Nova Law Review

Volume 23, *Issue* 2 1999 *Article* 1

Nova Law Review 23, 2

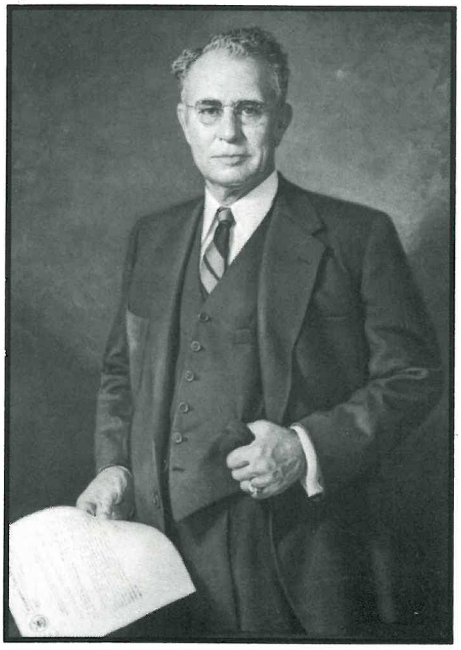
*

*

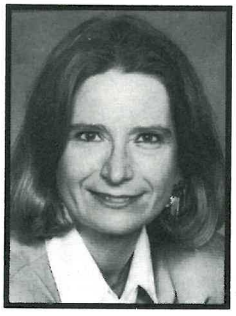
NOVA LAW REVIEW

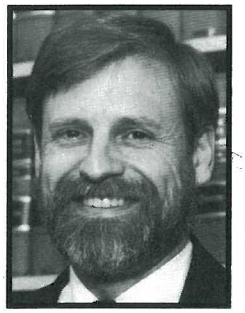
The Leo Goodwin Sr. Chair in Law
1998 Visiting Professors

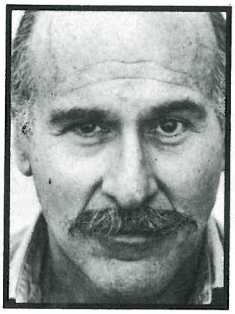
The Internet and the Law

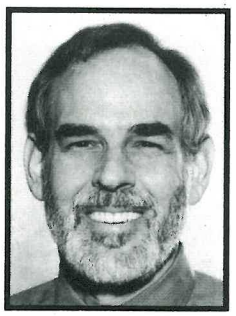


Leo Goodwin Sr.









VOLUME 23 **WINTER 1999** **NUMBER 2**

NOVA LAW REVIEW

VOLUME 23 WINTER 1999 NUMBER 2

TABLE OF CONTENTS

The Internet and the Law

NOTES AND COMMENTS

Privacy in the Digital Age: Work in Progress

Jerry Berman & Deirdre Mulligan*

TABLE OF CONTENTS

* Deirdre Mulligan is Staff Counsel at the Center for Democracy and Technology, a public interest organization dedicated to developing and implementing public policies designed to protect and enhance civil liberties and democratic values in the new digital media. Center for Democracy & Technology <http://www.edt.org>. This article was made possible through the generous support of the Deer Creek Foundation, and benefited from discussions with members of the Internet Privacy Working Group and various privacy and consumer advocates.

I. OVERVIEW

The Internet is at once a new communications medium and a new locus for social organization on a global basis. Because of its decentralized, open, and interactive nature, the Internet is the first electronic medium to allow every user to "publish" and engage in commerce. Users can reach and create communities of interest despite geographic, social, and political barriers. The Internet is an unprecedented mechanism for delivering government and social services, from education and healthcare to public information. As the World Wide Web grows to fully support voice, data, and video, it will become in many respects a virtual "face-to-face" social and political milieu.

However, it remains an open question whether the Internet's democratic potential will be achieved. The Internet exists within social, political, and technological contexts that can impede its democratic potential. Governments tout the Internet, but worry about its threat to their traditional authority. The private sector sees the economic potential of the Internet, but anti-competitive impulses are also part of the landscape. Users bring not only their social aspirations to the Internet, but also their potential for antisocial behavior. Adopting the frontier metaphor, we are now witnessing the struggle over governance of the Internet. After the revolution, what type of constitution do we want? Will it be pluralistic and democratic? Will it incorporate a bill of rights that protects individual liberty and equality?

Protection of privacy is one of the critical issues that must be resolved. Will the "Digital Age" be one in which individuals maintain, lose, or gain control over information about themselves? Will it be possible to preserve a protected sphere from unreasonable government and private sector intrusion? In the midst of this uncertainty, there are reasons for optimism. Individuals operating on the Internet can use new tools for protecting their privacy. From anonymous mailers and web browsers that allow individuals to interact anonymously, to encryption programs that protect e-mail messages as they pass through the network; individuals can harness the technology to promote their privacy. Equally important is the new found voice of individuals. Using e-mail, Web sites, listservers, and newsgroups, individuals on the Internet are able to quickly respond to perceived threats to privacy. Whether it be a proposal before the Federal Reserve Board requiring banks to "Know Your Customers,"[1] or the release of a product like

1. Notice of Proposed Rulemaking, 63 Fed. Reg. 67,563 (1998).

Intel's Pentium III, that will facilitate the tracking of individuals across the World Wide Web. Internet users have a forum for discussion, a simple method to find like-minded souls, and a platform from which to spread their message. This active vigilance is forcing the government and the private sector to reckon with a growing and vocal privacy constituency.[2]

But it is not just individuals' self-interest leading us toward increased privacy protection. Faced with numerous surveys documenting that the lack of privacy protections is a major barrier to consumer participation in electronic commerce, businesses are beginning to take privacy protection more seriously. Numerous efforts at self-regulation have emerged; both cooperative, such as TRUSTe,[3] the Better Business Bureau's Online Privacy Program,[4] and the Online Privacy Alliance;[5] and perhaps more importantly for the long-run, company specific. A growing number of companies, under public and regulatory scrutiny, have begun incorporating privacy into their management process and actually marketing their "privacy sensitivity" to the public. The collective efforts pose difficult questions about how to ensure the adoption and enforcement of rules in this global, decentralized medium.

Governments, are also struggling to identify their appropriate role in this new environment. To date, the United States policy appears to be largely based on the principle "first do no harm." The restraint shown thus far can be credited with providing the room for all affected parties to wrestle with the difficult issues presented by this new environment and move towards consensus. The principles to be abided by, and to some extent the enforcement schemes, are becoming more robust. Most importantly, the dialogue in recent months, evidenced by developments such as the recently passed Children's Online Privacy Protection Act ("COPPA")[6]—which was supported by children's advocates, privacy advocates, and companies—has taken an important turn. Less is heard about the means to achieve privacy protection—self-regulation versus legislation—and more focus is on the ends—privacy protections for individuals. These developments provide tangible evidence that common ground is within reach.

While expectations of privacy are under serious challenge, the self-interest of the various constituencies that make up the Internet—users, advocates, industry, and government—are all pushing toward the adoption of

---

2. Center for Democracy & Technology, *Privacy Not Price: Keeping People Off The Internet, CDT's Analysis of Recent Privacy Surveys* <http://www.cdt.org/privacy/survey/findings/surveyframe.html>.

3. *TRUSTe: Building a Web You Can Believe In* <http://www.etrust.org/>[hereinafter *TRUSTe*].

4. *BBB Online* <http://www.bbbonline.org/privacy/fr_bd_ix.html>.

5. *Online Privacy Alliance* <http://www.privacyalliance.org/>.

6. 15 U.S.C.A. § 6501 (1998).

technologies and rules that provide individuals with greater control over their information and their privacy.

II. WHAT MAKES THE INTERNET DIFFERENT?

If we are to design systems that protect privacy on the Internet—a globally, networked environment—we must understand the specific challenges to privacy posed by its functions and use. The Internet presents a series of new challenges for achieving public policy goals—be they protecting children from inappropriate material or protecting privacy.

A. *Increased Data Creation and Collection*

The Internet accelerates the trend toward increased information collection, which is already evident in our offline world. The data trail, known as transactional data, left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. Transactional data, click stream data, or "mouse droppings," as it is alternatively called, can include the Internet protocol address ("IP address") of the individual's computer, the browser in use, the computer type, and what the individual did on previous visits to the Web site, or perhaps even other Web sites. This data, which may or may not be enough to identify a specific individual, is captured at various points in the network and available for reuse and disclosure. Some of the data generated is essential to the operation of the network, like the phone number that connects a calling party to the intended recipient, the IP address is necessary, for without it the network cannot function. However, other pieces of data may serve purposes beyond network operation. Along with information intentionally revealed through purchasing or registration activities, this transactional data can provide a "profile" of an individual's activities. When aggregated, these digital fingerprints reveal the blueprint of an individual's life. This increasingly detailed information is bought and sold as a commodity by a growing assortment of players.

B. *The Globalization of Information and Communications*

On the Internet, information and communications flow unimpeded across national borders. The Internet places the corner store, and a store three continents away, equally at the individual's fingertips. Just as the flow of personal information across national borders poses a risk to individual privacy, citizens' ability to transact with entities in other countries places individual privacy at risk in countries that lack privacy protections. National

laws may be insufficient, on their own, to provide citizens with privacy protections, across borders. Whether it is protecting citizens from fraud, limiting the availability of inappropriate content, or protecting privacy, governments are finding their traditional ability to make and effectively enforce policies challenged by the global communications medium.[7]

C. *Lack of Centralized Control Mechanisms*

While developing appropriate domestic policy may be sufficient in a paper-based world or a centralized and closed network, where nations can control the flow of information about citizens thereby protecting them from areas where protection is insufficient, information in a networked environment flows effortless from country to country, organization to organization, and policy regime to policy regime. Effective monitoring of the generation, collection, and flow of information on this vast scale may tax the resources of those currently responsible for data protection or other policies.

In addition to the difficulty of enforcing rules, governments around the globe are struggling with how to develop appropriate and effective rules. Efforts to use legal and regulatory instruments developed to address issues in other media—broadcast, telephone, print—may not be effective, and in cases like the United States' Communications Decency Act, may be found impermissible.[8] The need for global, decentralized solutions has prompted

---

7. The United States Congress' first effort to regulate speech on the Internet, the Communications Decency Act of 1996, Pub. L. No. 104–104, 110 Stat. 133 (codified as amended 47 U.S.C. 230 (1997)) [hereinafter "CDA"], was held to violate the First Amendment by the Supreme Court. Reno v. ACLU, 521 U.S. 844 (1997). Congress' second attempt, the Child Online Protection Act (Pub. L. No. 105-277, § 1401–06, 112 Stat. 2681 (1998)) (codified at 65 U.S.C.A. § 6501 (1998)) [hereinafter "CDA II"], is currently the subject of a legal challenge. On February 1, 1999, a federal district court issued a preliminary injunction prohibiting the government from enforcing CDA II until the court is able to issue a decision on its merits. ACLU v. Reno II, E.D. Pa. Case No. 98-5591, Preliminary Injunction Order (February 1, 1999). In contrast, the Clinton Administration's November report on Electronic Commerce advocates the voluntary use of filtering and blocking tools as the appropriate means of addressing concerns with children's access to inappropriate information on the internet. *See generally* U.S. Gov't Working Group, on Electronic Comm., First Annual Report (1998). The report also states that the Administration did not support CDA II. *See generally id.*

8. Concerns over children's access to inappropriate content were raised early on. Therefore, we have the most information about efforts to address this problem. We know that in the United States, applying standards developed for broadcast is unconstitutional. We have information about activities in other countries. Many have acknowledged the difficulty of controlling inappropriate content through regulation and are now looking toward decentralized user-controlled solutions to this problem. *See generally Global Internet Liberty Campaign Home Page* <http://www.gilc.org/>.

various international bodies including the European Union, the Organization for Cooperation and Development, and the United Nations to examine how to best advance their missions in this new environment.[9] As Dr. Malcolm Norris, Data Protection Commissioner for the Isle of Man, concluded in his paper, *Privacy and the Legal Aspects of the Information Superhighway*, "I believe the Internet will prove to be very difficult to govern in the way that Governments may wish."[10]

Together, the characteristics of the new medium pose challenges to our traditional, top-down methods of implementing policy and controlling behavior. Providing a seamless web of privacy protection to data as it flows through this international network will require us to harness the business community's interest in promoting commerce, the government's interest in fostering economic growth and protecting its citizens, and the self-interest of individuals in protecting themselves from the overreaching of the government and the private sectors. It requires us to use all of the tools at our disposal—international agreements, legislation, self-regulation, public education, and the technology itself. We must begin by reaching consensus on what we mean by protecting privacy, but we must keep the characteristics of the online environment sharply in focus. Concentrating in this manner is essential for the nature of the Internet and may alter the manner through which we achieve our goals.

III. WHAT DO WE MEAN BY PRIVACY? AND HOW IS IT BEING ERODED?

Privacy means many things to many people and different things in different contexts.[11] For the purpose of our discussion, we will examine

---

9. In October 1995, the European Union ("EU") adopted the Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 1995 J.O. (L28) 31. The Directive seeks to establish a common ground of privacy protection for personal data within the community and to ensure that the privacy of EU citizens was protected during "cross-border data flows,"—transfers of data to non-EU countries. *OECD guidelines on the Protection of Privacy and Transborder Flows of Personal Data* <http://www.oecd.org/dsti/sti/ii/secur/prod/PRIV_EN.HTM> [hereinafter *OECD Guidelines*]. Member States must comply with the Directive through the implementation of national provisions. *Id.* In February 1998, the OECD held a conference on Data Protection in International Networks. OECD Workshop on "Privacy Protection in a Global Networked Society" (February 1998) <http//www.oecd.org//dsti/sti/it/secur/prod/reg985final.pdf>. The Workshop provided an overview of various efforts to ensuring privacy protection. *See United Nations Human Rights Website*<http://www.unhchr.ch/html/menu3/b71.htm>.

10. Dr. Malcolm O. Norris, *Privacy and the Legal Aspects of the Information Superhighway* <http://www.odpr.org/restofit/Papers/Papers/Privacy_Internet.html>.

11. This discussion focuses primarily on information privacy. Information privacy

several core "privacy expectations"[12] that individuals have long held, and which should carry over to their interactions on the Internet that are under siege.

