. While this option does allow parties to use more advanced encryption products in their private communications, it raises a host of civil liberties concerns. These concerns have derailed the administration's efforts to date and will play a prominent role in deciding the future of encryption regulation.

While the administration has decided to pursue a middle path, many others in the federal government favor much looser controls on encryption technology. These competing interests are sharply divided, but not along traditional partisan lines. An unusual alliance of business interests and civil liberties groups, with bipartisan support in Congress, have proposed legislation to eliminate export restrictions on encryption technology.

1. Background

The export of encryption products is regulated under two statutes, the Arms Export Control Act (AECA)[20] and the Export Administration Act (EAA).[21] The AECA is the more restrictive statute of the two. It is administered by the State Department under the International Traffic in Arms Regulations (ITAR).[22] Under these regulations, many encryption products and certain other "technical data" are treated as munitions, placed on a restricted munitions list, and can be exported only under carefully monitored circumstances.[23] The Commerce Department administers the EAA under the Export

20. Arms Export Control Act, 22 U.S.C. § 2767 (1994).

21. Export Administration Act, 50 U.S.C. § 2406 (1994).

22. International Traffic in Arms Regulations, 22 C.F.R. §§ 120-130 (1997).

23. United States Munitions List, 22 C.F.R. § 121.1 (1996). Ironically, treating computer related products like munitions is returning full circle to the military origins of the computer. ENIAC was developed in order to serve the heightened wartime need for fast and accurate ballistics calculations and to replace the large number of clerks, most often women, who performed these laborious calculations and who were known as "computers." Stone, *supra* note 7.

Administration Regulations (EAR),[24] which generally allow more freedom in the export of encryption technology.

Until November, 1996, most strong encryption products were listed on the munitions list, and their export was prohibited by the AECA. However, there have been a series of rapid changes on the regulatory, legislative, and judicial fronts which could fundamentally alter how encryption products are regulated.

2. The Clinton Administration's Encryption Proposals

a. Executive Order 13,026

In November, 1996, President Clinton announced a new policy which allows software manufacturers to export strong encryption products under license from the Commerce Department, provided that the manufacturers commit to developing a key recovery system.[25] As envisioned by the Clinton Administration, a key recovery system addresses the security and law enforcement issues raised by powerful public key encryption. A key recovery system gives third parties access to individuals' private keys used to decode messages. In some plans, these third parties would be government officials, and in others would be private parties. Regardless of who maintains the keys, a key recovery system gives law enforcement access to private keys, and therefore private messages, with a court order.

The Executive Order transfers encryption products from the Munitions List, where they were regulated by the State Department pursuant to the Arms Export Control Act, to the Commerce Control List, where they will be regulated by the Commerce Department under Executive Orders 12,924, 12,981, and the Export Administration Act.[26] Encryption products designed specifically for military use will remain on the Munitions List. Under the new framework applying to the export of encryption products, the products may be licensed for export only if the requirements of 50 U.S.C. sections 2405 and 2406 are satisfied. Export license applications will initially be reviewed on a

24. Export Administration Regulations, 15 C.F.R. §§ 730-774 (1996).

25. Exec. Order No. 13,026, 61 Fed. Reg. 58,767 (1996). The Executive Order has rekindled the debate that began with the Clipper Chip controversy three years ago, when the Administration endorsed a hardware-based encryption system with the keys held by federal law enforcement agencies.

26. *See* Export Administration Act, 50 U.S.C. §§ 2405-2406 (1994).

case-by-case basis to ensure consistency with U.S. foreign policy and national security objectives.[27]

The Order also directs the Commerce Department to promulgate regulations that enact the Order and govern the export of encryption products in greater detail.[28] The Order requires the regulations to state that transfer by electronic means, including through the Internet, of encryption code or products will constitute export of such materials.[29] Additionally, upon the enactment of any export control legislation, the Attorney General, Secretary of State, and Defense Secretary should reexamine whether adequate controls on encryption products can be maintained.[30] If not, the products should then be replaced on the Munitions List.[31]

b. Commerce Department Regulations

Executive Order 13,026 called for the Commerce Department to promulgate regulations to implement the Order. On December 30, 1996, the Commerce Department issued these regulations.[32] Many in the industry expected that the regulations would follow the Executive Order closely. However, the regulations surprisingly failed to eliminate many barriers to encryption export.

The regulations have been received poorly by many in the industry. The Computer and Communications Industry Association has decried them as "top-down industrial policy."[33] According to industry groups like the Business Software Alliance, the regulations have several major problems: (1) the regulations mandate the use of a key escrow system; (2) the administration's approach is too complex for consumers; (3) companies would be required to submit business and marketing plans as conditions for export; and (4) the timetable for developing a key recovery system is shortened from two years to six months.[34] The Business Software Alliance urged Vice President Gore,

27. Exec. Order No. 13,026, 61 Fed. Reg. 58,767.

28. *Id.*

29. *Id.*

30. *Id.*

31. *Id.*

32. Interim Rule, 61 Fed. Reg. 68,572 (Dec. 30, 1996).

33. *Hearings Before the Senate Comm. on Commerce, Science, and Transp.*, 105th Cong. (1997)(testimony of Edward J. Black, President, Computer and Communications Industry Association, Mar. 19, 1997).

34. *See* Kevin Power, *Advisory Group Adds its Suggestions to Encryption Plans*, GOVERNMENT COMPUTER NEWS, Jan. 13, 1997, at 44.

the Administration's point man on technology issues, to make more changes.[35] To address the regulations' shortcomings, the Alliance favored: (1) making key recovery systems optional; (2) that all products using a key recovery system be free of export restrictions; (3) that no deadline be placed on the development of key recovery systems; (4) that all companies be allowed to export 56-bit encryption systems; and (5) that all products be allowed to work together, regardless of status of key recovery system.[36]

But not all business interests oppose the Commerce regulations. Some believe that the plan is workable and have attempted to design compatible software systems. One industry coalition has created the International Cryptography Framework (ICF) which they hope will smooth the export of encryption products and encrypted material.[37] The ICF is designed to include "policy activation tokens," which can limit software's encryption strength depending on the nationality of the user.[38] The ICF platform is the second commercial product to endorse a key recovery system.[39]

The Commerce Department claims that its regulations will protect national security and foreign policy objectives and will foster the development of a key management infrastructure. The provisions that have generated the greatest opposition are: (1) the definition of "export" to include electronic transmission; (2) the requirement that 56-bit encryption software be accompanied with business plans that explain which steps the applicant will take during the two-year transition period; (3) that certain mass-market encryption products will be subject to one-time review; and (4) the requirement that key recovery agent must either pass various qualifications or have Secret level government clearance.[40]

Shortly before the regulations were published, Judge Patel of the Northern District of California struck down the State Department encryption export regulations on First Amendment grounds,[41] presenting an additional problem. The Commerce regulations are based in large part on the State Department regulations, and Judge

35. *Id.*

36. *Id.*

37. Thom Stark, *Encryption for a Small Planet*, BYTE, Mar. 1997, at 111.

38. *Id.*

39. *Id.*

40. *See* Interim Rule, 61 Fed. Reg. 68,572 (Dec. 30, 1996).

41. Bernstein v. United States Dep't of State, 945 F. Supp. 1279 (N.D. Cal. 1996). *See supra* Part I.A.4.a.

Patel's decision, discussed more fully below, has cast a large shadow over their constitutionality.

3. Legislative Proposals

While the Clinton Administration has generally supported tighter regulation of encryption technology exports, many in Congress have proposed sweeping deregulation of encryption technology. Several legislative proposals regarding encryption were considered in the 104th Congress, and while these bills died in committee, many have been reintroduced in the 105th Congress.

a. S. 377: Promotion of Commerce On-Line in the Digital Era Bill

Senator Conrad Burns (R-MT) introduced the "Pro-CODE" bill in the 104th Congress and has reintroduced it in the 105th Congress. This bill has emerged as perhaps the leading piece of pro-encryption legislation. Many believe its chances of passage are greater in the 105th Congress, now that its chief opponent, Senator Exon (D-NE), has retired. The Pro-CODE bill's premise is that the full growth of electronic commerce will not be realized if the Internet is an unsecured medium.[42] The bill's findings state that a variety of encryption products should be available to provide this secure environment, but that U.S. designers have been hampered by Commerce Department efforts to promulgate standards and guidelines that do not have widespread commercial support.[43] The bill states that there is no demand for the key escrow solution, and that there are a number of non-key escrow alternatives available.[44] Therefore, the bill:

- prohibits the Secretary of Commerce from promulgating any regulations that enact policies that result in encryption standards for systems other than the federal government;[45]
- prohibits the Secretary of Commerce from promulgating or enforcing regulations intended to impose government-designed encryption standards on the private sector by restricting the export of hardware or software with encryption capabilities;[46]

42. Promotion of Commerce On-line in the Digital Era ("Pro-CODE") Act of 1996, S. 1726, 104th Cong., § 2 (1996).

43. *Id.* § 2(a)(10).

44. *Id.* § 2(a)(15).

45. *Id.* § 4(a).

46. *Id.* § 4(b).

• prohibits the federal government or states from restricting the sale of any product with encryption capabilities;[47]

• prohibits federal or state governments from requiring as a condition of sale any mandatory key escrow system;[48]

• gives the Secretary of Commerce exclusive authority to control exports of computer technology and software with encryption capabilities, except where specifically designed for military application;[49]

• requires that only a general export license be needed for export of any encryption software as long as it is generally available, or in the public domain;[50]

• requires that the Secretary authorize the export of similar technology of any software or hardware to any country where the Secretary has already authorized export to financial institutions, unless there is evidence that the technology will be diverted to a military use.[51]

Hearings have already been held on the Pro-CODE bill in the 105th Congress, and the bill was strongly endorsed by several prominent trade associations, including the National Association of Manufacturers and the Computer and Communications Industry Association. Additionally, the bill was supported in the hearings by privacy groups, like the Center for Democracy and Technology. This level of high-profile support is a positive sign for supporters of the Pro-CODE bill.

b. H.R. 695: Security and Freedom Through Encryption Act

In the House of Representatives, Congressman Bob Goodlatte (R-VA) has introduced the SAFE bill, which is similar to the Pro-CODE bill, and has emerged as the leading pro-encryption legislation in the House.[52] The bill intends to deregulate the use and export of encryption products.[53] Like the Pro-CODE bill, the SAFE bill died in committee last Congress but will again find many supporters this year. The Goodlatte bill:

47. *Id.* § 5(a)(1).
48. *Id.* § 5(b).
49. *Id.* § 5(c)(1).
50. *Id.* § 5(c)(2).
51. *See id.* § 5(c)(3).
52. Security and Freedom Through Encryption (SAFE) Act, H.R. 3011, 104th Cong. (1996).
53. *Id.* § 2.

• makes it lawful for any person to use or sell any type of encryption;[54]

• creates enhanced penalties for the use of encryption in the furtherance of a crime;[55]

• gives the Secretary of Commerce exclusive authority over exports of encryption software and hardware, except that which was designed specifically for military use;[56]

• states that no validated license may be required for export of encryption software that is generally available or is in the public domain;[57]

• requires the Commerce Secretary to authorize the export of encryption software to any countries where exports of similar capability are allowed for use by financial institutions;[58]

• requires the Commerce Secretary to authorize export of encryption hardware if he determines that a similar product is available from a foreign supplier.[59]

In recent hearings, the SAFE bill received endorsements from groups ranging from the conservative Americans for Tax Reform to civil liberties groups like the Electronic Privacy Information Center to industry groups like the Business Software Alliance. The Justice Department made comments against the bill, to stress the necessity for key recovery systems and the minor threat such systems pose to civil liberties. The widespread support for the SAFE bill, though, means that given the proper opportunity, it could pass the House.

c. S. 376: Encrypted Communications Privacy Act

Senator Patrick Leahy (D-VT), who is extremely knowledgeable and active on computer law issues, has introduced the Encrypted Communications Privacy bill in the last two Congresses, and it has emerged as an alternative to the Burns Pro-CODE bill.[60] Leahy's bill takes a middle path in the encryption debate, by supporting government-run key escrow systems, while also enacting strict

54. *Id.*
55. *Id.*
56. *Id.*
57. *Id.*
58. *Id.*
59. *Id.*
60. Encrypted Communications Privacy Act of 1996, S.1587, 104th Cong. (1996).

standards governing their management.[61] Leahy's bill was subjected to strong criticism in the privacy community, which generally opposes any key escrow system.

The Leahy bill:

- establishes that all Americans are free to use any type of encryption system, with or without a key escrow system;[62]
- creates criminal penalties for unauthorized acts by escrow key holders;[63]
- creates standards for release of key by the key holder;[64]
- makes it legal to sell any type of encryption product within the United States;[65]
- gives the Secretary of Commerce control over all exports of encryption products, except those specifically designed for military applications;[66]
- provides that no license may be required for the export of encryption software that is generally available or is in the public domain or which is available for export to foreign financial institutions;[67]
- provides that the Secretary of Commerce shall authorize the export of hardware with encryption capabilities if a similar product is commercially available from a foreign supplier outside of the United States.[68]

The Electronic Privacy Information Center (EPIC) criticized the Leahy bill for removing export restrictions only on products that are generally available, a restriction that it feels will keep the U.S. behind many other exporters. EPIC also criticized the bill's endorsement of a key recovery system. In part because of this criticism, the Leahy bill may not have a significant chance of passage in its present form.

4. Judicial Approaches

While the White House, Congress, and industry battle over encryption export regulations, the courts have begun to indicate that

61. *See generally id.*
62. *See id.* § 4.
63. *See id.* § 5.
64. *See id.*
65. *See id.*
66. *See id.*
67. *See id.*
68. *See id.*

they may take actions to short-circuit the entire debate. One federal court has struck down the portion of the ITAR regulations prohibiting the export of encryption products, and another court is considering the validity of the new Commerce regulations. These actions indicate that the courts may strike down any manner of regulation restricting encryption exports.

a. *Bernstein v. State Department*[69]

Bernstein is the leading case dealing with encryption exports thus far. Bernstein wrote a complex encryption program and attempted to export the program in two formats: first, as an article explaining his program; and second, the actual computer source code for the program.[70] However, the State Department ruled that both forms of the program were restricted munitions under the ITAR regulations and prohibited their export.[71]

The State Department made its decision under the Arms Export Control Act.[72] The AECA and the ITAR implementing regulations give the President the power to designate a Munitions List and require listed products to be licensed before they may be exported.[73] The ITAR regulations designate "technical data" as one kind of product that can be covered under the AECA.[74] Technical data is defined to exclude general scientific information or information in the public domain or information available to the public through fundamental research at universities.[75]

Bernstein made three main arguments against the regulations: first, that the licensing scheme under ITAR was a prior restraint on cryptographic speech; second, that ITAR was vague and overbroad; and third, that there is a separate protected right to "cryptographic speech."[76] The Government argued that ITAR is content-neutral and survived intermediate scrutiny.[77] The court did not reach Bernstein's argument that there is a right to encrypted speech. Rather, it treated

69. Bernstein v. United States Dep't of State, 945 F. Supp. 1279 (N.D. Cal. 1996).
70. *Id.* at 1284.
71. *Id.*
72. *Id.* at 1283.
73. *Id.*
74. *Id.* at 1284.
75. *Id.*
76. *Id.* at 1285.
77. *Id.* at 1285-86.

encryption as being just one possible subject matter of speech.[78] It did address Bernstein's other arguments, though, and found that ITAR was a prior restraint because the regulations were specifically aimed at applied scientific research and encryption.[79] The court also found that the procedural safeguards afforded by the ITAR export controls did not save the regulations, as they gave the government standardless discretion to make licensing decisions about encryption products.[80] Therefore, the court found that the regulations were an unconstitutional prior restraint on free speech.[81]

Now, though, in the wake of the Commerce regulations, the ITAR regulations no longer apply to the export of encryption products. However, the *Bernstein* holding may also apply to the Commerce regulations, rendering them unconstitutional. The first test of the constitutionality of the Commerce regulations may be the *Karn* case in the United States Court of Appeals for the D.C. Circuit.

b. *Karn v. State Department*[82]

Phillip Karn, a software engineer, wrote an encryption program, and sought State Department permission to export it.[83] The State Department ruled that the source code of the program was a defense article and subject to export licensing requirements. Karn filed suit, claiming, like Bernstein, that the ITAR regulations are unconstitutional. On January 21, 1997, only a week following oral argument, the court decided that Karn's claim had to be reheard in the district court in light of the fact that the ITAR regulations had been superseded by the new Commerce regulations. In light of judicial and international developments, it is certain that encryption will remain one of the legislative battlegrounds regarding electronic commerce in the 105th Congress and possibly beyond.

78. *Id.* at 1286.

79. *Id.* at 1288.

80. *Id.* at 1289.

81. *Id.*

82. Karn v. United States Department of State, 925 F. Supp. 1 (D.D.C. 1996), *remanded by* 107 F.3d 923 (D.C. Cir. 1997).

83. The State Department had allowed Karn to export textbooks containing the code for his encryption program, but barred the export of the floppy disks, leading Karn to claim that his case is "really based on the notion that foreigners cannot type." *See* Doug Abrahms, *Breaking the Export Code*, WASH. TIMES, Jan. 15, 1997, at B6.

B. Privacy Issues

While the encryption battle is a large part of the current privacy debate in Washington, there has also been action on a number of other privacy-related subjects.[84] For example, several bills were either enacted in the 104th Congress and several others have surfaced in the 105th Congress:

1. H.R. 3508: Children's Privacy Bill

This bill, which was introduced in the last Congress by Congressman Bob Franks (R-NJ) but failed to pass, tries to address a growing concern that the Internet can be used to exploit children.[85] The bill makes it a crime punishable by one year imprisonment and subject to civil action for a:

- list broker to sell or buy personal information about a child without the parent's consent;[86]
- list broker to knowingly fail to comply with the request of a parent to disclose the source of information about the child, disclose all information that the broker has sold about the child, or to disclose all people who have received information about that child;[87]
- person who has contacted the child or parents for commercial purposes to fail to comply with the request of a parent to disclose the source of the information;[88]
- person who knowingly uses personal information about the child in connection with a game or contest to contact the child without the parent's consent;[89]
- person to knowingly use prison labor to process information about children;[90]
- person to knowingly distribute or receive any information having reason to believe that it will be used to abuse a child.[91]

84. For a discussion of the myriad privacy issues surrounding the growth of electronic commerce, see generally Maureen Dorney, 19 HASTINGS COMM/ENT L.J. 635 (1997).

85. Children's Privacy Protection and Parental Empowerment Act of 1996, H.R. 3508, 104th Cong. (1996).

86. *Id.* § 2(a).

87. *Id.*

88. *Id.*

89. *Id.*

90. *Id.* For a discussion of the issues surrounding the use of prison labor to process electronic information, see generally Bernstein, *supra* note 15.

91. *Id.* The Clinton Administration announced in June 1997 that it "will press for stricter rules on how information can be collected from children on the World Wide Web," requiring

2. H.R. 3685: Communications Privacy and Consumer Empowerment Act

Last Congress, Representative Edward Markey (D-MA) introduced this legislation to require the FCC to study the impact of new technology on privacy rights and take collective action, if necessary, to protect consumer privacy rights.[92] This legislation became part of the larger debate over the proper role at the FCC in regulating the Internet, and therefore never emerged from committee. Nevertheless, it could be reintroduced in the 105th Congress.

3. H.R. 98: Consumer Internet Privacy Protection Bill[93]

As people browse the Internet, Internet service providers can collect personal information about the user and which sites they visit. This information can be sold, subjecting users to floods of junk e-mail and sometimes invasion of users' privacy. This legislation was introduced early in the 105th Congress by Representative Bruce Vento (D-MN), and could require the written consent of Internet service subscribers before the service provider can disclose any personal information about the user to third parties.[94] The bill would also require that service providers provide subscribers access to any personal information collected about them on the web site.[95]

4. FTC Action

In January, the Federal Trade Commission (FTC) issued a staff report calling on communications and online companies to guard personal information about users more tightly. This report, and a June 1997 FTC workshop on Internet privacy issues, are indications that if companies fail to self-regulate and if Congress fails to step in, the FTC could take action to protect certain consumer privacy rights.[96]

---

parental consent before such information is obtained. Rajiv Chandrasekaran, *Protecting Children's Privacy Online; Administration Wants Firms to Get Parental Consent to Gather Data*, WASH. POST, June 14, 1997, at D1.