---

incorporates two components—at times distinct and at times inextricable—"the right to be let alone" first articulated by Justice Louis Brandeis over a century ago in his dissent in *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), and the right to control information about oneself, even after divulging it to others, as discussed by Professor Alan F. Westin in *Privacy and Freedom*. *See generally* ALAN F. WESTIN, PRIVACY AND FREEDOM (Atheneum 1967). While there is no definitive case finding a constitutional right for information privacy, the Supreme Court acknowledged that such a privacy right exists in *Whalen v. Roe*, 429 U.S. 589, 605 (1977) (upholding a state statute that required doctors to disclose information on individuals taking certain highly addictive prescription drugs for inclusion on a state database). "The information . . . is made available only to a small number of public health officials with a legitimate interest in the information . . . . Broad dissemination by state officials of such information, however, would clearly implicate constitutionally protected privacy rights . . . ." *Id.* at 606. The lack of strong constitutional privacy protection has placed added emphasis on federal and state statutory protections. *See, e.g.*, The Privacy Act of 1974, 5 U.S.C. § 552a; Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g; The Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401; The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (1995); The Communications Assistance and Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat 4279 (1994) (providing heightened protections for transactional data); The Cable Communications Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (1984) (codified as amended in scattered sections of 47 U.S.C.); The Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1994); Consumer Credit Reporting Reform Act of 1996, 15 U.S.C. 1681-s2 (1997); Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994 , 15 U.S.C. §§ 6101–6108; Driver's Privacy Protection Act of 1994, 18 USC § 2721 (1994); Privacy of Customer Information (The Customer Proprietary Network Information Rules of the Telecommunications Reform Act of 1996), 47 U.S.C. § 222 (c), (d) (1996). While statutory privacy protections for personal information have been crafted on a sector by sector basis, many are based on a common set of principles set forth in the *CODE OF FAIR INFORMATION PRINCIPLES*, which was developed by the Department of Health Education and Welfare in 1973. *See generally* DEPARTMENT OF HEALTH EDUCATION & WELFARE, *CODE OF FAIR INFORMATION PRINCIPLES* (1973), in SECRETARY'S ADVISORY COMMITTEE REPORT ON AUTOMATED PERSONAL DATA SYSTEMS, *Records, Computers and the Rights of Citizens*, U.S. DEPT. OF HEALTH, EDUC. & WELFARE, July 1973.

12. The phrase "expectations of privacy" is used here with intent. Despite case law suggesting that the legal protections afforded to our expectations of privacy are limited by the technical and social possibilities for surveillance, the authors believe that, as a society, we do share some basic expectations of privacy. Privacy legislation enacted by Congress in response to some of the Court's decisions lends some credence to this notion.

The "reasonable expectation" test was articulated in the seminal privacy case, *United States v. Katz*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring), in which the Supreme Court ruled that the Fourth Amendment protects "people, not places" from unwarranted searches and seizures. *Id.* at 351. Thereby reversing *United States v. Olmstead*, 277 U.S. 438 (1928), which held that the Fourth Amendment covered only physical places, and thus the warrant requirement did not apply

A. *The Expectation of Anonymity*

Imagine walking through a mall where every store, unbeknownst to you, placed a sign on your back. The signs tell every other store you visit exactly where you have been, what you looked at, and what you purchased. Something very close to this is possible on the Internet.

When individuals surf the World Wide Web, they have a general expectation of anonymity, more so than in the physical world where an individual may be observed by others. If an individual has not actively disclosed information about herself, she believes that no one knows who she is or what she is doing. But the Internet generates an elaborate trail of data detailing every stop a person makes on the Web. This data trail may be captured by the individual's employer if she logged on at work, and is captured by the Web sites the individual visits.[13] Transactional data, click stream data, or "mouse-droppings," can provide a "profile" of an individual's online life.

---

to police wiretaps. *Id.* at 361 (Harlan, J., concurring). Although hailed as a landmark privacy decision, the *Katz* test has been applied in later cases to undermine privacy interests. In *Katz's* progeny, the Court has applied the "reasonable expectation" test as a relative standard informed by the technological and social realities of the day. As technology has advanced, and as societal demands for sensitive personal information have increased, the Court has increasingly circumscribed the "zones" one may justifiably consider private. *See* California v. Greenwood, 486 U.S. 35, 40–41 (1988) (quoting United States v. Reicherter, 647 F.2d 397, 399 (3d Cir. 1981) (holding that people have no reasonable expectation of privacy in garbage once it is removed from the home and placed on the curb for pick-up, because garbage is placed "'in an area particularly suited for public inspection and . . . for the express purpose of having strangers take it'")); California v. Ciraolo, 476 U.S. 207, 214–15 (1986) (holding that the use of a fixed-wing aircraft to observe marijuana on defendant's property from 1,000 feet did not violate his protected "zone of privacy" because the defendant's subjective expectation of privacy was not one "that society is prepared to honor . . . [i]n an age where private and commercial flight in the public airways is routine."). The Court's application of this standard has proved particularly troublesome in the information privacy context. The Court has continually held that individuals have no privacy interest in information divulged to the private sector, even though modern society leaves citizens no option but to disclose to others, e.g., disclosure as a condition of participation in society and technology accumulating transactional data. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (holding that individuals have no privacy interest in the numbers dialed from their homes); United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that individuals have no reasonable expectation of privacy in personal financial records maintained by the bank). However, both *Smith* and *Miller* were later "overturned" by Congress through the enactment of statutes that created legally enforceable expectations of privacy. *See, e.g.*, 12 U.S.C. § 3401 (1994).

13. See The Center for Democracy and Technology's Snoop Demonstration at <http://snoop.cdt.org> for an example of the information that can be easily captured by sites on the World Wide Web.

Technologies such as "cookies,"[14] written directly onto your hard drive, enable Web sites to surreptitiously collect information about your online activities and store it for future use. Designed for the benign purpose of enabling Web sites to recognize a repeat visitor and respond accordingly, cookies were quickly adopted by Web sites to facilitate the tracking of specific individual's activities at Web sites for the purpose of customizing content and advertising. The surreptitious collection of information about individual's activities, across multiple Web sites enabled through some "cookie" implementations, gained the attention of Internet users, technicians, and policy makers.[15] Companies, such as Doubleclick, use this detailed transactional information to provide targeted online advertising. Others, such as Adfinity, combine these "mouse-droppings" or "click-stream data" with personal information collected from other sources into fully identifiable profiles of the individual's online and offline behavior.

The increased data collection enabled by the Internet and electronic commerce are part of a larger phenomena—the growing market in personal information. As one reporter stated:

> Let's face it: Companies are fascinated by me.
>
> Okay, maybe not me personally, but "me"—the consumer—collectively. I possess something nearly as valuable as spendable cash: information about myself. Before they can get to "me" to buy something, they need to know a lot about me: how old I am, how much I make, who I voted for, what I eat, wear, drive think or do.[16]

---

14. "Cookies" is a browser feature that assists Web site operators in tracking a user's activities. It was initially designed to address the "static state" problem of the World Wide Web, the fact that Web sites don't know whether a user is a first time or repeat visitor. *See* Joan E. Rigdon, *Internet Users Say They'd Rather Not Share Their 'Cookies,'* WALL ST. J., Feb. 14, 1996, at B6.

15. The initial response was the addition of a "cookie prompt" which alerts individuals that a Web site wishes to place a "cookie" on their browser. Peter Lewis, *Web Cookies: Trail of Crumbs*, SEATTLE TIMES: Search Results <http://archives.seattleti./display?storyID=55840 &query=cookie+AND+%22Ari+Schwartz%22>. Broader responses include the current attempt by members of the Internet Engineering Task Force ("IETF") to address privacy concerns with a rewrite of the "cookie" standard, and the availability of various technological tools that allow users to delete and/or disable "cookies." D. Kristol & L. Montulli, HTTP State Mangament Mechanism IETF Network Working Group, Request for Comments: 2109, D. Kristol Bell Laboratories, Lucent Technologies, L. Montulli Netscape Communications, February 1997 <http://www.ietf.org/rfc/rfc2109.txt>.

16. Paul Farhi, *ME INC.: GETTING THE GOODS ON CONSUMERS; Marketing Firms Want Basic Data About You and Me, But We're Wising Up to What Those Facts Are Worth*, WASH. POST, Feb. 14, 1999, at H01.

Evidence of the growing market for detailed "personal profiles" of individuals is rampant on the Internet. Be it personalized search engines and "portals," the pervasive use of "cookies" and other sticky bits of data that Web sites store on visitors' computers to aid the site in personalizing and targeting content and advertising, or the recent move by Intel to stamp each computer—and once the individual using the computer releases information, each individual—with a unique and traceable identity in cyberspace. The business communities rapacious appetite for information is all too apparent. Last August, some of the largest commercial sites on the World Wide Web announced that they would feed information about their customers' reading, shopping, and entertainment habits into a system developed by a Massachusetts company that was already tracking the moves of more than thirty million Internet users, recording where they go on the Internet and what they read, often without the users' knowledge.[17] In a sense, the system does what direct mail companies have done for years. But Internet based systems can be more precise, determining not only which magazines you subscribe to, but also which articles you read. More recently stories about "free" computers, valued at approximately $999, provided to individuals in exchange for detailed information about themselves and their families and permission to track their Internet usage, provide some indication of the value placed by a section of the business community on personal information and the lengths to which they will go to solicit it.[18]

While the private sector uses of personal information generated by use of the Internet have been scrutinized by the public and the press, the governments interest in and use of it has received less attention. But governments are interested in this data too. As the Federal Trade Commission revealed in its report to Congress on the Individual Reference Service Industry ("Look-up Services"), the government is a major customer of personal information about us.[19] While marketing information is not the fodder for "look-up services," it too is attractive to the government. A battle being waged today, over the "location" information available through many

17. Saul Hansell, *Big Web Sites to Track Steps of Their Users*, N.Y. TIMES ABSTRACT, Aug. 16, 1998, at 1, *available in* 1998 WL 5422846.

18. Karen Kaplan, *In Giveaway of 10,000 PCs, the Price is Users' Privacy Marketing: Recipients Must Agree to Let Pasadena Firm Monitor Where They Go on Internet and What They Buy*, L.A. TIMES, Feb. 8, 1999, at A1.

19. Individual Reference Services: FTC. *INDIVIDUAL REFERENCE SERVICES* 9 (Dec. 1997), *available in* 1997 WL 784156. The Individual Reference Services Industry is a sub-set of the information and industry which compiles information from the public and private sectors into information products that are used to locate, verify, and identify individuals, and provide dossiers of information about them. *See generally id.*

cellular networks, foreshadows the larger privacy considerations lurking in the vast data generated by individuals' use of the Internet.[20] In the course of processing calls, many wireless communications systems collect information about the cell site and location of the person making or receiving a call. Location information may be captured when the phone is merely on, even if it is not handling a call.[21] Both government and the private sector have their eye on this location information. While the government seeks to build added surveillance features into the network and ensure their access to the increasingly detailed data it captures, the private sector is considering how to use this new form of information. A company in Japan is experimenting with a World Wide Web site that allows anyone to locate a phone, and the person carrying it, by merely typing in the phone number.[22] As one reporter

---

20. In October of 1994, also commonly known as the "Digital Telephony" legislation, Congress enacted the Communications Assistance and Law Enforcement Act of 1994, providing heightened protections for transactional data. Pub. L. No. 103–414, 108 Stat 4279 (1994) (codified in scattered sections of 18 U.S.C. and 47 U.S.C.) [hereinafter "CALEA"]. The statute requires telecommunications carriers to ensure that their systems contain sufficient capability and capacity to permit law enforcement to conduct electronic surveillance. Although law enforcement officials must still obtain a search warrant in order to conduct a wiretap, the statute granted law enforcement new authority to influence the design of telecommunications networks. § 103(a), 108 Stat. at 4280.

Since its enactment, the Federal Bureau of Investigation ("FBI") has tried to use CALEA to require expanded surveillance features in the nation's telecommunications systems. Through statutory provisions which require public accountability and oversight over government design authority, telecommunications carrier liability, standards setting, and cost reimbursement, the Center for Democracy and Technology ("CDT") has attempted to curb the government's efforts to vastly increase surveillance capability. Telephone companies have yielded to some of the FBI's demands and have resisted others. In April 1998, acting upon a petition by CDT, the Federal Communications Commission ("FCC") launched an inquiry into whether the FBI's demands go farther than the law requires and infringe on privacy. Federal Communications Commission DA 98-762, *In the Matter of: Communications Assistance for Law Enforcement Act*, Docket No. 97-213 (April 20, 1998) (petition for Rulemaking under Sections 107 and 109 of the Communications Assistance for Law Enforcement Act, filed by the Center for Democracy and Technology). In September 1998, the FCC delayed implementation of CALEA by 20 months, until June 2000. In October 1998, the FCC tentatively approved many of the FBI's demands, including a proposal to turn cellular and other wireless phones into tracking devices. Action by the Commission, Memorandum Opinion and Order, FCC 98-223 (Sept. 10, 1998) (Chairman Kennard, Commissioners Ness, Powell and Tristani with Commissioner Furchtgott-Roth concurring and Commissioners Ness and Powell issuing a joint statement and Commissioner Furchtgott-Roth issuing a separate statement). At the same time, the FCC launched an inquiry into surveillance in pocket-switched networks. *Id.*

21. Albert Gidari, *Locating Criminals by the Book*, CELLULAR BUS., June 1996, at 70.

22. Edward W. Desmond, *The Scariest Phone System*, FORTUNE, Oct. 13, 1997, at 168.

put it: "Cellular telephones, long associated with untethered freedom, are becoming silent leashes."[23]

Now we head to the register. In the physical world, individuals can choose to purchase goods and services with a variety of payment mechanisms, the most common being cash, check, bank card, credit card, and a prepaid stored value mechanism, such as a travelers check or smart-card. Individuals can, and often do, pay by cash.[24] An individual's choice of payment mechanism impacts on her privacy. The amount of personal information generated and collected varies from theoretically none in a cash transaction to identity, item or service purchased, merchant, and date and time in a credit transaction. Similarly, the list of parties who have access to personal data can range from the individual and the merchant in a cash transaction, to the merchant, affiliated issuer, transaction processor, credit card company, and individual in a credit card transaction. In general, cash provides the most privacy protection during financial transactions in the offline world.[25] It is fungible, largely untraceable, and because its value is inherent and irrefutable, it requires no additional assurance of authenticity which often drives the collection of identity information.