92. Communications Privacy and Consumer Empowerment Act, H.R. 3685, 104th Cong. (1996).

93. Consumer Internet Privacy Protection Act of 1997, H.R. 98, 105th Cong. (1997).

94. *Id.* at § 2.

95. *Id.*

96. *See* Steve Lohr, *Rare Alliance on Privacy for Software*, N.Y. TIMES, June 12, 1997, at C1; *Privacy Fears and the Internet*, WASH. POST, June 16, 1997, at A20.

II
Copyright

Copyright is another leading example of the need for policymakers to strike a balance of competing interests. On one hand are creators and holders of rights to intellectual property, who are entitled to incentives and compensation, while on the other hand are distributors and users of the created works, who seek affordable and ready access to intellectual property. As observed by Professor Paul Goldstein, "copyright entails a delicate balance between private and public interests" which may be simultaneously contradictory and interwoven.[97] In order for the public to enjoy the full benefit of private and commercial uses of new technology, enforceable safeguards for intellectual property must keep pace with innovation—without overly restricting the flow of ideas. Over the years, United States copyright law has been stretched and changed to apply to many innovative ways of copying, displaying, and distributing original creative works. The fabric of United States copyright law, despite its historically elastic qualities, is straining to cover the myriad of novel issues raised by exploding innovation in computer and communications technology. The Gutenberg era legal framework may fit the digital, electronically connected world in which it is possible to transmit high-quality images worldwide to millions in the blink of an eye about as well as a Nehru jacket and bell bottoms from an old attic trunk; even if you manage to squeeze in, there are many business and social situations where it simply does not work.

After a long drum roll, the Commerce Department unveiled its recommendations for copyright legislation on September 5, 1995.[98] The report recommends several purportedly modest, but important alterations to current law such as clarifying that electronic transmissions over computer networks are "copies" subject to copyright.[99] Some observers were disappointed that the report sidestepped larger, tougher issues, including new rules for online "fair

97. PAUL GOLDSTEIN, COPYRIGHT'S HIGHWAY: THE LAW AND LORE OF COPYRIGHT FROM GUTENBERG TO THE CELESTIAL JUKEBOX (1994).

98. *Administration Report Urges Changes to Copyright Law*, CONG. DAILY, Sept. 5, 1995, *available in* 1995 WL 10436158.

99. *Id.*

use" of copyright material by teachers, researchers, reporters, and critics.[100]

Congress is far behind the curve on such matters, and legislators will be hard-pressed to access crucial copyright matters before the end of this century. As Professor Paul Goldstein notes in his book, once a new technology is widespread and individuals get accustomed to using it for free, it is virtually impossible to get Congress to impose copyright rules to restrict its use.[101]

A. H.R. 2441: NII Task Force Legislation

This bill was introduced last Congress by Representative Carlos Moorhead (R-CA), who chaired the intellectual property subcommittee in the House, but who has since retired.[102] It is currently unclear what approach Congressman Howard Coble (R-NC), Moorhead's successor as subcommittee chairman, will take to comprehensive copyright legislation. It is possible that copyright legislation in the 105th Congress will reflect new studies, such as the Copyright Office's "Looking Forward" study, which is expected to be issued shortly. This study could expand on the conclusions of the National Information Infrastructure (NII) Task Force and lead Congress to tackle larger copyright issues. However, as of late March 1997, no NII copyright legislation has yet been introduced, which does not bode well for comprehensive copyright reform in the 105th Congress.

Key features of the last Congress' bill include:

- amending definitions of "Distribution," "Publication," and "Importation" to include "transmission" making such transmissions subject to copyright law;
- preventing the import or manufacture of any product the primary purpose of which is to avoid, deactivate, or circumvent, any process that inhibits the violation of copyright rights under section 106 of the Copyright Act;
- prohibiting the removal of copyright management information from copies;

---

100. Others, such as Henry Barry, view the proposal as a Trojan Horse of harmful, dramatic changes designed to maximize the rights of intellectual property owners. *See* Henry Barry, *Information Property and the Internet*, 19 HASTINGS COMM/ENT 619, 626-29 (1997).

101. GOLDSTEIN, *supra* note 97, at 33.

102. 141 CONG. REC. E1892-02 (daily ed. Sept. 9, 1995)(statement of Carlos Moorhead); H.R. 2441, 104th Cong. (1995).

• allowing any party injured by a violation of these copyright rights to bring a suit and receive actual and statutory damages. If the defendant has violated the law within the three previous years, the court may award treble damages. If the defendant violates with the intent to defraud, he or she may be fined up to $500,000 and be sentenced to up to 5 years in jail.[103]

There was fairly strong opposition to this legislation in its original form, and some observers suggest that its proponents have attempted to secure through treaties and international agreement what they could not obtain in the United States through federal legislation.[104] For whatever reason, it is unlikely that the 105th Congress will make much progress on significant copyright legislation.

B. H.R. 1506: Exclusive Digital Sound Recording Right Bill

Representative Moorhead introduced this bill prior to his retirement to address sound recording rights in the age of digital recordings.[105] It is not clear whether the bill will be reintroduced in the 105th Congress. The bill has several major features:

• The bill amends 17 U.S.C. section 106 to add a right to perform a sound recording by way of digital audio transmission.

• The performance of a sound recording is not an infringement if it is part of a nonsubscription transmission, an initial nonsubscription retransmission, or a nonsubscription broadcast transmission.

• The performance of a sound recording is not an infringement when it is part of a retransmission of a nonsubscription broadcast transmission and: (1) the radio station's broadcast is not willfully repeated or retransmitted to distant sites; (2) the station's retransmission was by satellite carrier and retransmission was carried by cable systems as a discrete signal; or (3) the radio station's transmission is made by a noncommercial educational broadcast station.

• The performance of a sound recording is not an infringement when it is: (1) a prior or simultaneous transmission incidental to an exempt transmission; (2) a transmission within a business establishment; or (3) a retransmission by a retransmitter, including an multichannel video programming distributor.

---

103. H.R. 2441, 104th Cong., §§ 2, 4.

104. *See* Barry, *supra* note 100, at 630-33.

105. H.R. 1506, 104th Cong. (1994).

• Nonexempt subscription transmissions shall be subject to statutory licensing if: (1) the transmissions not part of an interactive service; (2) they do not exceed the sound recording performance complement; (3) they do not cause the title to be published in advance; and (4) the transmitting device does not cause the receiver to switch automatically from one program channel to another.

• No interactive service may be granted an exclusive license for the performance of a sound recording for a period of less than one year, except for licenses granted by licensors that hold fewer than 1000 sound recordings, who may grant the license for up to two years.[106]

C. H.R. 401: Intellectual Property Antitrust Protection Act

Judiciary Committee Chairman Henry Hyde (R-IL) introduced this bill, which would eliminate the presumption that market power is always present when a product protected by an intellectual property right is sold or licensed.[107] This presumption is used only by the Ninth Circuit Court of Appeals,[108] but it causes much uncertainty in the computer industry. The Administration hesitated to endorse this bill last term, despite widespread support in Congress.[109]

D. H.R. 3531: Database Investment and Intellectual Property Antipiracy Bill

Congressman Moorhead introduced H.R. 3531 last term.[110] This bill would apply to all databases that are the product of substantial qualitative or quantitative investment and are used in commerce.[111] The bill prohibits any person who has not received authorization from the database owner from extracting or using a substantial part of the database in a way that conflicts with the owner's use or adversely affects the market for the database.[112] Lawful users of the database are allowed to use insubstantial parts of the database for any purpose, and the bill explicitly states that it does not restrict any person from independently collecting data from any other source.[113] Databases

106. *Id.*
107. 143 CONG. REC. E90 (daily ed. Jan 9, 1997)(statement of Rep. Hyde).
108. Digidyne v. Data Gen., 734 F.2d 1336 (9th Cir. 1984).
109. *Administration: Intellectual Property Bill Not Necessary*, CONG. DAILY, May 14, 1996.
110. H.R. 3531, 104th Cong. (1996).
111. *Id.*
112. *Id.*
113. *Id.*

covered under the bill are protected for a period of twenty-five years.[114]

The bill also prohibits the import or manufacture of any device whose primary effect is to avoid or bypass, without the authority of the database owner, any system that prevents the unauthorized use of the database's contents.[115] Finally, the bill prohibits the knowing provision of false database management information.[116]

E. WIPO Treaties

Last December, delegates from over 125 countries and ninety nongovernmental organizations met in Geneva to try to agree on treaties to address copyright issues raised by the Internet.[117] The delegates reached agreement on two of three proposed treaties,[118] and the outcomes are largely consistent with U.S. law. Perhaps the most significant development of the conference was that several troublesome proposals were eliminated from the draft treaties.[119] For example, the proposed copyright treaty would have given the copyright holder exclusive rights over all temporary reproductions, including copies to computer memory, memory buffers of a CD player, or caching of text or images in a communications network. This provision was eliminated in the final treaty.[120] In addition, a proposal to bar devices with the "primary purpose or effect" of copyright circumvention was limited to prohibiting the act of copyright circumvention, preserving the viability of a number of useful technologies.[121]

1. WIPO Performances and Phonograms Treaty

• *Rights of Performers*: Performers are granted the following rights under the treaty: (1) moral rights to be identified as the

114. *Id.*

115. *Id.*

116. *Id.*

117. John Schwartz, *160 Countries Set Treaties on Internet Copyrights*, WASH. POST, Dec. 21, 1996, at A1. While it is beyond the scope of this Article to analyze matters like this in depth, the Geneva Conference must be noted as a matter of context. For an insightful and provocative analysis of these developments, see Barry, *supra* note 100.

118. *Id. See also WIPO Press Release No. 106*, WEST'S LEGAL NEWS, Jan. 16, 1997, *available in* 1997 WL 12502.

119. *WIPO Performances and Phonograms Treaty* (Dec. 23, 1996)<http://www.wipo.org/eng/diplconf/distrib/95dc.htm>.

120. *Id.*

121. *Id.*

performer of the performance;[122] (2) the exclusive right to authorize broadcast and communication to the public of their unfixed performances, or the fixation of their unfixed performances;[123] (3) the exclusive right to authorize the direct or indirect reproduction of their performances fixed in phonograms;[124] (4) the exclusive right to authorize the distribution of performances fixed on phonograms;[125] (5) the exclusive right to authorize rental of performances fixed on phonograms;[126] (6) the right to authorize the distribution of performances fixed in phonograms by wire or wireless means directly to the public.[127] Importantly, each party shall accord national treatment to each other signatory of the treaty.[128]

• *Rights of Producers*: Producers are granted the following rights: (1) the exclusive right to authorize reproduction of their phonograms;[129] (2) the exclusive right to distribute their phonograms;[130] (3) the exclusive right to authorize rental of their phonograms;[131] and (4) the exclusive right to distribute phonograms to the public by wire or wireless means.[132]

• *Common Rights*: both performers and producers enjoy a right to single equitable remuneration for the direct or indirect use of phonograms.[133]

• *Technological Protections*: Signatories must provide adequate legal protection and remedies against circumvention of effective technological measures that are used by performers and producers of phonograms.[134]

• *Rights Management Information*: Signatories must provide effective legal remedies against any person knowingly removing or altering the electronic rights management information, or distributing

122. *Id.* art. 5.
123. *Id.* art. 6.
124. *Id.* art. 7.
125. *Id.* art. 8.
126. *Id.* art. 9.
127. *Id.* art. 10.
128. *Id.* art. 3.
129. *Id.* art. 11.
130. *Id.* art. 12.
131. *Id.* art. 13.
132. *Id.* art. 14.
133. *Id.* art. 15.
134. *Id.* art. 18.

or making available to the public copies of fixed performances where the electronic rights management information has been removed.[135]

2. WIPO Copyright Treaty[136]

• *Relation to the Berne Convention*: The treaty compliments the Berne Convention, and detracts nothing from it.[137]

• *Computer Programs*: Computer programs will be treated as "literary works" under the Berne Convention, regardless of their mode or expression.[138]

• *Databases*: Databases are protected as intellectual creations. This protection extends only to the selection and arrangement of the data.[139]

• *Distribution Right*: Authors of literary works enjoy the exclusive right to distribute their works to the public. Signatories may, though, determine the conditions under which the distribution right is exhausted after the first sale or transfer of the original or copy of a work.[140]

• *Rental Rights*: Authors of works (including computer programs) enjoy the exclusive right to authorize rental of their works. This right does not apply where the computer program itself is not the essential object of the rental.[141]

• *Communication to the Public*: Authors of works enjoy the exclusive right to authorize communications of their works to the public.[142]

• *Technological Measures*: Signatories shall provide adequate legal protection and remedies against technological measures used to circumvent the rights under this treaty.[143]

• *Rights Management Information*: Signatories are to provide adequate legal protection and remedies against parties who remove or alter electronic rights management information or distribute works

135. *Id.* art. 19.

136. *WIPO Copyright Treaty* (Dec. 23, 1996)<http://www.wipo.org/eng/diplconf/distrib/95dc.htm>.

137. *Id.* art. 1.

138. *Id.* art. 4.

139. *Id.* art. 5.

140. *Id.* art. 6.

141. *Id.* art. 7.

142. *Id.* art. 8.

143. *Id.* art. 11.

knowing that the electronic rights management information has been removed.[144]

III
Federal Regulation of Electronic Commerce

A. Electronic Commerce Infrastructure Issues

Infrastructure is a prerequisite to any system of electronic commerce. While the metaphor of the "Bridge to the 21st Century" is now almost as stale as the "information superhighway," it is true that the electronic roads and bridges that make up the Internet must be secure and sound if they are to carry the expanding traffic of electronic commerce.

In addition, rules, protocols, and standards need to be flexible and future-oriented to anticipate and encourage innovation and new uses. Moreover, technical standards should not be allowed to preserve markets for existing business by blocking market entry of newcomers. We are already beginning to see signs that the infrastructure, as currently configured, cannot stand the heavy load of electronic commerce. For example, local telephone outages blamed on the Internet are making the news.[145] These events are catching the attention of government regulators and are stimulating new ventures offering microwave access to the Internet.

Two other key infrastructure developments are the reordering of the satellite industry and the new standards and rules for switching from traditional analog to digital television (DTV).

1. High Speed Internet Communications

Most of the reports of the telephone system's impending collapse stem from two incidents in November 1996. First, on election night many Web sites experienced record volume, temporarily rendering them inaccessible.[146] Then, later in the month, Pacific Telesis reported that Internet traffic had cut off telephone service to Silicon Valley.[147] While subsequent events showed that these reports were vastly

144. *Id.* art. 12.

145. *See Mixed Reviews for the Internet on its First Presidential Election*, N.Y. TIMES, Nov. 7, 1997, at A22; *Internet Not Biggest Threat to Phone System*, WASH. TIMES, Nov. 14, 1996, at B7.

146. *Election '96, On the Internet, A Massive Jam on Information Highway*, CHI. TRIB., Nov. 6, 1996, at 15.

147. *See* BNA Daily Executive Report, Nov. 4, 1996, at A-22.

overblown, the incidents prompted renewed telephone industry efforts to force Internet providers to pay access fees to local telephone carriers.[148] The FCC Chairman has directed the Network Reliability and Interoperability Council to examine the problem, and advise whether the FCC should take any action.[149] Whatever the outcome, the long-term solution is likely to come from technological developments and business solutions rather than regulation.[150]

In the Access Change Reform proceeding at the FCC, the Commission tentatively decided to preserve the present pricing structure for information services, but issued a Notice of Inquiry to conduct a broader examination of "fundamental issues about the implications of usage of the public switched network by information service and Internet access providers."[151]

Currently, enhanced service providers (ESPs), like Internet service providers, pay flat monthly rates to incumbent Local Exchange Carriers (LECs), regardless of their usage.[152] LECs estimate that by 2000, 25-30% of their traffic will be time-consuming Internet usage.[153] LECs claim that ESPs impose the same costs on the system as interstate voice telephony, and therefore should be subject to interstate access charges.[154] In response, ESPs argue that their flat fees, combined with the second phone lines often installed by ESP users, pay for the costs they impose on the network.[155]

While the FCC made a tentative decision to preserve the current system, it will be receiving comments on further changes.[156] In addition, the NRIC will be conducting a parallel study to examine the effect of Internet usage on the telephone system.[157] Either of these

148. Marc Ferranti, *'Net Interests Face Off Over Bottlenecks—Telecom Providers Demand That ISPs Pay In Order To Alleviate Congestion*, INFO WORLD, Feb. 10, 1997, *available in* 1997 WL 8251135.

149. *Handt Asks Network Reliability and Interoperability Council to Monitor Impact of Internet Growth on Public Networks*, FCC DAILY DIG., Nov. 1, 1996, *available in* 1996 FCC LEXIS 5884 [hereinafter *Handt*].

150. *See* WERBACH, *supra* note 1, at 84.

151. *In re* Access Charge Reform, *Notice of Proposed Rulemaking*, FCC 96-488, ¶ 283 (Dec. 24, 1996).

152. *Id.* ¶ 285.

153. *Id.*

154. *Id.* ¶ 286.

155. *Id.* ¶ 287.

156. *Id.* ¶ 288.

157. *See Handt, supra* note 149.

proceedings could result in sweeping change to the way that information services and the telephone system interact.

2. Satellite Communications

While the much-anticipated convergence of telephone and cable has yet to take place, satellites have emerged as a major integrated element of the communications infrastructure. For example, in early 1997 DirectPC was introduced, offering consumers high-speed Internet access over small direct satellite dishes.[158] Such changes make it clear that satellites increasingly are the backbone of global communications. The 104th Congress took no action on the major policy changes that might be needed to revamp the legal structure first established by the Satellite Act of 1962. Without an overhaul of licensing practices it might not be possible to maintain this country's preeminence in international satellite markets.

While matters such as the future structure of COMSAT (the federally chartered private corporation that is the United States signatory to international satellite organizations),[159] the privatizing of INTELSAT and INMARSAT (the two principal international intergovernmental satellite organizations),[160] and the need for more open access to satellite capacity do not necessarily require legislative action, there may be a practical need for Congressional hearings to air the issues, focus the executive branch on options, and generally move the process forward at a more vigorous pace. This subject will be one of the priorities of the House and Senate Commerce Committees in the 105th Congress.

3. Wireless Internet

Recent action by the FCC set aside frequencies that will allow fast and free and unlicensed Internet access.[161] The FCC anticipates that schools, businesses, and hospitals could use these frequencies to interconnect all of their computers without hard wiring their

158. Ken Yamada, *Three Stars Launch Internet Satellite*, COMPUTER RESELLER NEWS, Feb. 5, 1996, at 53.

159. Doug Abrahms, *Comsat Doesn't Want to Play Anymore*, WASH. TIMES, Mar. 25, 1997, at B6.

160. *Intelsat, Inmarsat on Path Toard Being Publicly Traded Stock Companies*, SPACE BUS. NEWS, Mar. 20, 1996, *available in* 1996 WL 7536536; *Inmarsat Owners Seeking Agreement on How to Privatize Organization*, COMM. DAILY, Mar. 26, 1997, *available in* 1997 WL 3943163.

161. *Operation of Unlicensed NII Devices*, Report and Order, 1997 FCC LEXIS 154 (Jan. 9, 1997).

systems.[162] These frequencies would be regulated no differently than garage-door openers, which should encourage their rapid development. In addition, the FCC is increasingly encouraging flexible use of existing licenses that affords opportunities for similar access. The FCC's auction rules and its increasingly expansive trend toward "flexible use" of spectrum is encouraging many business efforts to provide microwave conduits for Internet access.[163]

4. Digital Television

After several years of wrangling, broadcasters, consumer electronic manufacturers, and the computer industry have reached a compromise on digital television format.[164] Although the compromise leaves many questions unresolved, it opens the way for electronic commerce to be carried out over a single piece of hardware in the future.[165] The compromise leaves these disputes to be resolved by market forces, assures that the DTV standard will not be tied to 1940's technology, and that it is open and flexible enough to accommodate additional information. Soon, the very notion of separate television, computer, and telephone services will become passé. Instead we will see a variety of communication, entertainment, and information services offered to consumers through multipurpose appliances.