In the online environment, the digital equivalent of cash has not yet achieved widespread use. Most online purchases are made with credit cards, which identify the individual and facilitate the collection of purchasing data. The lack of a cash equivalent in the online world, and its reduced use in the physical world, will seriously alter the privacy of individuals' financial dealings.[26]

For example, consider the differences between an auction/yard sale in the physical world and Ebay, the premiere auction/classified listing/yard sale on the World Wide Web. Attendees at a traditional auction while physically

23. Peter Wayner, *Technology that Tracks Cell Phones Draws Fire*, N.Y. TIMES ABSTRACTS, Feb. 23, 1998, at D3.

24. In many countries, offline consumer-initiated financial transactions are dominated by cash and checks. The reference is to the number of transactions not to the relative economic value they represent. Many of the transactions represented are likely to involve relatively modest sums. For example, newspaper purchases, meals, and phone calls to name a few. *See FRB: Federal Reserve Board Speech* from Mar. 7, 1997 <http://www.bog.frb.fed.us/boarddocs/speeches/19970307.htm> (remarks by Federal Reserve Board Chairman Alan Greenspan at the Conference on Privacy in the Information Age, Salt Lake City, UT, Mar. 1997).

25. However, even "ordinary cash itself, after all, is less than completely anonymous since it is usually exchanged in person, bears a unique serial number, carries fingerprints, and can easily be marked for identification." A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 471 (1996).

26. As financial transactions in the physical world continue to migrate to stored value cards, smart cards and chip-based systems, the need to build privacy protections into these payment systems becomes more urgent.

present do not reveal who they are prior to participation. At Ebay, prior to bidding individuals must provide a name, home address, phone number and e-mail address. The differences between the information collected to support a similar activity in these two environments to some degree reveals the increased emphasis placed on knowing the identity of the individual with whom you are interacting where the payment mechanism is less secure than what cash affords. The translation of cash, the most privacy protective of payment mechanisms, into an online equivalent, is a pressing privacy issue.[27] Without it we will quickly move from a world of cash-based anonymity to one of full identification and increased tracking of individuals' purchases.[28]

B. *The Expectation of Fairness and Control Over Personal Information*

When individuals provide information to a doctor, a merchant, or a bank, they expect that those professionals/companies will base the information collected on the service and use it for the sole purpose of providing the service requested. The doctor will use it to tend to their health, the merchant will use it to process the bill and ship the product, and the bank will use it to manage their account—end of story. Unfortunately, current practices, both offline and online, foil this expectation of privacy.

---

27. As Froomkin points out, a privacy-enhancing feature of digital cash transactions in general is that, unlike traditional financial transactions, they do not occur face-to-face. *Id.* at 471.

28. Law enforcement is eager to access the vast data available about individuals' financial transactions. Under a new set of proposed regulations, United States banks must monitor their customers and alert federal officials to "suspicious" behavior. The proposed regulations were filed with the Federal Register on December 7, 1998 by the Federal Deposit Insurance Corporation, the Federal Reserve, Department of the Treasury's Office of Comptroller of the Currency, and Office of Thrift Supervision. *See* Minimum Security Devices and Procedures and Bank Secrecy Act Compliance, 63 Fed. Reg. 67,529–67,536 (Dec. 7, 1998) (to be codified at 12 C.F.R. pt. 326). The regulations require banks to review every customer's "normal and expected transactions" and tip off the IRS and federal law enforcement agencies if the behavior is unusual. *Id.* Under the so-called "Know Your Customer" rules the Federal Reserve, the Office of Thrift Supervision, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation have published identical requirements. *Id.* Today, if a bank detects any "suspicious activity," they must file a five-page report including your name, address, Social Security number, driver license or passport number, date of birth, and information about the transaction. *Id.* Under the new regulations they will also have to determine the "source of a customer's funds"—such as payroll deposits—and authorize federal agents to inspect "all information and documentation" of accounts upon request. *Id.* The information all goes into the Suspicious Activity Reporting System, a mammoth searchable database jointly administered by the IRS and FinCEN, around since April 1996. Over a dozen agencies including the FBI, IRS, Secret Service, bank regulators, and state law enforcement share access to this data. Declan McCullagh, *Banking With Big Brother, Wired News* <http://www.wired.com/news/print_version/politics/story/16749.html?wnp g=all>.

Whether it is medical information, or a record of a book purchased at the bookstore, information generated in the course of a business transaction is routinely used for a variety of other purposes without the individual's knowledge or consent. Some entities go so far as to declare the information individuals provide them as company "property."

There are multiple examples of companies using and disclosing personal information for purposes well beyond what the individual intended. For example, recent news stories have focused the public on misuses of personal health information by the private sector—particularly when it is digitized, stored and manipulated. Recently, the Washington Post reported that CVS drug stores and Giant Food were disclosing patient prescription records to a direct mail and pharmaceutical company.[29] The company was using the information to track customers who failed to refill prescriptions, and then sending them notices encouraging them to refill and to consider other treatments.[30] Due to public outrage and perhaps the concern expressed by senators crafting legislation on the issue of health privacy, CVS and Giant Food agreed to halt the marketing disclosures.[31] But the sale and disclosure of personal health information is big business. In a recent advertisement Patient Direct Metromail advertised that it had 7.6 million names of people suffering from allergies, 945,000 suffering from bladder-control problems, and 558,000 suffering from yeast infections.[32]

While many expect strong concern for privacy to surround sensitive information such as health and financial records, several recent incidents involving the sale and disclosure of what many perceive as less sensitive information indicate a rising of privacy concerns among the public.[33] In recent years, a number of corporations, as well as government entities, have learned the hard way that consumers are prepared to protest against services that appear to infringe on their privacy. In 1996, public criticism forced Lexis-Nexis to withdraw a service known as P-Trak, which granted easy online access to a database of millions of individuals' Social Security numbers. Also in 1996, Yahoo faced a public outcry over its People Search service. The service, jointly run with a marketing list vendor, would have

29. *See* Robert O'Harrow Jr., *Prescription Sales, Privacy Fears, CVS, Giant Shares Customer Records With Drug Marketing Firm*, WASH. POST, Feb. 15, 1998, at A1.

30. *Id.*

31. *See* Robert O'Harrow Jr, *CVS Also Cuts Ties To Marketing Service; Like Giant, Firm Cites Privacy on Prescriptions*, WASH. POST, Feb. 19, 1998, at E1.

32. Cheryl Clark, *Medical Privacy is Eroding, Physicians and Patients Declare*, SAN DIEGO UNION TRIB., Feb. 21, 1998, at B2.

33. *Internet Power Feeds Public Fear*, USA TODAY, Aug. 13, 1997, at B1. When news spread across the Internet about the availability of individuals' Social Security numbers through the Lexis-Nexis service P-track the public and policy makers were outraged. Pat Flynn, *Lexis-Nexis E-Mail Scare Proves Wrong*, SAN DIEGO UNIONTRIB., SEPT. 21, 1996, at C1.

allowed Net searchers to put an instant finger on 175 million people, all culled from commercial mailing lists. After hearing the complaints, Yahoo decided to delete 85 million records containing unlisted home addresses. During August of 1997, American Online ("AOL") announced plans to disclose its subscribers' telephone numbers to business partners for telemarketing.[34] AOL heard loud objections from subscribers and advocates opposed to this unilateral change in the "terms of service agreement" covering the use and disclosure of personal information.[35] In response, AOL decided not to follow through with its proposal.[36] At the beginning of the year, the Washington Post reported that several states had entered into agreements to sell state drivers' license photos to Image data. Under public scrutiny the deal seemed quite different,—state governors and legislatures quickly moved to block the contract. Florida Governor Jeb Bush terminated the contract saying: "I am personally not comfortable with the state mandating license photos for the purpose of identifying authorized drivers, and then selling those photos at a profit for a completely different purpose."

The technologies' surveillance capacity to collect, aggregate, analyze and distribute personal information coupled with current business practices have left individual privacy unprotected. While recent surveys[37] and public pressure have raised the privacy consciousness of companies, particularly those operating online,[38] individuals' information is frequently used and disclosed for purposes well beyond what the individual provided it for.

---

34. Rajiv Chandrasekaran, *AOL Will Share Users' Numbers for Telemarketing*, WASH. POST, July 24, 1997, at E1; Rebecca Quick, *Soon AOL Users Will Get Junk Calls, Not Just Busy Signals and E-mail Ads.*, WALL ST. J., July 24, 1997, at B6. Its important to note that while AOL has been taken to task for failures to protect subscribers privacy, the AOL privacy policy has been recognized by many advocates as one of the best in the industry. *See Department of Commerce Workshop on Online Privacy*, June 1998 <http://www.doc.gov/>.

35. *See* Letter from the Center for Democracy and Technology, Electronic Frontier Foundation, EFF-Austin, National Consumers League, Privacy Rights Clearinghouse, and Voters Telecommunications Watch to Steve Case, President, AOL (on file with the author).

36. Rajiv Chandrasekaran, *AOL Cancels Plan for Telemarketing; Disclosure of Members' Numbers Protested*, WASH. POST, July 25, 1997, at G1.

37. For an overview of recent surveys of consumer concerns with privacy see, *The Center for Democracy and Technology*, <http://www.cdt.org/privacy/surveys/findings/introbody.html>.

38. The "Online Industry" has been active on the privacy front by creating self-regulatory principles, funding and developing mechanisms to provide accountability and service consumer complaints, and developing seals to identify Web sites that abide by industry-developed privacy guidelines. *See Online Privacy Alliance*, *supra* note 5; *BBB OnLine*, *supra* note 4; *TRUSTe supra* note 3.

C. *The Expectation of Confidentiality*

When individuals send an e-mail message, they expect that it will be read only by the intended recipient. Unfortunately, this expectation too is in danger. For starters, if an individual is using an office computer, it is possible, and legal, for her boss to monitor her messages. If she is using her home computer, her privacy is still not fully assured.

While United States law provides e-mail the same legal protection as a first class letter, the technology leaves unencrypted e-mail as vulnerable as a postcard. Compared to a letter, an e-mail message travels in a relatively unpredictable and unregulated environment. As it travels through the network, e-mail is handled by many independent entities: in comparison, a letter is handled only by the United States Postal Service. To further complicate matters, the e-mail message may be routed, depending upon traffic patterns, overseas and back, even if it is a purely domestic communication. While the message may effortlessly flow from nation to nation, the statutory privacy protections stop at the border. In addition, unlike the phone or postal systems, the Internet does not have central points of control. While the decentralized nature of the Internet allows it to cope with problems and failures in any given computer network, by simply routing in another direction, it also provides ample opportunities for those seeking to capture confidential communications.[39] The rogue action or policy of a single computer network can compromise the confidentiality of information.

But e-mail is just one example, today our diaries, our medical records, our communications, and confidential documents are more likely to be out in the network than under our bed. This has drastic consequences for our privacy—as information moves further out onto the network our existing statutory framework provides less and less protection.

It's useful to look at the weak state of privacy protections for other personal papers and records. Individuals traditionally kept their diaries under their mattress, in the bottom drawer of their dresser, or at their writing table. Situated within the four walls of the home, these private papers are protected by the Fourth Amendment. With the advent of home computers, individual diaries moved to the desktop and the hard drive. Writers, poets, and average citizens quickly took advantage of computers to manage and

39. Attempts to regulate the availability of encryption on the Internet highlight the frustrations that regulators may experience. As many scholars and advocates have pointed out, national attempts to restrict the availability of encryption are likely to be ineffective. For if even one jurisdiction or one network in one jurisdiction fails to restrict it, individuals worldwide will be able to access it over the Internet and use it.

transcribe their important records and thoughts. Similarly, pictures moved from the photo album to the CD-ROM.

Today, network computing allows individuals to rent space outside their home to store personal files and personal World Wide Web pages. The information has remained the same. A diary is a diary is a diary. But storing those personal thoughts and reflections on a remote server eliminates many of the privacy protections they were afforded when they were under the bed or on the hard drive. Rather than the Fourth Amendment protections—including a warrant based on probable cause, judicial oversight, and notice—the individual's recorded thoughts may be obtained from the service provider through a mere court order with no notice to the individual at all.

The weak state of privacy protection is evident in the business setting too. Let's look at medical records. Hospitals, their affiliated clinics, and physicians are using intranets to enable the sharing of patient, clinical, financial, and administrative data. Built on Internet technologies and protocols, the private networks link the hospital's information system, to pharmacy and laboratory systems, transcription systems, doctor and clinic offices and others. The United States government is contemplating the development of a federal government-wide computer-based patient record system.[40] According to news reports, the Internet and World Wide Web-based interfaces are under consideration.[41] The private sector is moving to integrate network computing into a sensitive area of our lives, the doctor's office.[42]

As computing comes to medicine, the detailed records of individuals' health continue to move not just out of our homes, but out of our doctor's offices. While the use of network technology promises to bring information to the fingertips of medical providers when they need it most, and greatly ease billing, prescription refills, and insurance preauthorizations, it raises privacy concerns.

In the absence of comprehensive federal legislation to protect patient privacy, the legal protections afforded medical records may vary greatly depending upon how the network is structured, where data is stored, and how long it is kept. If records are housed on the computer of an individual

---

40. *Why the Government Wants a Computerized Patient Record*, Health Data Network News, Vol. 7, No. 6, Mar. 20, 1998, at 1.

41. *Id.* at 8.

42. *See generally Six Boston Hospitals Turn To the Internet as a Clinical Network Tool*, Health Data Network News, Vol. 6, No. 6, June 20, 1997, at 1; *More Clearinghouses Conclude the Internet Makes Economic Sense*, Health Data Network News, Vol. 6, No. 6, June 20, 1997, at 1; *Hospital Banks on Web Technology for Integration*, Health Data Network News, Vol. 6, No. 16, Nov. 20, 1997, at 3.

doctor then access to that data will be governed by the Fourth Amendment.[43] Law enforcement would be required to serve the doctor with a warrant or subpoena and the doctor would receive notice and have the chance to halt an inappropriate search. Under federal law, the patient however, would receive no notice and have no opportunity to contest the production of the records. When information is in transit between a doctor and a hospital through a network, law enforcement's access is governed by the warrant requirements of The Electronic Communications Privacy Act of 1986 ("ECPA"); and, neither doctor nor patient receive prior or contemporaneous notice. If the records are stored on a server leased from a service provider, the protections are unclear. They may be accessible by mere subpoena. If they are covered by the "remote computing" provisions of ECPA this would severely undermine privacy in the digital age.[44]

The confidentiality of our sensitive information is challenged by a legal framework that hinges protections on who maintains the information, how the network is structured, where data is stored, and how long it is kept. As our wallets become "e-wallets" housed somewhere out on the Internet rather than in our back-pockets, and as our public institutions, businesses, and even cultural institutions find homes online, the confidentiality of our communications, papers, and information is at risk of compromise.