B. Interagency Working Group on Electronic Commerce

The working group, made up of officials from a number of federal agencies ranging from the National Security Council to the FTC, and chaired by Ira Magaziner, one of the primary authors of the Clinton Administration's first term health care reform initiative, recently issued its blueprint for the regulation of electronic commerce.[166] The draft report concludes that all parties can benefit from a non-regulatory market-oriented approach to electronic commerce.[167] The working group's recommendations have a heavy, recurring emphasis

162. *Id.*

163. Parenthetically, this is why security and privacy of "over-the-air" communications is also an issue of cyberlaw.

164. *TV of the Future—And Look Who's in Charge*, U.S. NEWS & WORLD REP., Dec. 9, 1996, at 14.

165. Louise Kehoe, *TV Does Digital: The U.S. Kicks Off the World's Digital Television Revolution by Being First to Establish a PC-Friendly Digital Standard*, FIN. POST., Nov. 30, 1996, at 99.

166. David L. Guglielmi, *Developing a Framework for Global Electronic Commerce*, BUS. AM., Mar. 1, 1997, at 21.

167. *Id.*

on global regulatory approaches to resolve the Internet's unsolved legal issues including: (1) fostering the Internet as a non-regulatory, market-driven environment; (2) ensuring a transparent and harmonized global legal environment; and (3) allowing competition and consumer choice to shape the marketplace.[168] As described below, the Task Force's conclusions will likely shape the administration's proposals in a number of areas in the coming years. However, these proposals may have no realistic chance of being enacted because of their heavy reliance on international regulation.

1. Financial Issues

a. Tariffs

Magaziner's Task Force concluded that most nations recognize the purported benefits of free trade, and would not want to introduce tariffs on trade over the Internet. However, some countries may want to tax Internet commerce. Therefore, the Task Force recommends that the United States encourage the World Trade Organization (WTO) to declare the Internet a "duty-free environment."[169] Under this framework, no new special taxes would be applied to electronic commerce; rather, only existing taxes that do not hinder commerce and are simple and transparent would be applied.[170]

b. Electronic Payment Systems

The Task Force also concluded that Internet commerce will not fully develop until safe and reliable payment systems are put into place.[171] A number of global banking bodies, as well as the G-7, are looking at this issue, and their recommendations will be an important starting point for government action.[172] Although the Task Force made no concrete recommendations regarding payment systems, it

168. *Id.* Compare this with the three policy goals identified by the FCC: (1) "Promote competition in voice, video, and interactive services"; (2) "Facilitate network investment and technological innovation"; and (3) "Allow all citizens to benefit from advanced technologies." WERBACH, *supra* note 1, at ii-iii.

169. A Framework for Global Electronic Commerce (visited Jan. 10, 1997)<http://www.iitfinist.gov/electronic.commerce.htm>, at I.1.

170. *Id.*

171. *Id.* at I.2.

172. *Id.*

warned the Clinton Administration that before it regulates in this area, it should first seek private industry's opinions and input.[173]

2. Legal Issues

a. UCC for Internet Commerce

The Task Force recommended that the Clinton Administration support the development of a domestic and global uniform commercial legal framework to facilitate global commerce over the Internet.[174] The American Law Institute and the National Conference of Commissioners of Uniform State Law are already working to adapt the UCC to the Internet. Magaziner believes that the government should support this at the domestic level while endorsing international efforts, such as the United Nations' Commission on International Trade Law model law, that support the use of electronic commerce.[175]

b. Intellectual Property Protection

i. Copyrights

The Working Group presented tentative conclusions that the United States should seek to ensure that international treaties: (1) guarantee copyright protection for computer programs as literary works; (2) ensure protection for databases while allowing fair use; (3) specify roles of collecting societies and direct licensing systems, including a prohibition on mandatory licensing; (4) ensure the integrity of the copyright management system; and (5) discourage the inappropriate use of devices to defeat anti-copying systems.[176]

ii. Patents

The Task Force recommended that existing patent agreements should be amended to: (1) prohibit countries from authorizing exploitation of GII-related patents without the owner's authority; (2) require countries to protect GII-related technology; and (3) establish international standards to determine the validity of a patent claim.[177]

173. *Id.*
174. *Id.* at II.3.
175. *Id.*
176. *Id.* at II.4, Copyrights.
177. *Id.* at II.4, Patents.

These goals will be pursued in 1997 at two trilateral conferences involving U.S., European, and Japanese patent officials.[178]

iii. Trademarks

A major trademark issues arising on the Internet involves domain names and infringement.[179] The Task Force refrained from making any recommendations until the close of the Trademark Office's hearings, which will address trademark and unfair competition issues in relation to domain names.[180]

c. Privacy

The Task Force concluded that any future legislation or regulation addressing privacy issues should be based on notice and consent.[181] According to the Task Force, the United States should adopt a two-tiered privacy strategy: first, it should engage its trading partners to develop a "market-based approach" to privacy; and second, the United States should continue to discuss with European and other nations any problems that threaten the free flow of information.[182]

d. Security

Encryption is necessary for electronic commerce to succeed, and the United States has tried to foster the development of advanced encryption technology, despite the fact that those same advanced encryption products can threaten effective law enforcement.[183] For that reason, the United States has enacted a policy that allows companies to export 56-bit encryption products for the next two years, provided that they commit to build and market products that protect the public safety, including third party key escrow systems.[184] While such systems are necessary for international export of encryption technology, the systems are not required for domestic use of a product.[185] The Task Force supports the Clinton Administration's current efforts, while encouraging it to work with other countries to

178. *Id.*
179. *Id.* at II.4, Trademark.
180. *Id.*
181. *Id.* at II.5.
182. *Id.*
183. *Id.* at II.6.
184. *Id.*
185. *Id.*

develop a comprehensive international approach to encryption regulation.[186] For example, the Task Force recommends that the United States work with the OECD, which is in the process of developing international encryption guidelines.[187]

3. Market Access

a. Telecommunications Infrastructure and Interoperability

The Task Force recommends that the United States government address market access issues by continuing to pursue international agreements that restrict service providers from reaching all users.[188] For example, the United States is currently working with the WTO to address the issues listed below, and to ensure that no actions taken by the WTO Group on Basic Telecommunications adversely affects the Internet.[189] The Task Force has a number of areas of concern:

- leased lines: which often must be leased from government monopolies at inflated rates;[190]
- local loop pricing: meaning that on-line service providers must purchase local exchange service from monopolies;[191]
- interconnection: monopolies often price interconnection above cost, or even refuse to interconnect;[192]
- connection: some telecommunications providers have limited which devices can connect to the network;[193] and
- Internet voice and multimedia: some nations regulate Internet realtime services as "like services" and subject them to telephony regulation. Such regulation could hinder development.[194]

b. Content

The Task Force's recommendations in this area place it at odds with Congress on a number of issues, and could be the most contentious of its conclusions. The Task Force concluded that the United States has "long supported the broadest possible free flow of

186. *Id.*
187. *Id.* These guidelines were to be completed in early 1997.
188. *Id.* at III.7.
189. *Id.*
190. *Id.*
191. *Id.*
192. *Id.*
193. *Id.*
194. *Id.*

information across international boarders."[195] While this conclusion could be disputed, the Task Force uses it to drive its content control recommendation that any controls should come from self-regulation, rating systems, and technological solutions.[196] This recommendation has major effects in five different regulatory areas:

- foreign content quotas: many countries have broadcast laws that require a certain percentage of domestically produced content. Many have redefined these broadcast laws to include all new services, including the Internet;[197]
- advertising regulation: many nations strictly regulate the types of advertising and teleshopping that is permitted;[198]
- content regulation: many nations have some types of content barriers that can pose an unfair barrier to U.S. providers;[199]
- regulation to prevent fraud: many nations are tightening their regulations of Internet fraud;[200] and
- regulation of seditious material: providers can be exposed to liability for materials they transmit, be it seditious propaganda or socially unacceptable material.[201]

c. Technical Standards

The Task Force concluded that the communications "technology is moving too rapidly" for the government to mandate interoperability standards.[202] Rather, it believes that interoperability standards should be left to the marketplace.[203] Uniform technology standards will be needed for electronic payments, security, security infrastructure, electronic copyright management, conferencing, and high-speed networking.[204]

195. *Id.* at III.8.
196. *Id.*
197. *Id.*
198. *Id.*
199. *Id.*
200. *Id.*
201. *Id.*
202. *Id.* at III.9.
203. *Id.*
204. *Id.*

C. Tax Treatment of Electronic Commerce

1. Treasury Paper on Tax Implications of Electronic Commerce

In November 1996, the Department of the Treasury issued a long-awaited policy paper that laid out the strategic approach the Treasury plans to take regarding tax issues raised by electronic commerce.[205] The Treasury's approach is similar to that taken by the NII Task Force's White Paper, concluding that the present tax laws are adequate to address electronic commerce, and require only small modification to address the most novel issues.[206]

The Treasury claims that it will not attempt to impose any new or special taxes on electronic commerce, and will use tax neutrality as its basic goal.[207] The policy paper also examines major issues presented by electronic commerce, including: (1) problems that arise in identifying the jurisdiction in which to tax a certain transaction; (2) classification of income from transactions in digitized information; (3) compliance problems raised by smart cards and other forms of electronic cash; and (4) identifying parties to a given transaction.[208] According to the policy paper, the key limiting factors on the growth of the Internet are bandwidth and improved payment mechanisms.[209] Additional topics reviewed include potential electronic commerce applications, such as stock trading, Internet gambling, health care, videoconferencing services, on-line information, photographs, retail, software, and offshore banking.[210]

a. General Tax Considerations

Neutrality requires that all like transactions be treated alike, regardless of the form of the transaction.[211] Developing a tax system applicable to the Internet presents several problems: (1) identifying key taxing points, which normally involve financial institutions but

205. UNITED STATES DEP'T OF THE TREASURY, OFFICE OF TAX POLICY, SELECTED TAX POLICY IMPLICATIONS OF GLOBAL ELECTRONIC COMMERCE (1996)(visited May 29, 1997)<http://www.ustreas.gov/treasury/tax/internet.html>[hereinafter TAX POLICY PAPER].

206. *Id.* at 43.

207. *Id.* at 19.

208. *See id.* at 23-40.

209. *Id.*

210. *Id.* at 8-11.