IV. WHERE DO WE GO FROM HERE?

It is clear that our existing legal framework did not envision the pervasive role information technology would play in our daily lives. Nor did it envision a world where the private sector would collect and use information at the level it does today. Our legal framework for protecting individual privacy in electronic communications while built upon constitutional principles and statutory protections, reflects the technical and social "givens" of specific moments in history. From a belief that the government's collection and use of information about individuals' activities and communications was the only threat to individual privacy and that a solid wall separated the data held by the private and public sector; to the notion that the Internet would be used primarily for a narrow slice of activities and that private and public spaces were easily demarcated, these

43. The recordkeeper would have Fourth Amendment protections. Whether the patient's privacy is protected at all would largely depend upon state law, which is scattered and inconsistent. Until a federal law protecting individual's privacy in health information is crafted to protect data regardless of where it is stored or whose control it is under, privacy is in danger.

44. 18 U.S.C. § 2703(b) (1994).

vestiges of a pre-Internet, pre-networked world, stress our existing privacy framework.

Crafting proper privacy protections in the electronic realm has always been a complex endeavor. It requires a keen awareness of not only changes in technology, but also changes in how the technology is used by citizens, and how those changes are pushing at the edges of existing laws. From time to time these changes require us to reexamine our fabric of privacy protections. The issues raised in this article indicate that it is time for such a review.

The Internet has changed the quantity and quality of data available about individuals' lives, but unfortunately our business practices, norms, and laws have not progressed to ensure individuals' privacy. At the outset, there are six areas where we must step up our activities to strengthen privacy protections. Clear proposals can be attached to some, while at this time others require further consideration.

A. *Maintain a Consistent Level of Privacy Protection for Communications and Information Regardless of Where They are Stored*

Increasingly, our most important records are not "papers" in our "houses" but "bytes" stored electronically at distant "virtual" locations for indefinite periods of time and held by third parties. As discussed in Part I, the Internet, and digital technology generally, accelerate the collection of information about individuals' actions and communications. Our communications, rather than disappearing, are captured and stored as well on servers controlled by third parties. With the rise of networking and the reduction of physical boundaries for privacy, we must ensure that privacy protections apply regardless of where information is stored.

Under our existing law, there are now essentially four legal regimes for access to electronic data: 1) the traditional Fourth Amendment[45] standard for records stored on an individual's hard drive or floppy disks; 2) the Title III-Electronic Communications Privacy Act[46] standard for records in transmission; 3) the standard for business records held by third parties, available on a mere subpoena to the third party with no notice to the individual subject of the record;[47] and 4) for records stored on a remote server such as the research paper, or the diary, of a student stored on a university server, or the records, including the personal correspondence, of

45. U.S. CONST. amend. IV.
46. 18 U.S.C. §§ 2570–2711 (1994).
47. Fed. R. Civ. P. 45(b)(1).

an employee stored on the server of the employer, the scope of which is probably unclear.

As the third and fourth categories of records expand because the wealth of transactional data collected in the private sector grows and people find it more convenient to store records remotely, the legal ambiguity and lack of strong protection grows more significant and poses grave threats to privacy in the digital environment. Independent Counsel Starr's investigation into books purchased by Monica Lewinsky highlights the potential sensitivity of records routinely collected by businesses and the intersection of privacy and First Amendment concerns.[48] During his investigation into President Clinton's relationship with White House intern Monica Lewinsky, Starr sought information confirming the purchase of a specific book by Miss Lewinsky. Starr served a subpoena upon Kramer Books, a local DC bookstore, demanding the production of records reflecting purchasing activities.[49] While the book store valiantly objected to the subpoena on First Amendment and privacy grounds, and Starr eventually obtained Miss Lewinsky's records through other channels, this incident raised concern among the book-buying public.[50] To search Miss Lewinsky's residence for information about her reading habits Starr would have needed a warrant, but in the hands of the bookstore the records were available under a less stringent standard.

Sometimes the equation is flipped—the government has collected the data and the private sector seeks access to it. During the law suit brought by several states, including Massachusetts, against the tobacco industry for repayment of state health care costs for smoking related illnesses, lawyers for the tobacco industry sought access to a Massachusetts database containing records on every hospital visit by every person in the entire state population.[51] While the State's purpose for collecting the data was to compare what it paid for health care to private insurers, it failed to enact privacy protections to limit access to the database.[52] Because the State's argument for repayment was premised on its ability to prove damage to state residents from tobacco products, the tobacco companies wanted to see the data supporting it.[53] Massachusetts acted responsibly, hiring a team of

48. DAVID STOUT, *Lewinsky's Bookstore Purchases Are Now Subject of a Subpoena*, N. Y. TIMES, Mar. 25, 1998, at A1.

49. DOREEN CARVAJAL, *Testing a President: The Investigation; Book Industry Vows to Fight 2 Subpoenas Issued Kenneth W. Starr*, N.Y. TIMES, Apr. 2, 1998, at A1.

50. STEPHEN LABATON, *Lewinsky's Lawyers to Turn Over Records of Book Purchases*, N. Y. TIMES, June 22, 1998, at A1.

51. John Schwartz, *Private Data, Public Worries*, WASH. POST, June 8, 1998, at F24.

52. *Id.*

53. *Id.*

cryptographers to ensure that the data released wouldn't identify individuals, however the fact remains that the data was not protected by law.[54]

Even our communications are vulnerable under today's law. Under the existing legal framework, the same e-mail message would be afforded different privacy protections depending on whether it was sought: while on the individual's computer; in transmission; unread in storage for less than 180 days; or, read but left on the service provider's server. The differences in protection afforded e-mail depending on whether it is captured in transmission, accessed in storage while unread, or accessed in storage after it has been read seem unwarranted, for the communication and individuals' expectations of privacy remain the same. In an era where e-mail is more commonly accessed as a stored record than through an interception, the concepts developed for governmental access to business records in the relatively static, paper-based environment are an ill-fit and provide weak protections for individual privacy. It is time to provide a framework that reflects individuals' expectations.

B. *Raise the Legal Protections Afforded to Transactional Data When it is Collected*

Where information is needed, we must ensure that it is protected from misuse and unfettered government access. Congress acted by legislation to establish a right of privacy in bank records in the wake of a Supreme Court decision finding they were without constitutional protection.[55] Institutions all across the economy are quickly becoming store houses of information about individuals' marketplace behaviors,—unlike records held by banks, these new databases are unprotected. The possibilities of computer analysis have given value to tidbits previously considered meaningless: the little digital footprints individuals leave showing who they called, where they used their credit cards, what websites they visited, what products they purchased, and when they entered the "intelligent" highway using the automatic toll booth. While a certain website or product registration card may only ask for a few minor pieces of personal information, together they constitute a fairly complete profile of one's associations, habits, health condition and personal interests, combining credit card transactions with magazine subscriptions, telephone numbers, real estate records, car registrations and fishing licenses.[56] The digital deposits of these transactional

54. *Id.*

55. United States v. Miller, 425 U.S. 435 (1976).

56. ROBERT O'HARROW, JR., *Data Firms Getting Too Personal?*, Wash. Post, Mar. 8, 1998, at A1.

details are so deep that the practice of exploiting their commercial value is called "data-mining," evoking the intensive, subterranean, and highly lucrative labors of an earlier age.

It's time to ensure that the records of our reading habits, our online browsing, and all the details of our lives left behind, online and in electronic commerce, are not treated as mere "business records" available, without our knowledge or permission, at the government's request. For even the most mundane of records can harbor risks to privacy. A December Washington Post article revealed that Drug Enforcement Administration ("DEA") officials were reviewing records of grocery store purchasing data collected to support "frequent shopper" or loyalty programs.[57] What would DEA officials possibly hope to uncover? According to the Post, they were seeking to identify purchasers of large numbers of small plastic bags and baking powder — common grocery supplies used by drug dealers to dilute and package cocaine and other drugs.[58] As businesses intensify their data collection efforts we must take steps to strengthen the privacy protections afforded this data.

Congress took the first small step towards recognizing the changing nature of transactional data in the networked environment with amendments to the Electronic Communications Privacy Act[59] enacted as part of the Communications Assistance for Law Enforcement Act of 1994 ("CALEA").[60] The 1994 amendments recognized that transactional data was emerging as a hybrid form of data, somewhere between addressing information and content, and was becoming increasingly revealing of personal patterns of association. For example, addressing information was no longer just a number and name, but contained the subject under discussion and information about the individual's location. Therefore, Congress raised the legal bar for government access to transactional data by eliminating subpoena access and requiring a court order, albeit one issued on a lower relevance standard.[61] This Congress passed legislation to foster online interactions between citizens and the government by facilitating the

57. ROBERT O'HARROW, JR., *Bargains at a Price Shoppers' Privacy, Cards Let Supermarkets Collect Data,* WASH. POST, Dec. 31, 1998, at A1. *See also* ROBERT O'HARROW, JR. *Behind the Instant Coupons, A Data Crunching Powerhouse*, WASH. POST, Dec. 31, 1998, at A20.

58. ROBERT O'HARROW, JR., *Bargains at a Price Shoppers' Privacy, Cards Let Supermarkets Collect Data,* WASH. POST, Dec. 31, 1998, at A1.

59. 18 U.S.C. §§ 2510–2711 (1994).

60. Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. § 1001 and scattered sections of 18 U.S.C. and 47 U.S.C.).

61. 18 U.S.C. § 2703(b)(2)(A)–(B), (c)(1)(B), (d) (1994).

government's acceptance of digital certificates.[62] The legislation includes forward looking privacy protections for the transactional data generated by citizens' use of digital certificates.[63] On a case by case basis, the courts are addressing the privacy issues raised by this revealing data. However, as electronic commerce becomes pervasive, transactional data will continue to proliferate. A piecemeal approach may not provide the privacy protections that this potentially sensitive information deserves.

C. *Encourage Technologies that Limit the Collection of Personally Identifiable Data*

Law is only one tool for protecting privacy. In this global, decentralized medium, we must promote applications of technology that limit the collection of transactional information that can be tied to individuals.[64] Some tools developed to protect privacy by limiting the disclosure, or cloaking it, of information likely to reveal identity, or decoupling this identity information from the individual's actions and communications, exploit the decentralized and open nature of the Internet.[65] For example, Crowds provides anonymity to individuals surfing the Web by mingling their requests for access to Web sites with those of others.[66] By routing Web site access requests in a series of unpredictable paths, the identity of the requester is hidden. Similarly, Onion Routing uses the decentralized nature of the Internet coupled with public key encryption to provide privacy protections for Internet communications.[67] Communications

---

62. The Government Paperwork Elimination Act, Pub. L. No. 105–277, §§ 1701–1710, 112 Stat. 2681, 2681–749 (1998) (codified at 44 U.S.C.A. § 101 (1998)).

63. § 1708, 112 Stat. at 2681–750.

64. For a thoughtful discussion of the privacy protection possible through technologies that limit data collection, see THE NETHERLANDS AND INFORMATION AND PRIVACY COMMISSIONER, I, II *Privacy-Enhancement Technologies: The Path to Anonymity* (Ontario, Canada Aug. 1995) [herinafter NETHERLANDS]. In his paper, "Privacy-Enhancing Technologies: Typology, Critique, Vision," Herbert Burkert suggests that Privacy-Enhancing Technologies ("PETs") can be differentiated into four categories: subject-oriented; object-oriented; action-oriented; and, system-oriented. Burkert's approach provides a heuristic method useful for thinking broadly about the role of PETs. Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision*, in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE, 125–142 (Philip E. Agre & Marc Rotenberg, eds. MIT Press 1997).

65. For a review of several privacy-enhancing technologies see, volume 42, no. 2, Feb. 1999 of the Communications of the ACM on Internet Privacy, guest editor Lorrie Faith Cranor. February 1999.

66. *Crowds Home Page* < http://www.research.att.com/projects.crowds/>.

67. David Godschlag et. al., *Onion Routing: Publications Onion Routing for Anonymous and Private Internet Connecting* <http://www.onionrouter.net/publications/html>.

are passed through a series of routers before reaching the recipient. Resembling an onion, the message is encircled in a series of layers. Each router is able to peel one layer of the onion enabling it to learn the next stop in the messages path. Passing messages in this fashion protects an individual's identity by obfuscating the originator and recipient of the message from points in the network. These technical advances, if adopted by users, can provide protections for privacy.

Of particular importance are payment mechanisms that preserve anonymity. By using cash, individuals can engage in many daily transactions without revealing their identity. Depending on the design choices we make, the online environment could wipe out the expectation of privacy that the physical world's cash purchase provides or the technology of electronic payments could preserve privacy. Similarly, digital certificates, if guided by privacy concerns, could be designed to limit the instances in which identity is used as a broad substitute for specific traits or abilities.

A number of companies have attempted to craft cash-like payment mechanisms.[68] Digicash is a frequently mentioned payment mechanism that provides cash-like anonymity to individual users.[69] Digicash relies on blind digital signatures, a cryptographic technique, to prevent the bank, or other money issuer, and merchant from linking the individual's identity to specific transactions.[70] Blind signatures provide the merchant with the ability to determine the value and establish the authenticity of the payment while shielding the individual's identity. The bank, while privy to information about the user's identity, and able to deduct the appropriate sum from the individual's account, is incapable of tying the particulars of a transaction to the individual.[71]

---

68. Catherine Lee Wilson, *Banking on the Net: Extending Bank Regulation to Electronic Money and Beyond*, 30 CREIGHTON L. REV. 671 (1997).

69. *Digi-Cash Welcome* <http://www.Digi-Cash.com./digicash/index.html>. However, unlike cash, Digi-Cash in its current applications does not provide anonymity to the recipient. Generally, other available digital cash systems use digital signatures but do not provide for anonymity.

70. *Ecash-An Introduction to ecash* <http://www.digicash.com/ecash/intro/index.html>. Digi-Cash couples its blind digital signature technology with online clearing of transactions. *Id.* Online clearing of transactions means that prior to accepting a payment the recipient is able to check to ensure the obligation will be met. *Id.* This is similar to the online check used in credit card authorization. *Id.*

71. *Id.* The decoupling of accounting and identity are facilitated by front-end debiting. The user produces a digital document containing both her identity and a pseudonym. She sends it to her bank with only the identity readable. The bank verifies the document, deducts the appropriate amount from her account, and sends it back to the user as a document of fixed value with a stamp indicating its authenticity. The user then gives the digital document to a merchant obscuring her identity and revealing her pseudonym. The merchant can read the value and the

The ability to engage in cash-like transactions in the online environment is important to the protection of privacy. The enhanced data generation and collection that occurs during the process of browsing a virtual store front, a merchant's World Wide Web site, increases the privacy concerns associated with the revelation of identity during the payment process. The capacity to connect information far in excess of the specifics of a given financial transaction to the individual's identity increases the risks to individual privacy relative to the concerns in the offline world.

Digital cash technology can vastly reduce the need for the collection and revelation of identity information. By providing alternative methods of authenticating value, the online environment can afford cash-like anonymity while providing some of the protections against theft associated with traditionally data intensive payment mechanisms. For example, Digicash's reliance on blind digital signatures may limit the risk of theft by providing for non-identity dependent methods of verifying the transaction at the point that value is removed from the individual's account.

The development of electronic payment mechanisms that protect privacy hinges on the use of strong cryptography and the creation of a robust public key infrastructure to support its use.[72] By designing payment mechanisms to limit the collection of personally identifiable information by banks, clearinghouses, and merchants, it is possible to preserve the privacy which individuals currently enjoy during cash transactions and perhaps move the developers of other payment mechanisms to enhance privacy protection. The private sector and the government should foster the development of payment mechanisms and other technologies that foster anonymity and privacy.

D. *Establish Rules and Implement Technologies That Give Individuals Control Over Personal Information During Commercial Interactions*

We must adopt enforceable standards, both self-regulatory and regulatory, to ensure that information provided for one purpose is not used or redisclosed for other purposes. At the same time, we must recognize that in this freewheeling, open marketplace, there will be limits to the effectiveness of regulation and self-regulation. Therefore, we must look to technological tools that will empower individuals to control their personal information.

---

stamp on the document indicating its authenticity. When presented to the bank the merchant's account will be credited. *See* NETHERLANDS, *supra* note 64, at 40–42.

72. Law enforcement desires to monitor financial transactions and the interest of merchants and others involved in commerce in exploiting data about individuals for marketing purposes may be a barrier to the market adoption of privacy-protective electronic payment mechanisms.

The Federal Trade Commission and the Department of Commerce are engaged in initiatives designed to promote "fair information practice principles" in the online environment. The business community is also engaged in efforts to protect privacy through self-regulatory guidelines and enforcement mechanisms. All such efforts should focus on the Code of Fair Information Practices ("CFIP") developed by the Department of Health, Education and Welfare ("HEW") in 1973[73] and the Guidelines for the Protection of Privacy and Transborder Flows of Personal Data, adopted by the Council of the Organization for Economic Cooperation and Development in 1980.[74] Coupled with the World Wide Web Consortium's Platform for

---

73. Secretary's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens,* U.S. Dept. of Health, Education and Welfare, July 1973.

> There must be no personal data record-keeping systems whose very existence is secret.
>
> There must be a way for an individual to find out what information about him is in a record and how it is used.
>
> There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
>
> There must be a way for the individual to correct or amend a record of identifiable information about him.
>
> Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

Id.

74. 1. Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data quality: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose specification: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the "purpose specification" except: (a) with the consent of the data subject; or (b) by the authority of law.

Privacy Preferences ("P3P")[75], rules based on the FIP will provide a framework that protects privacy by limiting data collection to that which is necessary for transactions and ensuring that individuals are the arbiters of their personal information. The challenge of implementing privacy practices, such as notice and consent, on the Internet is ensuring that they are implemented in a fashion that builds upon the medium's real-time and interactive nature and uses it to foster consumer privacy.

While the path to this policy is currently quite contested, there is some indication of a growing willingness to collaborate in order to develop privacy protections. Debate over the capacity of self-regulation and market forces to adequately address privacy concerns is common in the privacy and consumer protection arenas, and will continue to rage. Advocates often take the position that self-regulation is inadequate due to both a lack of enforcement and the absence of legal redress to harmed individuals. Industry tends to strongly favor self-regulation, stating that it results in workable, market-based solutions while placing minimal burdens on affected companies. These positions, while in tension, have both accurately

---

5. Security safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual participation: An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him:

- within a reasonable time;
- at a charge, if any, that is not excessive;
- in a reasonable manner; and,
- in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and, (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified completed or amended.

8. Accountability: A data controller should be accountable for complying with measures which give effect to the principles stated above.

OECD Guidelines, supra note 9.

75. For an overview, *see* Joseph Reagle & Lorrie Faith Cranor, *The Platform for Privacy Preferences*, Comm., at 48–55.

described the self-regulatory process. A close look at the enactment of federal privacy legislation over the years reveals that the battle itself, with all its sound and fury, is the path to legislation.

Historically, for privacy legislation to garner the support of at least a section of the industry, which is generally critical to successful legislative efforts, it must build upon the work of some industry members—typically binding bad actors to the rules being followed by industry leaders—or, be critically tied to the viability of a business service or product as with the Video Privacy Protection Act and the Electronic Communications Privacy Act.[76]

---

76. The Electronic Communications Privacy Act of 1986 (ECPA), which updated the 1968 Wiretap Act, was the result of a collaborative public interest/private sector effort. 18 U.S.C. §§ 2510–2711 (1994). Industry feared that without legal protection against eavesdropping and interception, consumers would be reluctant to use emerging electronic media, such as cellular phones and e-mail, to communicate. The resulting law extended legal protection akin to that provided First Class mail, and was developed and supported by a diverse coalition of business, civil liberties, and consumer advocates who understood that consumers would be unwilling to fully embrace electronic mail and other new technologies without strong privacy protections.

Similarly, the 1995 amendments to ECPA crafted privacy protections for transactional information that was content-like in its ability to reveal facts about a person's life. In these instances, developing and enacting a legislative privacy regime was viewed by the business community as a necessary component of creating and supporting a flourishing market for their products. The nexus between privacy protection and business necessity resulted in a diverse public interest/industry coalition supporting increased protections for transactional data. Communications Assistance and Law Enforcement Act of 1994, Pub. L. No. 103–414, § 207, 108 Stat. 4279 (codified at 18 U.S.C. §§ 2510—2711 (1994)). There is dispute over whether other sections of CALEA solve or create privacy problems.

Other privacy legislation supported by the public and private sectors The Cable Communications Privacy Act of 1986 and the Video Privacy Protection Act of 1988 reflect a similar coalescing of interests. Enacted within a couple of years of each other, both laws resulted from the affected industry's realization that a lack of assurance that viewing preferences were protected from prying eyes, would have a chilling effect on consumers' viewing and renting habits. The revelation in a Washington, DC, weekly paper, that a reporter,—or anyone for that matter—could walk in off the street and discover Supreme Court nominee Judge Bork's taste in movies provided privacy advocates with the perfect story to gain Congress's attention. Privacy advocates arrived on the Hill with Erols, the Video Software Dealer's Association, the Direct Marketing Association, and others who realized that the viability of their businesses depended on consumer trust and confidence that video rental lists were safeguarded by strong legal restrictions on government and private sector access.

In other instances, industry has been moved to support privacy legislation in the wake of public revelations of bad practices or a particularly compelling horror story. The Fair Credit Reporting Act of 1970 ("FCRA") was initially drafted and supported by the credit reporting industry in response to congressional hearings which revealed widespread misuse of credit

Today, the dialogue over assuring privacy on the Internet and in electronic commerce is well situated for a successful legislative effort. Privacy-aware companies are seeking to develop and implement self-regulatory programs. Surveys have shown that the viability of online commerce depends upon the existence of real protections for consumers' privacy. Similar to the development of early privacy laws, some industry actors have led the way crafting self-regulatory policies that are the prototype for subsequent legislation supported by self-regulated players who for reasons of public trust, liability, and/or government concern want to bind bad industry actors.

Advocates of both self-regulation and legislation each have a vested interest in exploring and resolving the hard issues. Questions of what is personally identifiable information in the context of the Internet, what does access require, and what is the appropriate way to police and provide remedies in this environment must all be explored. The work of the Online Privacy Alliance to develop principles to protect children's privacy became a starting point for the recently passed Children's Online Privacy Protection Act.[77] The collective desire to provide privacy protections that protect individuals' privacy, and encourage them to participate in the online environment, provides the common ground for the development of sound policies and enforcement strategies in the coming year.

E. *Create a Privacy Protection Entity to Provide Expertise and Institutional Memory, a Forum for Privacy Research, and a Source of Policy Recommendations on Privacy Issues*

The work outlined above, and the state of privacy today, all weigh in favor of creating a privacy entity within the federal government. The existing approach has hindered the development of sound policy and failed to keep pace with changes in technology. The United States needs an independent voice empowered with the scope, expertise, and authority to guide public policy. Such an entity has important roles to play on both

---

information and an alarming rate of inaccuracies in credit reports. An enraged Congress, with the support of privacy and consumer organizations, indicated a commitment to passing a law regulating the use of consumer credit information. Realizing that legislation was inevitable, the industry set about crafting a policy that they could support. The Driver's Privacy Protection Act of 1994 was largely triggered by the murder of actress Rebecca Shaffer and eventually garnered the support of the majority of the affected industries. Through information in her driver license file at the department of motor vehicles, Shaffer's stalker was able to learn her whereabouts.

77. The Privacy Act of 1974, 5 U.S.C. § 552a (1973).

domestic and international fronts. It would serve as the forum for collaboration with other governments, the public interest community, and the business community.

There are a myriad of functions an entity charged with promoting privacy could perform. Unfortunately, the debate over the scope and power of such an agency or office has consistently stymied attempts to create one. As in many areas, the perfect has been the enemy of the good. At this junction, foremost on this entity's agenda should be developing and articulating a comprehensive vision of privacy protection for the United States, and coordinating efforts to advance it in both the public and private sector. The emergence of the Internet and other advanced technologies require us to reflect, study, adapt, and apply existing privacy principles and at times develop new ones. Without expertise and devoted resources this task will not be undertaken.

To function well, such an entity should have the ability to

1. monitor and evaluate developments in information technology with respect to their implications for personal privacy;
2. conduct research, hold hearings, and issue reports on privacy issues in both the public and private sector;
3. develop and recommend public policy appropriate for specific types of personal information systems;
4. comment upon government and private sector proposals that impact on privacy;
5. review agency activities under the Privacy Act;
6. participate in government proposals that impact on privacy.[78]

The level of 1) public concern; 2) agency activity; 3) private sector investment; and 4) non-governmental organization focus on individual privacy, cry out for the formation of an entity able to comprehensively and effectively address privacy issues.

In July, Vice President Gore announced the Administration's intent to appoint an individual to oversee and coordinate the governments privacy

78. A number of these recommendations mirror those made by Flaherty in his recommended responsibilities for a United States privacy protection commission. He goes on to state that such a commission should have a statutory mandate and as much independence as possible from the executive and legislative branches of government. (source on file with author).

activities as part of the "Electronic Bill of Rights."[79] While the duties and powers of this individual are unclear, the announcement signals the Administration's recognition that privacy is an issue of growing importance and one that the Administration must play a role in coordinating. As of publication, no appointment has been made.

F. *We Must Question Our Tendency to Rely on Government as the Central and Sometimes Sole Protector of Privacy*

In the decentralized and global environment of the Internet, the law's impact will be limited. In an area such as privacy, where the government's actions have often been detrimental rather than supportive, we must ask if other options—such as technology may provide stronger protection. We must encourage the development and implementation of technologies that support privacy. They are critically important on the Internet and other global medium. Strong encryption is the backbone of technological protections for privacy. Today technical tools are available to send anonymous e-mail, browse the World Wide Web anonymously, and purchase goods with the anonymity of cash.

Public policy is quickly becoming as much a product of computer code and product decisions as law. Advocates who once focused nearly exclusively on federal and state legislatures and agencies are increasingly seeking to influence the design of technical standards and specifications, and even specific product designs. From the Internet Engineering Taskforce and the World Wide Web Consortium, to the United States Telephone Association, decisions that will affect the future of privacy are made each day. Advocates, the public, and policy-makers have taken fire at specific products ranging from Lexis-Nexis Ptrak[80] to the soon to be released Intel Pentium III Processor seeking to ward off privacy invasions. But as we ward off the bad, we must move for the development of the good—seeking to foster technologies,—both standards and specific products,—that protect privacy.

Future technical developments have the capacity to provide an underlying framework for privacy, providing greater anonymity, confidentiality, and a platform for fair information practices.[81] Technologies

---

79. *Vice President Gore Announces New Steps Toward an Electronic Bill of Rights* Presswire, July 31, 1998, at 1, *available in* 1998 WL 16515766.

80. *See supra* Part IV.

81. These incorporate the basic concepts of three recommendations of the Danish and Canadian Privacy Commissioners: 1) eliminate the collection of identity information, or if it is needed, keep it separate from other information; 2) minimize the collection and retention of identifiable personal information; and 3) make data collection and use transparent to data subjects

must be a central part of our privacy protection framework, for they can provide protection across the global and decentralized Internet where law or self-regulation may fail us.

V. CONCLUSION

No doubt, privacy on the Internet is in a fragile state, however, there is new hope for its resuscitation. The business community, enlightened by survey upon survey documenting consumers' privacy concerns, has recently begun serious efforts at self-regulation. The White House, the Federal Trade Commission, the Department of Commerce, and Congress all show interest in ensuring that privacy is protected as the digital economy is embraced. A growing number of advocacy organizations, ranging from consumer to civil liberties to libertarian organizations, have begun to focus on privacy. Thanks to the Internet, the public voice is being heard more clearly than ever—more often than not weighing in strongly in support of privacy protections through law and technology.

There is a special need now for dialogue. Providing a web of privacy protection to data and communications as they flow along networks requires a unique combination of tools—legal, policy, technical, and self-regulatory. Cooperation among the business community and the nonprofit community is crucial. Whether it is setting limits on government access to personal information, ensuring that a new technology protects privacy, or developing legislation—none will happen without a forum for discussion, debate, and deliberation.

---

and provide them with the ability to control the disclosure of their personal information, particularly identity information. *See supra* Part IV.