211. *Id.* at 19.

may be absent on the Internet; (2) identifying Internet users; and (3) detecting the content of messages given encryption protection.[212]

b. Establishments

A company must be engaged in trade or business in the United States in order to be subject to United States tax.[213] A foreign corporation that merely solicits through advertising and sends a good to the U.S. is not engaged in trade in the United States.[214] Many tax treaties require that a business become a permanent establishment before it can be subject to tax in a foreign country.[215] These basic tax concepts should be considered when applying tax laws to the electronic commerce setting. If a company is merely soliciting U.S. business by Internet, it has likely not engaged in trade in the United States. Similarly, if a foreign company merely uses a U.S.-based server, it has not engaged in a trade in the United States. Regarding a permanent establishment, under current regulations, a company's warehouse does not constitute a permanent establishment.[216] A server for a foreign company may be considered the equivalent of a warehouse.[217]

c. Digitized Information

With the advent of digitized information, many income classification issues arise involving copyright law and royalties received from the use of copyrights.[218] The proposed regulations, which represent an initial attempt to resolve income classification issues, may be applicable to all digitized information at some future date. The proposed regulations treat transactions involving computer programs as being either "(1) transfers of copyright rights; (2) transfers of copies of copyrighted programs; (3) the provision of services for the development or modification of a computer program; or (4) the provision of know-how regarding computer programming techniques."[219] There is a close relation between the proper function of copyright law and the proper function of tax laws.

212. *Id.* at 19-20.
213. *Id.* at 22.
214. *Id.* at 24.
215. *Id.*
216. *Id.* at 26.
217. *Id.* at 26.
218. *Id.* at 28.
219. *Id.* at 29.

2. Treasury Regulations

In November 1996, the Department of the Treasury proposed regulations to classify transactions involving computer programs.[220] The proposed regulations attempt to distinguish between the transfer of a copyright and the transfer of the subject matter of a copyright.[221] The Treasury believes that "the rules should take into account the special features of computer programs" and "transactions that are functionally equivalent should be treated similarly."[222]

The regulations provide that all transactions regarding computer programs fall into one of four categories.[223] The proposed regulations then provide guidance for determining how specific transactions should be classified into one of these four categories.[224]

3. H.R. 143: Software Export Equity Act

Many U.S. exports qualify for favorable tax treatment if the manufacturing corporation establishes a Foreign Sales Corporation (FSC).[225] The Software Export Equity Act, introduced at the beginning of the 105th Congress, would amend the Internal Revenue Code of 1986 to provide this benefit to software manufacturers.[226]

4. State Tax Issues—Federal Preemption

States have taken varied regulatory responses to electronic commerce.[227] Some states have tried to eliminate taxes on companies involved with electronic commerce, while others have treated it as a cash cow.[228] Widely varying state tax laws have the potential to stunt electronic commerce's growth, and Congress is considering action to preempt state taxes on electronic commerce. Senator Ron Wyden (D-OR) and Congressman Chris Cox (R-CA) have introduced the Internet Tax Freedom Act to prevent states from enacting any new

220. Classification of Certain Transaction Involving Computer Programs, 61 Fed. Reg. 58,152 (1996)(to be codified at 26 C.F.R. pt. 1).

221. *Id.*

222. *Id.*

223. *Id.* at 58,153. *See also supra* note 219 and accompanying text.

224. *See id.* at 58, 156-58.

225. *See* I.R.C. § 927 (West 1988).

226. H.R. 143, 105th Cong. (1997).

227. Dietra Henderson, *Internet Becomes Target for Taxes,* SEATTLE TIMES, Mar. 16, 1997, at E1.

228. *See id.*; Neil Munro, *If it Grows, Tax It,* COMM. ACM, 1997 WL 9941153.

taxes on electronic commerce until a comprehensive federal approach is developed.[229]

On the other hand, the state of New York has taken the lead in eliminating state taxes in an attempt to attract high-tech companies.[230] Specifically, Governor Pataki proposes to provide Internet access services, and companies that advertise through Internet access providers based in New York with an exemption from state taxes.[231]

D. Smart Cards/Electronic Cash

1. Security and Smart Cards

The market for so-called "smart cards"[232] should boom "from 250 million transactions in 1996 to 25 billion transactions in the year 2005."[233] As smart cards begin to become a reality, the Justice Department has become worried about possibilities for money laundering, fraud and counterfeiting.[234] The dispute between law enforcement and privacy advocates over smart card privacy could rival the encryption debate as the most contentious issue in Internet development. Law enforcement has proposed to track the identities of smart card users, or use an escrowed identity system similar to the proposed encryption escrow systems.[235]

2. Regulation by the Federal Reserve Board

The Federal Reserve Board (FRB) proposed regulations last March to cover smart cards under Regulation E.[236] Congress then

229. H.R. 1054, 105th Cong. (1997); S. 442, 105th Cong. (1997).

230. Henderson, *supra* note 227, at E1.

231. *Id.*

232. For the purposes of this article, we have used the term "smart card" to refer collectively to both smart cards and other forms of electronic cash. Smart cards have been defined as card-shaped data carriers, containing integrated circuits for data storage. Both smart cards and other forms of electronic cash would allow consumers to conduct transactions without cash, making direct deductions from their bank accounts.

233. Linda Dailey Paulson, *Smart Cards to Boom By 2005*, NEWSBYTES, May 28, 1997, *available in* 1997 WL 10959186.

234. *See, e.g.*, Graeme Browning, *Dragnet*, NAT'L J., May 17, 1997, *available in* 1997 WL 7228528.

235. *But see White House to Propose Unlimited Export of Encryption for Electronic Commerce*, BNA WASH. INSIDER, May 8, 1997, *available in* LEXIS, News Library, BNAWI file ("Essentially, the decision means that for financial and electronic transactions, the administration will allow the unlimited export of encryption products, whether of not they are key-recovery.").

236. Electronic Fund Transfers, 61 Fed. Reg. 19,662 (May 2, 1996)(to be codified at 12 C.F.R. pt. 205).

stepped in, imposing a nine-month moratorium on any FRB regulation of smart cards.[237] House Bill 3610 directed the FRB to study how Regulation E should be applied to cash cards without adversely affecting their cost.[238] Now that the moratorium has expired, the FRB has recommended moving forward to regulate smart cards.[239]

E. Clinton Next Generation Internet Initiative

The Clinton Administration recently announced the Next Generation Internet Initiative,[240] which has three main goals: (1) connecting universities and labs with high-speed connections; (2) promoting experimentation with the next generation of networking technologies; and (3) demonstrating new applications that meet important national goals and missions, including health care, national security, distance education, energy research, biomedical research, and environmental monitoring.[241]

F. Computer Maintenance Competition Assurance Act

Introduced by Congressman Joe Knollenberg (R-MI), the Computer Maintenance Competition Assurance Act of 1997 is meant to address the copyright problem that arises whenever a computer is turned on and software is copied into RAM.[242] This copy is protected under section 117 of the Copyright Act, meaning computer repairers cannot turn on a computer to read the diagnostics software without being subject to potential litigation. This bill authorizes third parties to make a copy of software for the limited purpose of servicing computer hardware components.[243]

G. Spamming

Spamming, or electronic junk mail, is another sign that electronic commerce is experiencing growing pains. While many Internet users

237. H.R. 3610, 104th Cong. (1996); H.R. Rep. No. 863, 104th Cong. (1996).

238. H.R. 3610.

239. *See* Niles S. Campbell, *Reg E Ill-Suited for Smart Card Products; Better Approach May Be New Law, Fed Says*, BNA'S BANKING REPORT, Apr. 7, 1997, *available in* LEXIS, News Library, BNABNK file.

240. White House Office of the Press Secretary, *Background on Clinton-Gore Administration's Next Generation Internet Initiative* (Oct. 10, 1996)<http://www.iitf.nist.gov/documents/press/internet.htm>.

241. *Id.*

242. 143 CONG. REC. E21-03 (daily ed. Jan. 7, 1997)(statement of Rep. Knollenberg).

243. *Id.*

have experienced the inconvenience of being spammed by unwanted e-mail messages, few have begun to realize the potential problems raised by spamming. First of all, volume must be a concern. Spamming can be achieved at a much lower cost than any other form of similar junk mailing or direct advertising. Moreover, it raises some privacy concerns, to the extent that spammers access personal information about a user's Internet use patterns to tailor the spam he sends.[244]

AOL, a frequent recipient of spamming attacks, took action almost a year ago, "bombing"[245] the Internet service providers of Cyber Promotions, Inc. a frequent disseminator of "unsolicited e-mail messages" offering weight loss products, health aids, and phone sex.[246] Cyber Promotions brought suit, claiming that AOL violated its First Amendment rights.[247] The federal court for the Eastern District of Pennsylvania held that AOL was not a state actor, and that Cyber Promotions had no First Amendment right to send unsolicited e-mail.[248]

This case, while providing a comprehensive analysis of First Amendment issues on the Internet, does not answer the numerous First Amendment issues raised on the Internet proper, as opposed to private networks like AOL.

IV
Case Studies

A. Pharmaceutical Promotion on the Internet

The promotion of pharmaceuticals on the Internet is an example of the benefits, pitfalls, and regulatory uncertainties presented by electronic commerce. Pharmaceutical advertisements on the Internet raise the typical issues posed by all electronic commerce which we have already reviewed, such as tax and security, but also raise a host of FDA/health regulatory questions specific to food and drug law. For

244. *See generally* Leslie Miller, *Most Surfers Fear Revealing Too Much on the Web*, USA TODAY, Mar. 27, 1997, at 4D; Randi Feigenbaum, *Garbage In—And In and In, An Explosion of Junk E-Mail Threatens to Overwhelm the Net*, BUS. WK., Sept. 9, 1996, at 110.

245. AOL sent all of the undeliverable e-mail messages sent by Cyber Promotions and sent the e-mail in a bulk transmission in order to disable Cyber Promotion's Internet service providers. Two of Cyber Promotion's three ISPs then dropped Cyber Promotion's accounts. *See* America Online v. Cyber Promotions, 948 F. Supp. 436, 437 (E.D. Pa. 1996).

246. *Id.* at 439.

247. *Id.* at 438.