Amelia H. Boss
Professor Temple University, School of Law

Amelia H. Boss, a graduate of Bryn Mawr College and Rutgers-Camden Law School, is a Professor of Law at Temple University School of Law, where she teaches in the commercial law, bankruptcy, and electronic commerce areas. She is a member of the Permanent Editorial Board of the Uniform Commercial Code, and the former chair of the Uniform Commercial Code Committee of the American Bar Association. She serves as the American Law Institute member of the Drafting Committee to revise Article 2 of the UCC on sales, of the Drafting Committee on the new Article 2B on licensing of software, and of the Drafting Committee to revise Article 1 on general provisions. In the past, she served as an advisor/observer to the revisions on Article 5 (letters of credit) and Article 8 (investment securities). She is a member of the American Law Institute and served on the Members Consultative Group on the Restatement of the Law of Suretyship. Professor Boss is a member of the Council of the Section of Business Law of the American Bar Association, and will assume the role of secretary of the section in August. She is a member of the former fellow of the American College of Commercial Financial Lawyers and is a member of the Board of Directors of the Institute of International Commercial Law.

Professor Boss currently serves as advisor and as the United States Delegate to the United Nations Commission on International Trade Law (UNICITRAL) on issues relating to electronic commerce. She represented the U.S. in the development of the UNCITRAL Model Law on Electronic Commerce, and is now representing the U.S. in UNCITRAL work on digital signatures. She serves as the American Bar Associations representative to an effort by the National Conference of Commissioners on Uniform State Laws to draft a Uniform Electronic Commerce Act, dealing with *inter alia* with digital signatures. She is Editor-in-Chief of *The Data Law Report* (published bi-monthly by Clark Boardman Callaghan), is on the editorial board of *The EDI Law Review* and the *Journal of Bankruptcy Law and Policy*, and is the editor of the new book series, *ABC's of the UCC*, published by the American Bar Association.

Searching for Security in the Law of Electronic Commerce

Amelia H. Boss

TABLE OF CONTENTS

I. INTRODUCTION

Since before the time Gutenberg invented the printing press, centuries of jurisprudence have been devoted to and predicated upon paper-based systems of communication, particularly in the area of commercial law. With advances in technology and the implementation of electronic modes of communication in businesses and market places in general, however, the world has begun to move away from paper as the primary mode of communication and the primary method of doing business.[1] This continues the process begun with the introduction of the telegram and the telephone, both of which contributed to the elimination of paper in the conduct of business negotiations.

Electronic commerce, however, is fundamentally different from either telephonic or paper-based commerce. First, there is no tangible piece of paper that one can treat as the final expression of the parties' intent; reliance must be placed upon electronic messages, which are either stored in an electronic medium or, in the case of risk-averse business people, printed out at

1. According to the Organization for Economic Co-operation and Development ("OECD"), the volume of electronic commerce may rise to $1 trillion by 2005. Organization for Economic Co-operation and Development, *The Economic and Social Impacts of Electronic Commerce: Preliminary Findings and Research Agenda*, ch. 1 (1998) <http://www.oecd.org/subject/e_commerce/summary.htm>; *see generally Id.* at ch. 3. *See generally* U.S. Department of Commerce, *The Emerging Digital Economy* (1998) <www.doc.gov/ecommerce/EmergingDig.pdf>.

one end. Second, the electronic message is often generated by a computer and may not provide the typical indicia of trustworthiness. For example, with paper, we can recognize the handwriting, identify the stationery, check the postmark and address, and check for visible changes to the writing. On the telephone, we can recognize the voice and verify the number we are calling. Third, commercial transactions have traditionally required time and, frequently, additional verifiable information for completion. For example, in the sale of goods, the time between the execution of the sales agreement and the ultimate shipment or delivery of goods allows for verification of creditworthiness and of other information such as shipment details. Electronic transactions, on the other hand, are often executed online instantaneously between computers, and the ability to verify the identity of the parties and other information is radically reduced. Indeed, one emerging characteristic of much of electronic commerce, such as the web-based transaction, is the transitory nature of the relationship between the parties. Last, the tangible nature of the transaction, e.g., the sale of goods, has allowed for security measures such as the creation and potential enforcement of security interests in the property that was sold. By contrast, the subject matter of electronic commerce is increasingly intangible,[2] reducing the ability to monitor and enforce the obligations of the other party.[3]

---

2. Although tangible goods are frequently sold in electronic commerce, online transactions involving intangibles such as software and information are multiplying. On the emergence of a new species of property, information, as one important aspect of the development of electronic commerce, see Amelia H. Boss, *The Emerging Law of International Electronic Commerce*, 6 TEMP. INT'L & COMP. L.J. 293, 298–300 (1992); Katherine Mahoney, *Information as a Commodity: New Imperatives of Commercial Law*, 55 LAW & CONTEMP. PROBS. 77, 103 (1992); Raymond T. Nimmer & Patricia Ann Krauthaus, *Electronic Commerce: New Paradigms in Information Law*, 31 IDAHO L. REV. 937, 937 (1995); Margaret Jane Radin, *Property Evolving in Cyberspace*, 15 L.J. & COM. 509, 511–13 (1996). The increasing predominance of information as the subject matter of the deal has given rise to efforts to create legal structures accommodating these new transactions, the main one of which has been the drafting of a new article to the Uniform Commercial Code, Article 2B, to cover transactions in software and information, *see* U.C.C. art. 2B (Proposed Draft Dec. 1998), *available at* <http:www.law.upenn.edu/bll/ulc/ulc.htm#UCC2B>, or, alternatively, computer information transactions. *See* U.C.C. art. 2B (Proposed Draft Feb. 1, 1999), *available at* <http:www.law.upenn.edu/bll/ulc/ulc.htm#UCC2B>. Evolution of new types of transactions creates concern about the rules applicable to those transactions, and concomitantly, there is some desire for certainty and predictability in developing a legal framework. As with the case of electronic contracting, which is discussed in this article, there are instances where the demand for such rules may be misplaced, arising from the assumption that only positive law may create an environment where transactions may be trusted.

3. Traditional factors in commercial transactions that contribute to amicable and effective resolution of disputes, e.g., ongoing relationships between the parties, sufficient time to structure the transaction, and potential collateral, are often absent in online transactions.

The emergence of electronic commerce has raised a host of questions about our existing rules and legal system. One frequent plea is to remove the barriers to electronic commerce, barriers that are, to a great degree, the vestiges of a commercial law system based on paper. Legal requirements, such as those for a "writing," a "signature," and an "original" need to be reconsidered in the context of electronic commerce. Efforts are underway to respond to these demands in the following ways: in the domestic arena, the Uniform Commercial Code[4] and the proposed Uniform Electronic Transactions Act ("UETA");[5] and on the international level, the formulation of the United Nations Commission on International Trade Law ("UNCITRAL") Model Law on Electronic Commerce.[6]

---

4. Pending revisions to Article 2 of the Uniform Commercial Code, as well as the pending proposal to include computer information transactions in a new Article 2B, include provisions addressing the application of such requirements in an electronic environment. *See* Raymond T. Nimmer, *Article 2B: An Introduction*, 16 J. MARSHALL J. COMPUTER & INFO. L. 211, 227–37 (1997) (reviewing electronic and online commerce provisions of Article 2B); Raymond T. Nimmer, *Electronic Contracting: Legal Issues*, 14 J. MARSHALL J. COMPUTER & INFO. L. 211, 212 (1996); Amelia H. Boss, *Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform*, 72 TULANE L. REV. 1931, 1956–63 (1998) (reviewing the changes being made in Article 2B and the Uniform Electronic Transactions Act to accommodate electronic commerce). Other completed revisions to the Code do so through a variety of techniques. Article 5, for example, adopts terms such as "record" in place of "writing" and contemplates presentation of non-paper documents. *See* U.C.C. § 5-102 (a)(14) (1997) (defining record); *id.* § 5-102(a)(6) (defining document to include presentation in any media permitted by the letter of credit or standard practice); *id.* § 5-102 cmt. 2 (revised Article 5 "contemplates and facilitates the growing recognition of electronic and other nonpaper media as 'documents'"). *See also* R. David Whitaker, *Letters of Credit and Electronic Commerce*, 31 IDAHO L. REV. 699, 699–701 (1995). Article 8 eliminates any statute of frauds writing requirement for contracts transferring interests in securities. *See* James S. Rogers, *An Essay on Horseless Carriages and Paperless Negotiable Instruments: Some Lessons From the Article 8 Revision*, 31 IDAHO L. REV. 689, 691 (1995); U.C.C. § 8-113 (1997). Completed in 1999, revised article 9 also uses the terms "record" and "authenticate" in place of "writing" and "signed." U.C.C. § 9-102(a)(7) (authenticate); *id.* § 9-102(a)(69) (record).

5. Currently scheduled for completion in August of 1999, the Act contains electronic contracting rules for transactions outside the scope of the Uniform Commercial Code. *See Uniform Law Commissioners Drafts* <http://www.law.upenn.edu/bll/ulc/ulc.htm> (for drafts of the UETA).

6. The United Nations Commission on International Trade Law ("UNCITRAL") has taken the lead at the international level in formulating the law governing electronic commerce, and in 1996, it gave its final approval to a new Model Law on Electronic Commerce which contains many provisions adapting the formalities of the law to an electronic environment. *See* REPORT OF THE UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW ON THE WORK OF ITS TWENTY-NINTH SESSION, U.N. GAOR, 51st Sess., Supp. No. 17, U.N.Doc. A/51/17 Annex I (1996), *reprinted in* 36 I.L.M. 200 (1997). *See* Amelia H. Boss & Jane

In many arenas, however, demands are being made on legislators and lawmakers to go beyond mere removal of legal barriers and to "support" the development of electronic commerce by the establishment of a legal framework that encourages and promotes its use. The argument is that the law should build confidence in the system by providing rules that support and promote these new ways of doing business.

In many respects, these demands are quite understandable, as they combine two needs. The first is the perceived need for rules to guide conduct on the Internet. The public and the press have in recent years become so enamored of technology that they use phrases such as "revolutionary" to describe it. The characterization of cyberspace as something new and alien creates in people a fear that it is indeed unknown and unknowable, and people distrust the unknown. The result is concern about what will govern this unknown and uncharted territory. Some have argued that the Internet as a unique jurisdiction should be subject to its own body of rules,[7] while others have attempted to resolve issues on the Internet by analogizing it to other areas of law.[8] The real challenge is to examine the

---

Kaufmann Winn, *The Emerging Law of Electronic Commerce*, 52 BUS. LAW. 1469, 1469 (1997); Judith Y. Gliniecki & Ceda G. Ogada, *The Legal Acceptance of Electronic Documents, Writings, Signatures, and Notices in International Transportation Conventions: A Challenge in the Age of Global Electronic Commerce*, 13 NW. J. INT'L L. & BUS. 117 (1992); Daniel J. Greenwood & Ray A. Campbell, *Electronic Commerce Legislation: From Written on Paper and Signed in Ink to Electronic Records and Online Authentication*, 53 BUS. LAW. 307, 307–09 (1997) (comparing provisions of the UNCITRAL Model Law with domestic legislation). For an overview of the relationship between the domestic efforts and the international efforts, see *supra* note 4. There are, of course, other efforts both within UNCITRAL and other international organizations to consider other aspects of electronic commerce.

7. *See, e.g.*, David G. Post & David R. Johnson, *Chaos Prevailing on Every Continent: Towards a New Theory of Decentralized Decision-Making in Complex Systems*, 73 CHI. KENT L. REV. 4 (forthcoming 1999). In other contexts, the tendency to see the Internet as a separate place necessitating different legal rules has been criticized. Andrew L. Shapiro, *The Disappearance of Cyberspace and the Rise of Code*, 8 SETON HALL CONST. L.J. 703, 703 (1998) (concluding that the Internet is simply an alternative communications technology, and that there is no more a need for the 'law of cyberspace' than there ever was for the "law of the alphabet.").

8. One scholar surveyed the evolution of "Internet law," tracing it through two stages. In the first stage, the Internet was analogized to other areas where the legal doctrine was well established. In the second stage, a more advanced analysis focused on the nature and quality of the activity taking place. *See* Michael A. Geist, *The Reality of Bytes: Regulating Economic Activity in the Age of the Internet*, 73 WASH. L. REV. 521 (1998). Professor Geist's analysis was limited to developments in the area of jurisdiction and did not encompass the area of security and electronic commerce. Similarly, others trying to find trends in the law applicable to the Internet have focused on First Amendment issues. *See, e.g.*, Clay Calvert, *Regulating*

need for rules *in context* and determine whether the issue under consideration is sufficiently different in an Internet or online context to justify a different set of rules than would otherwise exist.[9]

The second need is security. In large part, the newness of the technology, unfamiliarity with the operation of the Internet, and the potential for fraud and error have given rise to concerns about the "trustworthiness" of the system. Indeed, "security" is one of the key words that is often bandied about in the context of electronic commerce; that is, the need for security and trustworthiness in online transactions.[10] Concerns about "security" are heard in all venues: legal,[11] technological,[12] business,[13] and theoretical.[14]

Cyberspace: Metaphor, Rhetoric, Reality and the Framing of Legal Options, 20 HASTINGS COMM. & ENT. L.J. 541, 554 (1998). Each area is distinguishable, however, from the concerns of the present Article. For example, in the area of jurisdiction, the primary forum for the development of "Internet law" has been the courts, not the legislature. By contrast, to date, the primary forum for the development of Internet law in the commercial context has been the private sector, and there have been few judicial decisions. Only recently have the legislatures become involved.

9. *See, e.g.*, Allan R. Stein, *The Unexceptional Problem of Jurisdiction in Cyberspace*, 32 INT'L LAW 1167, 1167 (1998) (arguing that "there is nothing about legal relations over computer networks that in any way challenges our conventional notions about how sovereign authority is allocated in the world"); Amelia H. Boss, *The Jurisdiction of Commercial Law: Party Autonomy in Choosing Applicable Law and Forum Under Proposed Revisions to the Uniform Commercial Code*, 32 INT'L LAW 1067, 1068 (1998) (nothing about electronic commerce requires different rules on enforceability of choice of law and forum clauses). In Canada, a study for the federal government reached the same conclusion. Industry Canada (1998), *The Internet is not a No-Law Land*, *available at* <http://strategis.ic.gc.ca/>. *See also* John D. Gregory, *Solving Legal Issues in Electronic Commerce*, CAN. BUS. L.J. (forthcoming 1999) (some legal issues in electronic commerce can be and are being resolved by application of existing rules, once people become familiar with the new medium).

10. A sampling of the legal literature in the area of electronic commerce demonstrates the currency of the theme of "security." *See Public Key Infrastructure Symposium*, 38 JURIMETRICS J. 241 (1998).

11. Frequently, the legal arguments concerning security focus on restrictions on cryptography. *See* STEWART A. BAKER & PAUL R. HURST, THE LIMITS OF TRUST: CRYPTOGRAPHY, GOVERNMENTS, AND ELECTRONIC COMMERCE (The Hague, London & Boston, 1998).

12. Recently, there has been an extensive amount of writing on concepts of trust from a technological perspective. *See, e.g.*, COMMITTEE ON INFO. SYS. TRUSTWORTHINESS, TRUST IN CYBERSPACE (Fred B. Schneider ed. 1999), *available at* <http://www.nap.edu/readingroom/>.

13. *See* Dan Greer, *Risk Management Is Where the Money Is*, THE RISKS DIG., Col. 20, Issue 6 (Nov. 12, 1998) <http://catless.ncl.ac.uk/risks/20.06/htm>: "The focus of 'security' research today is the study of 'trust management'—how trust is defined, created, annotated, propagated, circumscribed, stored, exchanged, accounted for, recalled and adjudicated in our electronic world." *Id.*

The need to provide "security" or "secure systems" for electronic commerce is being expressed not just at the technical and implementation levels but in legislatures as well.[15]

Combined with this is the reality that many legislators also want to be seen as at the cutting edge of technology and have introduced legislation at both the state and the federal levels.[16] State legislators, in particular, want to be the first to enact "electronic commerce" statutes, thereby attracting businesses into their region and appearing to be global leaders to their constituents. There might be, however, a problematic result: the passage of "technology" legislation that is premature and potentially counter-productive.[17]

II. THE NEED FOR SECURITY

Concerns about security, whether real or perceived,[18] need to be put into perspective. Security cannot be "legislated." It is a combination of factors: the technology utilized,[19] its business implementation and state of development, and the legal structure. Doing business "securely" on the information highway is not a simple matter of developing the right technologies to "lock up" information sent electronically to protect it against

14. Ed Gerck, *Towards Real-World Models of Trust: Reliance on Received Information* <http://www.mcg.org.br/trustdef.htm> (presenting an abstract definition of trust derived from different application areas, including communication systems, digital certificates, cryptography, law, linguistics, social sciences, etc.).

15. The United Kingdom has framed the issue as "building confidence in electronic commerce." *See Building Confidence in Electronic Commerce* (Mar. 5, 1999) <http://www.dti.gov.uk/cii/elec/elec_com.html>.

16. *See, e.g.*, Philip S. Corwin, *Electronic Authentication: The Emerging Federal Role*, 38 JURIMETRICS J. 261 (1998) (discussing federal bills during the 105th Congress).

17. Australian Electronic Commerce Expert Group, *Electronic Commerce: Building the Legal Framework*, Executive Summary <http://www.law.gov.au/aghome/advisory/eceg/welcome.html> ("There is the risk, particularly given the lack of any internationally uniform legislative approach, that an inappropriate legislative regime may be adopted without regard to market-oriented solutions.").

18. There is a view, generally accepted by persons familiar with technology, that in certain areas technology has the capability of offering *more* security in commercial transactions than paper-based systems. *See* WARWICK FORD & MICHAEL S. BAUM, SECURE ELECTRONIC COMMERCE: BUILDING THE INFRASTRUCTURE FOR DIGITAL SIGNATURES AND ENCRYPTION (Upper Saddle River, NJ 1997); MICHAEL S. BAUM & HENRY H. PERRITT, JR., ELECTRONIC CONTRACTING, PUBLISHING, AND EDI LAW (John Wiley & Sons, Inc. 1991).

19. *See* Raymond T. Nimmer & Patricia Krauthaus, *Electronic Commerce: New Paradigms in Information Law*, 31 IDAHO L. REV. 937, 945 (1995) ("the creation of system-based assurances of authenticity constitutes a condition precedent for continued expansion in the modern use of the systems in important marketplaces").

theft or alteration, nor is it a simple matter of developing authentication techniques that allow us to determine with extreme accuracy the actual originator or creator of a given message. "Secure" electronic commerce cannot be achieved merely by legislating those circumstances when requisite "security" is present. Rather, the "security" which business people seek when they begin doing business electronically requires the creation of an entire infrastructure—legal, social, economic, and political—one that is based on practice which recognizes, validates, and supports electronic commerce.

By comparison, many of us feel secure in our homes. This security does not necessarily flow from the existence of technological devices to keep out unwarranted intrusions: fences, burglar alarms, bolts, locks, or caller identification on the telephone. To a great degree, the availability of those devices does contribute to our sense of security, but the relationship is not necessarily a direct correlation. Indeed, the more such technological security devices there are in a home, the less likely it is that the inhabitant feels "secure." While some locks or keys may be necessary, the strongest feelings of security flow from the knowledge that locks and bolts are not needed, that one can leave the house unlocked with the expectation that upon return, things will be as they were upon departure.

Security is more than the technological exclusion of others from our premises and more than mere legislation. Security flows in large part from the ability to predict, with a fair degree of certainty, what lies ahead in our daily lives, the ability to control it, and the ability to identify, again with a fair degree of certainty, the risks that we may face so that we can take protective measures. It also comes from the knowledge that there is a social, political, economic, and legal system that protects us and recognizes our rights. It is the overall structure, not any particular technology or law, that creates that security. In our society, that overall structure includes the right to use and control property, the ability to acquire and hold that property, the knowledge that ownership of the property is free and clear of the claims of others, the ability to exclude others from one's property, the ability to move freely about the property and come and go as desired, the ability to allow others access to one's property as desired, the ability to sell or otherwise dispose of one's property, and the right to enforce that sale or transfer. Security flows from the knowledge that the economic, social, and legal systems recognize these rights, and that redress is available from those who violate or infringe them.[20]

20. Security in the home also flows from the knowledge that there is an economic, social, political, and legal structure out there that protects our home that sends firemen and police as needed, arrests trespassers or thieves and brings them to justice through the court system, and provides us with the services needed to use and enjoy our property.

Similarly, for businesses involved in electronic commerce, "doing business securely" means an entire complex of things. It encompasses the ability to enter into a commercial transaction that proposes an exchange on terms beneficial to each party, whether a sales, services, or commodities agreement, with the reasonable expectation that it will be performed. Contracts are performed because our economic, social, and legal structures support these types of transactions and provide incentives for performance as well as disincentives for breach. These economic, social, and legal consequences of breach are the main reasons contracts are performed. Thus, security in transactions means the knowledge that transactions will be performed as expected and the stability and certainty that come with that knowledge. Risk management, the ability to assess the possibilities and risks of non-performance and to take the steps necessary and appropriate to encourage performance or guard against breach, is a key ingredient.[21]

In the electronic environment, what is arguably lacking at the moment is a discernable legal and social structure that allows the parties to adequately assess the risks of electronic commerce and to respond by making intelligent choices concerning their own rights and liabilities, including allocation of risks in transactions with others. For example, without an appropriate legal structure that recognizes and validates electronic commerce, the presence of all the encryption or authentication devices in the world will not give businesses the security they need to conduct business in the electronic environment. The legal structure must include laws recognizing the ability to contract electronically, enforcing deals entered into electronically, and setting forth the rules applicable to the transaction while recognizing the power of the parties, within reason, to set the terms as between themselves and choose the applicable law. This type of security—"legal security"—flows from a legal framework, one that may, to a large extent, already exist, but to the extent the application of that framework in the online environment is less than clear, the resulting sense of security may be impaired. It must be recognized, however, that "legal security" is only part of the overall "security" picture.

---

21. A companion to the concept of "security" is that of "trust": the argument is that systems, both legal and technological, need to be created which people may trust. Again, trust has many meanings. To some, "trust" in electronic transactions may mean "I can count on this transaction being enforced." Alternatively, the trust issue may be expressed as "I can count on that this transaction will be carried out." A third possible phrasing: "I can trust the parties to and persons involved in the transaction." And last: "I can trust that the systems themselves are 'trustworthy.'" Thus, you may have trust in the legal structure supporting the transaction, trust in the parties to the transactions, trust in the performance of the transactions themselves, without regard to legal enforcement, and trust in the systems. There are, additionally, a variety of sources for "trust:" knowledge, experience, familiarity, and authority.

The desire for "security" has manifested itself in online commerce in somewhat traditional ways. Early on, in the absence of legislative and judicial recognition and validation of electronic commerce and the corresponding lack of industry-wide standards, customs, or standards to guide conduct, attempts were made to set the rules for electronic commerce through "trading partner agreements" between the parties doing business electronically.[22] Numerous regional and national model trading partner agreements, or interchange agreements, were developed to provide commerce with a contractual framework for facilitating the adoption and use of electronic commercial practices, thereby providing the parties with some degree of certainty as to the terms applicable to their transactions. Although there are differences between the various proposed interchange agreements, a key ingredient of virtually all of them was the parties' articulation of the technological security measures to be employed in transacting business electronically, and delineation of the circumstances under which each party would be bound by messages purportedly originated by that party.[23]

In situations where the parties were not in prior contact or direct contact, or where the transactions were such that prior negotiation of such agreements was impossible or impractical, alternative contractual models were adopted. One tactic is the articulation by one of the parties to the contract of the applicable terms, e.g., by posting of the terms on the relevant

22. "The idea of a model interchange agreement was first raised at the international level by the Nordic Legal Community in the early 1980s." Amelia H. Boss, *Electronic Data Interchange Agreements: Private Contracting Toward a Global Environment,* 13 NW. J. INT'L L. & BUS. 31, 38 (1992). In turn, the idea spread, and during the 1980s and early 1990s, there was a proliferation of "model interchange agreements" produced by EDI user groups representing specific industries by electronic data interchange associations, attorney groups, government agencies, and international organizations. *Id. See also* Amelia H. Boss & Jeffrey B. Ritter, ELECTRONIC DATA INTERCHANGE AGREEMENTS: A GUIDE AND SOURCEBOOK (1993). In the United States, such a model interchange agreement was proposed by a group within the American Bar Association. *See* The Electronic Messaging Services Task Force, *The Commercial Use of Electronic Data Interchange—A Report and Model Trading Partner Agreement,* 45 BUS. LAW. 1645 (1990).

23. Many of the following issues are addressed in those agreements: selection of EDI messages, message standards, and methods of communication; responsibilities for ensuring that the equipment, software, and services are operated and maintained effectively; procedures for making any systems changes which impair the ability of trading partners to communicate; security procedures and services; the points at which electronic messages have legal effect; the roles and contracts with any third party service providers; procedures for dealing with technical errors; the needs, if any, of confidentiality; liabilities in the event of any delay or failure to meet agreed EDI communications requirements; the laws governing the interchange of EDI messages and the arrangements of the parties; and methods for resolving any potential disputes. *See* Boss, *supra* note 22; Boss and Ritter, *supra* note 22.

website [24] or by postings stating that any transactions were to be governed by a given set of practices.[25] A variation of this type of contract was the development of operating rules within defined systems that purport to bind all participants in the system.[26] Establishment of voluntary "codes of conduct"[27] and the development of industry standards[28] are two other options

---

24. The desires of commercial parties to govern online transactions by posting, or having available on a website, the terms and conditions that purport to cover the transactions entered into on the website have led to the use of what have been called "click-wrap" or "shrink-wrap" licenses. Questions as to the enforceability of such terms and conditions have in turn given rise to litigation. Step-Saver Data Sys. v. Wyse Tech., 939 F.2d 91, 103 (3d Cir. 1991); ProCD Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996); Vault Corp. v. Quaid Software Let., 847 F.2d 255, 258 (5th Cir. 1988). They have also stimulated efforts to address such terms on the state level, the national level, and the international level, amidst considerable controversy. For an overview of the range of reactions to these issues, see Symposium, *Intellectual Property and Contract Law in the Information Age: The Impact of Article 2B of the Uniform Commercial Code on the Future of Transactions in Information and Electronic Commerce*, 13 BERKELEY TECH. L.J. 809 (1998); Symposium, *Intellectual Property and Contract Law for the Information Age: The Impact of Article 2B of the Uniform Commercial Code on the Future of Information and Commerce*, 87 CAL. L. REV. 1 (1999). *See also* Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239 (1995); Apik Minassian, *The Death of Copyright: Enforceability of Shrinkwrap Licensing Agreements*, 45 UCLA L. REV. 569 (1997); Jennett M. Hill, Note, *The State of Copyright Protection for Electronic Databases Beyond ProCD v. Zeidenberg: Are Shrinkwrap Licenses A Viable Alternative for Database Protection?*, 31 IND. L. REV. 143 (1998); Joseph C. Wang, Note, *ProCD, Inc. v. Zeidenberg and Article 2B: Finally, the Validation of Shrink-Wrap Licenses*, 16 J. MARSHALL J. COMPUTER & INFO. L. 439 (1997); Christopher L. Pitet, Note and Comment, *The Problem With "Money Now, Terms Later": ProCD, Inc. v. Zeidenberg and the Enforceability of "Shrinkwrap" Software Licenses*, 31 LOY. L.A. L. REV. 325 (1997); Thomas Finkelstein & Douglas C. Wyatt, Note, *Shrinkwrap Licenses: Consequences of Breaking the Seal*, 71 ST. JOHN'S L. REV. 839 (1997).

25. In the case of providers of certain services, this was accomplished through the development of statements of practice, such as the certification practice statements used by certification authorities in the context of digital signatures. *See, e.g.*, the certification practice statements published on the Internet by GTEI–CyberTrust, <http://www.bbnplanet.com/products/security/cytrust/cps.htm>; True Trust Limited <http://fw4.iti.salford.ac.uk/truetrust/cps/>; and Verisign http://www.verisign.com/ repository/CPS/>.

26. An example is the system rules for international inter-bank transfers, established by the Society for Worldwide Interbank Funds Transfers ("SWIFT").

27. In 1987, the International Chamber of Commerce took the first step by developing and producing the Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission (ICC Publication no. 452). The UNCID rules, the first product in this area, were aimed at facilitating the interchange of trade data effected by teletransmission through the establishment of agreed rules of conduct between parties engaged in such transactions. The UNCID rules were not self-executing but voluntary, requiring the agreement of the parties to incorporate its terms in their own relationship. *See* The Working Party on Facilitation of

that have been explored. One current project proposes to establish a common set of legal "Eterms" which can be incorporated by parties into their electronic messages, thereby providing the private legal structure to guide the transaction.[29] In addition, there has been a move to provide certainty through the use of choice of law and forum clauses and a corresponding desire to strengthen the enforceability of such clauses in electronic commerce[30]

In 1997, the White House issued its report, A Framework for Global Electronic Commerce,[31] which set forth the administration's policies with regard to the law of the Internet. The administration firmly emphasized that in the area of electronic commerce, the private sector should lead, and government regulation should be discouraged. Governments were urged to avoid undue restrictions on electronic commerce and at the same time encouraged to allow new business models and products to evolve. If and when government intervention is deemed necessary to facilitate electronic commerce, the administration cautioned that the government's "aim should be to support and enforce a predictable, minimalist, consistent, and simple legal environment for commerce."[32]

The White House recognized that despite the preferability of private sector leadership, there might be a need to draft rules governing global electronic commerce. In that regard, it urged the elimination of administrative and regulatory barriers to commerce and the recognition of certain fundamental principles. The primary principle is, of course, freedom of contract, the ability of "fully informed buyers and sellers" to set their own rules. Equally important, the administration urged that any legislation or rules be "technology neutral," i.e., the rules should neither require nor

---

International Trade Procedures, *UN/ECE Trade Facilitation Recommendation No. 26* (March 1995) <http://www.unece.org/trade/rec/rec26en.htm>.