248. *Id.* at 441-44.

example, there are strict limits on what information pharmaceutical manufacturers use to promote prescription and over-the-counter drugs, and what advertising they can provide to patients directly. Many in industry have begun to use the Internet for promotional purposes, and the FDA has, in many ways, indicated that it will vigorously extend its rules into that domain.[249]

The DEA has called for a ban on all Internet advertising of controlled substances, claiming that they will promote the use of legal drugs for illegal purposes. The DEA's proposal would limit drug companies to placing materials similar to the *Physicians' Desk Reference* on the Internet.

1. Advertising versus Labeling

Drug promotional activities, including advertising and labeling, are regulated under the Federal Food, Drug and Cosmetic Act (FFDCA).[250] It is not clear whether drug promotional activities on the Internet is subject to FFDCA rules. Despite the uncertainty, the FDA recently issued its first warning letter to the Liposome Company for making misleading claims about the drug Abelcet on the Internet.[251]

2. Off-Label Information

Drug manufacturers are currently restricted in what types of information they may give doctors and patients regarding "unapproved" uses or so-called off-label uses of their drugs. Some pharmaceutical companies have discussed creating on-line chat rooms where such unapproved uses could be discussed. In addition, other drug companies currently support disease-related groups that have already established such chat rooms. Similarly, the home pages of many pharmaceutical companies contain links to sites where off-label information may be disseminated. The regulatory status of all of these activities is unclear.

3. International Promotion

There are strict rules governing export of U.S. drugs abroad, and promotion of products approved and available overseas, but not yet

249. *See generally* Curt Werner, *FDA Turning Wary Eye on Internet Abusers*, HEALTH INDUS. TODAY, Sept. 1, 1996, *available at* 1996 WL 7904630.

250. 21 U.S.C.A. §§ 301-395 (West 1996).

251. Ronald M. Schwartz, *FDA Issues Warning on Wayward Website*, AM. DRUGGIST, Feb. 1, 1997, at 21.

approved by the FDA. Yet, it is unclear to what extent such rules apply to the Internet. For example, because many drugs are approved in Europe before they are approved in the United States, drug companies may consider using the Internet to make materials available to United States citizens before FDA regulations would otherwise allow. The FDA has not taken any action in this area thus far, but it will certainly be an area of contention in the future.

B. Internet Gambling

Gambling is beginning to spread on the Internet despite significant uncertainty about the legality and profitability of the practice. First, Internet gambling is faced with the same basic problems as all other electronic commerce: the infrastructure must be sound; gamblers must have access to computers;[252] and the financial transactions must be secure. However, there are special problems associated with gambling. First, there are some doubts about whether this industry, which is fueled in part by the "ambiance" of casinos, will be successful in the sterile atmosphere of cyberspace. Internet gaming enthusiasts respond by pointing to the success of off-track betting parlors and state lotteries as support for the idea that Internet gambling can succeed without posh Las Vegas amenities. Also, there is a problem with the image of Internet gambling. Users might hesitate to entrust any sum of money to Internet casinos, lest they be ripped off by shady operators based in offshore locations. Still others worry that Internet gambling will be too successful and too appealing, and that individuals will, free of regulatory controls imposed in the casino setting, keystroke their way to financial ruination from their home PCs.

Internet gambling is faced with significant questions regarding its legality under current law. The basic federal wire gambling statute[253] appears to prohibit Internet gambling, and there has been legislation proposed just to make certain that it does.[254] Pressure in the future is also likely to come from state attorneys general, who have urged

252. One gambling executive noted that his on-line casino "didn't want to take a propeller-head and have to teach him how to gamble." Rather, he wanted to go after known gamblers, even "giving them computers, if necessary." *See New York Times Tackles On-Line Gaming* (visited Apr. 24, 1997)<http://www.RGTonline.com/TheBigStory.html#InternetGaming:TheFull Story/>.

253. 18 U.S.C. § 1084 (1994).

254. *See* S. 474, 104th Cong. (1996).

federal prosecutors to banish Internet gamblers from cyberspace,[255] and the National Gambling Impact Study Commission, which will also examine the impact of Internet gambling.[256]

On the other hand, there are significant legal defenses against regulation of Internet gambling. Federal courts have indicated that they will give the highest form of First Amendment protections to the Internet.[257] Also, Internet gamblers have shown a willingness to establish themselves outside of federal jurisdiction to avoid prosecution.[258] These diverse legal issues indicate that while the financial success of Internet gambling is far from certain, its growth will present significant legal questions for years to come.

1. Transmission of Wagering Information Law

Federal law prohibits any person engaged in the business of wagering or betting from using a wire communication in placing of any bets on any sporting events or contests.[259] While this almost certainly applies to the Internet, it is significantly limited by the requirements that (1) the bet pertain to sporting events or contests, and (2) that the defendant be engaged in the business of betting or wagering. These loopholes have led many to push for new legislation to prohibit gambling on the Internet.

2. S. 474: Internet Gambling Ban

Senator Kyl (R-AZ) introduced this bill, which attempted to close the two major loopholes in 18 U.S.C. section 1084. The bill struck the language requiring that the wagers be related to a sporting event. Then, it added a provision criminalizing the transmission of any wager, money, or information relating to a wager by any person over the wire or by electronic communication.[260] The bill also gives the Justice Department the power to seize any equipment used in committing the offense.[261]

255. *See, e.g.*, Hubert H. Humphrey III, *Virtual Casinos, Real Stakes*, N.Y. TIMES, Nov. 19, 1996, at A25.

256. *See* H.R. 497, 104th Cong. § 4 (1996).

257. *See* ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa.), *prob. juris. noted*, 177 S. Ct. 554 (1996).

258. *See* United States v. Thomas, 74 F.3d 701 (6th Cir. 1996).

259. 18 U.S.C. § 1084(a) (1994).

260. S. 474, 104th Cong. (1996).

261. *Id.*

3. National Association of Attorneys General (NAAG) Report

The NAAG published a report in June 1996 that reviewed current on-line gambling operations and made several recommendations to address them. The NAAG had two major recommendations: (1) enact state laws to allow civil actions for violation of state gambling laws; and (2) amend 18 U.S.C. section 1804 to specifically address Internet gambling.

According to the NAAG, most states have enacted a series of laws that either prohibit gambling, or allow some gambling in a delicately balanced legislative scheme. Internet gambling threatens this balance. At the time of the report, there were only a handful of operational Internet casinos, but the low number was likely due to technological, not legal, limits. Difficulty in finding inding secure forms of cash transfer and lack of trust in Internet gambling operations are the greatest barriers to widespread Internet gambling. Despite this obstacle, many operational sites have been accessed millions of times each.

The NAAG identified certain legal issues raised by Internet gambling that it proposes to address:

• *Jurisdictional Issues*: It is not clear under present law whether the content provider can be held liable in the state of the user just because they allow access to their offshore site. *United States v. Thomas*, the leading case on this point, was decided under very different facts. There, the court found jurisdiction, but the content provider had specific communications with the defendant.[262] It may be that forum states do not have jurisdiction over offshore Internet gamblers who simply allow users to access their site.

• *Liability of Internet Service Providers*: If states are not able to obtain jurisdiction over content providers, they may turn to service providers. However, the law in this area is divided as well. In *Cubby v. Compuserve*,[263] CompuServe was held not to be liable for defamatory information placed on the system by users. But in *Stratton Oakmont v.*

262. *See* United States v. Thomas, 74 F.3d 701 (6th Cir. 1996). *See also* Inset Sys. v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996)(holding that company soliciting business in Connecticut through an advertisement on the Internet has "minimum contacts" with Connecticut for the purposes of establishing personal jurisdiction); Edias Software Int'l v. Basis Int'l, CIV 96-932 (D. Ariz. Nov. 21, 1996)(holding that e-mail messages directed to forum state and messages posted to a CompuServe forum are adequate to establish personal jurisdiction over a defendant).

263. Cubby v. Compuserve, 776 F. Supp. 135 (S.D.N.Y. 1991).

Prodigy Services,[264] Prodigy was found liable for the placement of defamatory information placed on its system because it exercised editorial control over the content of its system. However, service providers may have found total insulation from liability in the recently-passed Telecommunications Act of 1996, which prevents interactive computer services from being treated as the speaker of any information provided by another content provider.[265]

• *NAAG Recommendations*: In light of these barriers, NAAG recommends three steps to battle on-line gambling: (1) increased education; (2) expanded ability to sue gambling content providers in state civil actions; and (3) reform of the federal wire statute to make it clear that gambling content providers are liable.

4. Test Case: Minnesota v. Granite Gate Resorts[266]

The Minnesota Attorney General brought this consumer protection action against an online casino in 1995. The state claimed that the casino violated Minnesota consumer fraud laws by claiming that Internet gambling is lawful, when in fact it is prohibited by 18 U.S.C. section 1084 and several Minnesota laws.[267] The court ruled that it had jurisdiction over Granite Gate. The court applied the familiar "minimum contacts" test used by the United States Supreme Court, and found that Granite Gate had a substantial volume of contacts with Minnesota, had purposely availed itself of the Minnesota forum.[268] The logic of this decision makes Internet gambling operations amenable to suit in any jurisdiction in the United States. This reasoning could allow law enforcement a major tool against Internet gamblers.

5. Potential Action by National Gambling Impact Study Commission

While a number of states and Congress are likely to take up some form of legislation to curtail Internet gambling, Internet gambling is also likely to play a major role in the proceedings of the National Gambling Impact Study Commission, which Congress formed last year

264. Stratton Oakmont v. Prodigy Servs., 1995 WL 323710 (N.Y. Sup. Ct. 1995).

265. *See* CDA, *supra* note 3. *See also* Ian C. Ballon, *Pinning the Blame in Cyberspace: Towards a Coherent Theory for Imposing Vicarious Copyright, Trademark, and Tort Liability for Conduct Occurring Over the Internet*, 18 HASTINGS COMM/ENT L.J. 729, 759-61 (1996).

266. No. C6-95-7227, 1996 WL 767431 (D. Minn. Dec. 11, 1996)(order denying defendants' motion to dismiss for lack of jurisdiction).

267. *Id.* at *5.

268. *Id.* at *6-*11.

to study the social and economic impact of gambling, and Internet gambling. Established gambling interests will be represented on the Commission, but small start-up Internet gambling companies will not be represented.[269]

V

Social Distributional Issues & Participatory Democracy

When Gutenberg invented the first moveable-type printing press and published his famous Bible around 1445, this historic event did not immediately launch an information revolution throughout society. Books became available, but usually only for the rich. It was the creation of public institutions like public libraries that finally made book knowledge accessible, along with technology improvements that helped make printed material more affordable that made the revolution a reality.

In our time, access to information networks will be the gateway to economic opportunity and participating democracy. While networks are already providing some classrooms with vast resources and access to cyberspace, it is going to be ever more frequented by business and residential users. Those of modest means could become disconnected. The gulf between information haves and have-nots could be even greater abroad, where a phone, much less the Internet, remain out of reach for the majority of the world's population.

Currently in the United States, only 20% of the public has access to the Internet, but there are a number of initiatives underway to see that the other 80% of the population are included. "Universal service" has been a cornerstone of telephone service in the United States, and will likely be applied more generally in information services in the future. These developments are simultaneously occurring on a number of fronts. The Telecommunications Act of 1996 made schools and libraries universal service providers, and charged them with the responsibility of extending new information services to the public. The FCC recently issued the details of how to achieve this goal.[270] President Clinton has urged that all schools and libraries be given free access to the Internet, with telecommunications carriers picking up the

269. See Bill Lambrecht & Tim Poor, *Gephardt Names Union Official to Gaming Panel—Appointee Has Ties to Casinos*, ST. LOUIS POST-DISPATCH, Feb. 13, 1997, at 9A (discussing appointments of pro-gambling interests to Commission).

270. *See Report and Order*, FCC 96-45 (May 7, 1997); *In re* Access Charge Reform, *Notice of Proposed Rulemaking, Third Report and Order, and Notice of Inquiry*, FCC 96-488 ¶ 32 (1996).

bill. With less than fifty percent of libraries connected to the Internet, the cost could be significant, and has been a knotty problem for the FCC to resolve.

Shortly before the 1996 election, the Clinton Administration announced its long-awaited plan to give schools and libraries free access to the Internet.[271] Under the plan, carriers providing the service would be compensated from the Universal Service Fund.[272] In November, the federal-state joint board issued its recommended decision on universal service, which represented a compromise between the Administration's ambitious proposals and industry opposition.[273] Under the decision, most schools would get a discount of 60% on telecommunication and Internet access services, and inside wiring.[274] The poorest schools would be eligible for a 90% discount. The universal service fund was capped at $2.25 billion in annual assessments to pay for these discounts.[275] The FCC largely adopted this recommended decision, and issued its final decision in May 1997.[276]

While the FCC's recent implementing order is an important first step, there are many challenges ahead: most classrooms are not wired for telephones or computers, the building structure of many schools makes rewiring time-consuming and costly, and few schools have a sufficient number of high-quality computers.

A. Cunningham Proposal

Congressman Randy "Duke" Cunningham (R-CA) has introduced legislation that would create tax incentives for private investment to bring high-technology equipment into local classrooms.[277] There are many questions that have to be answered as part of introducing such legislation, such as: (1) which schools are

271. Susan Page, *Clinton: Give Schools, Libraries Free Internet*, USA TODAY, Oct. 11, 1996, at 2A.

272. Conservative estimates of providing basic telecom access to the schools range between $1.5 and 2.5 billion, while the Personal Communications Industry Association estimates that it could cost between $10 and $40 billion.

273. *Joint Board Issues Sketchy Recommendation on Reforming Universal Service*, COMM. DAILY, Nov. 8, 1996, *available in* 1996 WL 12300446.

274. *Id.*

275. *Id.*

276. *See supra* note 270.

277. 21st Century Classrooms Act for Private Technology Investment, H.R. 1153, 105th Cong. (1997). *See also Competitive Local Services: New Bill Would Give Tax Breaks for Tech Donations to Schools*, TELECOMM. REPORTS, Mar. 24, 1997, *available in* 1997 WL 7757199.

eligible to receive tax-exempt donations; (2) how to ensure that only technology that is part of the school's technology plan is tax-exempt; and (3) how items should be valued for the credit. The Cunningham legislation was introduced in March 1997.

B. The Business of Government and Campaign Finance

Major changes lie ahead for the way the government conducts business. Government documents, hearing transcripts, and bills are already easier to acquire online than from traditional sources. Members of Congress maintain their own home pages and can be reached via e-mail.[278] Some want the U.S. Government Printing Office to distribute all new laws, reports, and other publications electronically by 1998.[279] Under such proposals print versions would not long be sent to the 1,500 "depository" libraries across the country.[280] If people can pay taxes, join a press conference, or answer an opinion poll from their desk top, why not vote from there as well? In the 1996 election, one percent of the population, according to a *USA Today* survey, said they relied on the Internet as their main source of election coverage.[281] Even at such relatively low rates of usage, over thirty percent of Bob Dole's campaign volunteers signed up for the campaign through the Internet. Although these are small numbers, they foreshadow the centrality of the Internet in future political campaigns. When you consider that 90% of Internet users vote, and that the average Internet user makes between $55,000-60,000 per year, it is clear that there is a key new constituency that can be reached at low cost. Even if people will not vote for the next President by Internet, they will still use the Internet to gather critical information about all of the candidates.

Congress' current battles over campaign finance proposals are based on a very limited concept of communications and commerce. As communications break away from the traditionally dominant

278. Over two-thirds of the members have set up "offices" on the Web, and large volumes of material are transmitted by Congressional organizations. *See* Saffir, *supra* note 5. The House and Senate went online in 1993. By 1995 millions of Internet users were accessing the point and click web sites of both chambers. Last summer about 160 representatives had web sites, and this number has increased to 255. *Id.* Senate home pages received 3.7 million "hits" in April 1997, and the Library of Congress legislative service received nearly 10 million hits. *Id.*

279. David Judson, *Libraries Chief Seeks 'Equity' in Digital Age*, USA TODAY, Feb. 14, 1996, at 9A.

280. *Id.*

281. *See* Stone, *supra* note 2.

television broadcast systems and move to new media, the way that campaigns are run will be reshaped. The 1996 election was the first that had a significant, measurable Internet presence, and while presidential home pages were more of a novelty than anything else, they are a sign of things to come. When televisions and computers have merged, and consumers have a choice of thousands of channels of entertainment and information, candidates for office might be able to bring larger amounts of information to voters for far less than they currently spend today. This could take much of the pressure off of candidates to raise massive amounts of money, and perhaps obviate the need for major campaign finance reform, or at least the reform as currently envisioned by the major parties. No one has yet claimed that a political candidate has won or lost an election in cyberspace, but 1996 may be the last election year when that is the case.

VI
Conclusion

Neal Stephenson's insightful, and somewhat Hunter Thompsonesque travelogue about a new global linkage for Cyberspace which appeared in *Wired* magazine paints vivid images of the electronic marketplace:

> Wires warp cyberspace in the same way wormholes warp physical space: the two points at opposite ends of a wire are, for informational purposes, the same point, even if they are on opposite sides of the planet. The cyberspace-warping power of wires, therefore, changes the geometry of the world of commerce and politics and ideas that we live in. The financial districts of New York, London, and Tokyo, linked by thousands of wires, are much closer to each other than, say, the Bronx is to Manhattan.[282]

The legal framework necessary for electronic commerce to flourish has a lot of catching up to do to keep pace with the evolving, growing, unpredictable new world market of cyberspace. At present legal rules are developing in fits and starts, on an *ad hoc* basis, in a virtual policy vacuum. Business ventures that depend on on-line services, face uncertainty about applicable rules; rules that for good or bad, will be large, if not critical determinants of the success and expansion of such enterprises. Even in the very recent past, it was popular, especially among Internet aficionados, to promote and fiercely defend the concept of cyberspace as an unregulated realm to

282. Neal Stephenson, *Mother Earth, Motherboard*, WIRED, Dec. 1996, at 98, *available in* <http://www.wired.com/4.12/motherearth/>.

be kept free from government intrusion. Ironically, the United States federal government has long been supportive and immersed in the development of the Internet from its very beginnings, through grants and as the largest institutional user of the Internet.[283] Increasingly, as the lack of legal order causes disruption and forces disputes to a head, even the most ardent electronic frontier libertarian might agree that Dodge is a better place when Matt Dillon is in town. Still, the wrong legal rules have a great potential to stifle, delay, and stunt the progress of electronic commerce. All this seems to be understood by lawmakers who, after all, can remember many examples of twentieth century communications businesses confined like bonzai plants in separate industrial compartments. Although the federal government, in general, has so far ignored or minimized efforts to regulate cyberspace, this no doubt will change. Both Congress, in the 1996 Telecommunications Act, and the FCC, in various policy pronouncements, state intentions to avoid "unnecessary" regulation of online services. Still, the federal presence in the future can be expected to be larger—if only to forestall a myriad of different state and local regulations and taxes.

Progress by lawmakers in fashioning substantive rules for electronic commerce is coming slowly, with numerous issues searching for coherent policy. In some areas, such as the encryption debate, legislation has, at this writing, been reported favorably out of committee in Congress, but this legislation still faces opposition by the Clinton Administration. The FCC's recent universal service order, by funding efforts to connect every classroom in the country, makes a big step toward assuring widespread affordable access and ability of every American to use the Internet. But on this effort, and other areas, notably copyright, much work remains to be done.

The lasting answers to the new legal questions posed by the Internet can only emerge through serious and sustained study. So far Congress has been challenged to avoid tripping over established political battle lines. Its approach often has been to struggle with the difficult and perhaps futile approach of applying existing regulatory classifications to cyber-commerce, or attempting to apply rules from particular geographic jurisdictions to Internet services that are oblivious to geopolitics.

As a starting point it will be necessary for lawmakers to achieve consensus on basic principles. One area where there is already

283. WERBACH, *supra* note 1, at ii.

agreement is that legal rules should be pro-competitive, and that vigorous competition is preferable to regulation as a way to govern market behavior. This is the central principle underlying the 1996 Telecommunications Act, and there should be, in theory, support for applying the same principle to rules for cyberspace. Another new principle worth considering is that rules be flexible and future friendly. The government has been singularly unsuccessful in predicting business success and failures, and rules should be developed that leave this outcome to the market. Since the winners and losers are unpredictable, and because technology is changing so rapidly, the challenge is to develop rules that are as good tomorrow as they are today. This will in turn also enable innovation but not guarantee it. Even if lawmakers can agree on basic principles, a great deal of work lies ahead to write rational rules for law and order in cyberspace.