28. *E.g.*, in the context of digital signatures, concerns about certification services and the fear that the public would be misled has led to exploration of the establishment of private systems for accreditation of certification authorities according to preestablished industry standards. Charles R. Merrill, *The Accreditation Guidelines-A Progress Report on a Work in Progress of the ABA Information Security Committee*, 38 JURIMETRICS J. 345, 347–48 (1998) (detailing accreditation guidelines' project and need for developing standards of trustworthiness).

29. *See* Andreas Mitrakas & Janjaap Bos, *The ICC ETERMS Repository to Support Public Key Infrastructure*, 38 JURIMETRICS J. 473 (1998).

30. *See* Boss, *supra* note 9.

31. *See* William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce* <http://www.iitf.nist.gov/eleccomm/ecomm.htm>.

32. *Id.* Two other principles were also iterated: that governments should recognize the unique qualities of the Internet and that electronic commerce should be facilitated on a global basis.

assume a particular technology and be flexible enough to permit the development of new technologies in the future.[33]

In recognizing the need for legislation, and at the same time urging a minimalist approach, the White House report reflected discussions in business, academic, and political circles over the past several years. These discussions, however, revealed two distinct approaches, with distinct policy recommendations and legislative proposals flowing from them. These need to be examined in more detail.

III. THE DEBATE: A CONFLUENCE OF TWO STREAMS

The advent of electronic communications technologies and electronic commerce has, over the years, given rise to two distinct movements with regard to law reform, each with its own set of adherents.

Initially, concerns about electronic commerce focused on existing legal structures and principles. The main concern was the application of existing law to transactions entered into electronically. Attempts were made to identify existing barriers to electronic commerce and to determine the extent to which modification of these and other general transactional rules were required in an electronic environment. On the international level, the notion that governments should review legal requirements governing trade and commerce to determine their suitability for electronic commerce surfaced over fifteen years ago.[34] Domestically, the need to review existing laws has been recognized on both the federal[35] and state levels. Those approaching these issues tended to view the question as follows: what changes are

33. A concept related to that of "technology neutrality" is that of "implementation neutrality," the recognition that any rules or laws neither assume nor require the implementation of certain technology in preset ways. A third concept is neutrality, seeking an equivalence between transactions regardless of the medium used for communication. The basic goal of all these efforts is that the law should not discriminate between information on paper and information in electronic form.

34. The removal of legal barriers to electronic commerce became an international issue as early as 1985, when the United Nations Commission on International Trade Law ("UNCITRAL") called upon all governments to "review legal requirements of a handwritten signature or other paper-based methods of authentication on trade related documents with a view to permitting, where appropriate, the use of electronic means of authentication." U.N. GAOR, 40 th Sess., Supp. No. 17, at 72, U.N. Doc. (A/40/17).

35. *See, e.g.*, Matter of National Institute of Standards and Technology-Use of Electronic Data Interchange Technology to Create Valid Obligations, Dec. of the Comp. Gen. Of the U.S., File B-245714 (Dec. 13, 1991) <http://www.softwareindustry.org/issues/docs-org/cg-opinion.pdf> ("Contracts formed using Electronic Data Interchange Technologies may constitute valid obligations of the government for purposes of 31 U.S.C. § 1501, so long as the technology used provides the same degree of assurance and certainty as traditional 'paper and ink' methods of contract formation.").

necessary, in the area of commercial law, evidence, etc., to accommodate electronic commerce. Attempts to accommodate electronic commerce focused on the adaptation of the traditional transactional rules. The goal was to assure that electronic commerce was not discriminated against solely because of the medium in which it occurred.

For example, the law has traditionally required "writings" and "signatures" as a prerequisite for the enforcement of many transactions,[36] and the application of those requirements to electronic commerce has been problematic. The legislative response, at least within the context of commercial law,[37] was twofold: either to eschew the terms "writing" and "signature" in new legislation in favor of terms such as "record" and "authentication,"[38] or to provide affirmatively that existing writing and signature requirements could be met by electronic messages.[39] Most of these changes occurred within the context of more generalized substantive revisions of commercial law aimed at updating and modernizing commercial law to accommodate electronic commerce.

By contrast, a second movement started *not* with a focus on existing law, but rather with a focus on technology and its implementation. Concerns about security motivated members of the digital community to begin

---

36. This, of course, is the notion behind our statute of frauds, which dates back to the adoption by the British Parliament of the first such statute in 1677. Since then, the writing requirement of the statute of frauds has been adopted with some modification in nearly all of the United States. Subject to several exceptions, the statute provides that no suit or action may be instituted under certain categories of contracts unless that contract is written and signed by the party to be charged. *See generally* James J. White & Robert S. Summers, UNIFORM COMMERCIAL CODE §§ 2-1 to 2-12 (3d ed. 1988). However, the British Parliament repealed its statute of frauds in 1954. *Id. See also* R. J. Robertson, *Electronic Commerce on the Internet and the Statute of Frauds*, 49 S.C. L. REV. 787 (1998).

37. The legislative response was actually preceded by a contractual response by the parties to the transaction. *See supra* notes 21–29 and accompanying text.

38. The term "record" was developed over time expressly to deal with electronic records and had been developed and refined by the American Bar Association and the National Conference of Commissioners on Uniform State Laws as a generic term for use throughout proposed legislation. It has since become standard language in products of the National Conference of Commissioners on Uniform State Laws. *See* Patricia B. Fry, *X Marks the Spot: New Technologies Compel New Concepts for Commercial Law*, 26 LOY. L.A. L. REV. 607 (1993) (detailing history of the concept of "record"). *See also* U.C.C. §§ 5-102(14), 5-104, & 8-113 (using the term "record"); §§ 5-104, 8-113 (using the term "authenticate").

39. *See, e.g.*, Uniform Electronic Transactions Act § 106(c) (Proposed Draft Jan. 29, 1999) ("If a rule of law requires a record to be in writing . . . an electronic record satisfies the rule of law."); *id.* § 106(d) (Proposed Draft Jan. 29, 1999) ("[i]f a rule of law requires a signature. . ., the rule of law is satisfied with respect to an electronic record if the electronic record included an electronic signature."). *Compare* UNCITRAL Model Law on Electronic Commerce, Articles 6 (writing), and 7 (signature).

exploration of technological means of providing security to participants in electronic commerce. Three issues were identified as "security" risks: 1) authenticity—the problem of identifying the source or sender of a message and authenticating that it did indeed come from that sender; 2) integrity—the problem of proving that the message is complete and has not been altered since it was sent; and 3) non-repudiation—the risk that the sender may repudiate it after receipt.[40]

One technology, digital signatures, quickly became the "favorite" among many technology afficionados, who claimed it offered a technology-based cure for many of the security risks encountered in online commerce. In many regards, the description of the technology as "digital signatures" is a misnomer. In essence, what is being advanced is a method of encryption—or more appropriately, dual key encryption using two mathematically related numbers, or keys.[41] Each key pair consists of two keys: a person's private key, which is kept private, and the public key which can be made publicly available. When the private key is applied to a message, the message is transformed or encrypted, and a string of numbers is created, the "digital signature" for that message, which is unique to both the key used to encrypt and to the message itself. The recipient of that message can, by using the public key corresponding to the key used by the sender, determine whether the message was sent by the person holding that corresponding private key and determine whether the message had been altered since it was made.[42]

---

40. Although "non-repudiation" is often referred to as a desirable attribute of security procedures, a persuasive argument has been made that whether a person may repudiate a message is actually a legal construct related to the question of the message's authenticity. John D. Gregory, *Solving Legal Issues in Electronic Commerce*, CAN. BUS. L.J. (forthcoming 1999).

41. Although the two numbers are mathematically related, in theory it is computationally infeasible to ascertain what is known as the "private key" of the sender using the "public key" applied by the recipient to unlock the message. If the key utilized is sufficiently long, it would apparently take "extremely powerful computers [many] years and millions of dollars, to crack a single public/private key pair." Greenwood & Campbell, *supra* note 6, at n.14.

42. Thus, "digital signatures" have been defined as:

> [A] transformation of a message using an asymmetric cryptosystem such that a person having the intitial message and the signer's public key can accurately determine whether:
>
> (a) the transformation was created using the private key that corresponds to the signer's public key; and
>
> (b) the message has been altered since the transformation was made.

UTAH CODE ANN. § 46-3-103(10) (1998). For a good tutorial on digital signatures, see <http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>. *See also* Information Security Committee, Section of Science and Technology, American Bar Association, *Public Key Infrastructure Symposium-Tutorial*, 38 JURIMETRICS J. 243 (1998).

One major obstacle to the easy use of this technology is assuring the potential recipient of a message, and user of one-half of the key pair, of the identity of the holder of the other key. In situations where the two parties know one another and can directly exchange keys, there is no problem. In systems such as on the Internet where the parties do not necessarily know each other, identity of the holder of a private key is an issue. To resolve this problem, industry has proposed an implementation of dual key encryption which involves the creation of a "public key infrastructure," or PKI, under which a third party, known as a certification authority, or CA, has the task of verifying the identity of the holder of a key and that the key being used by the recipient is the reciprocal of the key used by the sender.[43]

Supporters of the technology began to develop various models—public key infrastructures—for the use of digital signatures in commerce.[44] In large part, the development of these models involved decisions as to the appropriate business structures to use for electronic commerce. Moreover, the creation of new public key infrastructures raised interesting issues about the relationship between the various parties in the structure. In attempts to resolve these relationship issues and to encourage use of the technology, supporters began to advance the notion that a new legal structure was necessary to promote and facilitate the development of public key infrastructures. As a result, the proponents, concerned primarily with advancing the technology and its business implementations, are now advancing a legal construct to support and promote their specific implementation models.[45]

---

43. This explanation is obviously very simplified. Assume that a message purports to come from Bill Gates and is "digitally signed." The recipient will first want to know that the key it applies to the message is indeed the reciprocal to one held by Bill Gates. Second, it will want to know that the person who obtained the key using the name "Bill Gates" was indeed Bill Gates. Third, the recipient will want to know that the person who actually *used* the key was either Bill Gates or someone acting with authority for Bill Gates.

44. Interestingly, the implementation models that have been advanced have changed over time. Initially, for example, it was contemplated that certification authorities would provide "certificates" directly to the holders of private keys and that the key holders would then use these certificates in communications with others. As the various models have developed over time, however, it appears to be more common for the certification authority to supply the certificate *not* to the key holder but to the relying party, the recipient of the message who wants to verify the identity of the key holder.

45. As one proponent of such legislation has stated:

> [I]t is our desire to make current technology more available and more useful for real-world applications. This can be done by objectively reviewing what the various available technologies can do, grouping them according to their attributes of security, reliability, scalability, and so on, *and creating legislative constructs (including for self-regulation) appropriate to each technology.*

In 1995, Utah, the home to high technology companies with an interest in the topic, followed by Minnesota[46] and Washington,[47] became the first to enact a digital signature statute setting forth specific rules governing digital signatures and public key infrastructures.[48] The main characteristic of this legislation is its regulatory nature, providing for a licensing scheme for certification authorities.[49] Licensed certificate authorities under the statutes are given significant limitations on their liability to other parties within the public key infrastructure.[50] Indeed, it can be argued that the primary purpose behind the legislation is this limitation of liability, and that the licensing regime serves that limitation. The liability scheme was seen as necessary to assure commercial developers "that the risks of potential liability to users of the system could be kept within tolerable limits."[51] Although the statutes also attempted to address the rights and responsibilities of other participants in the public key infrastructure, only a small portion of the digital signature statutes pertains to the *legal effect* to be given to the use of the digital signature. These statutes frequently went further than saying that a person may use a digital signature and effectively meet any writing or signature requirements. Consistent with the philosophy of attempting to provide a comprehensive scheme to apportion all liability of the parties, these laws provided that where a digital signature was accompanied by a verifiable certificate issued from a certification authority licensed under the statute, it was entitled to the presumption that it was affixed by the holder of the

---

Michael S. Baum, *Technology Neutrality and Secure Electronic Commerce: Rule Making in the Age of "Equivalence"* at 4, n.5 (1998) <http://www.verisign.com/repository/pubs/tech_neutral/> (emphasis added). Reviewing and grouping may perform wonderful services to businesses attempting to implement electronic commerce, allowing parties to choose the attributes of security important to them. Whether legislation and new legal constructs are needed to facilitate those choices is a different issue.

46. *See* UTAH CODE ANN. tit. 46, Ch. 3 (1996).

47. Minnesota Electronic Authentications Act, MINN. STAT. ANN. § 325 (West 1998) <http://www.revisor.leg.state.mn.us/stats/325K/>.

48. Washington Electronic Authentications Act, WASH. REV. CODE ANN. § 19.34 (West 1998) <http://www.wa.gov/sec/dsrcq.htm>.

49. For example, the Utah statute confers authority on a state agency to license certificate authorities that operate within their jurisdiction. UTAH CODE ANN. §§ 46-3-201–204 (1998).

50. *See, e.g., id.* § 46-3-309 (limiting liability of certification authority to amount it includes in its certificate and specifically excluding consequential damages).

51. Jane Kaufman Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 TUL. L. REV. 1177, 1241 (1998). "This limit on the potential liability of the [Certificate Authority] to subscribers and relying parties, above and beyond any liability that it has expressly undertaken and set forth in its certification practice statement, is a pivotal risk allocation rule." *Id.* at 1242.

private key and was therefore attributable to it.[52] Although these signing and attribution provisions were only a part of a larger digital signature statutory scheme, they overlapped with the efforts begun earlier to define signing and attribution in the commercial context.

In effect, these two separate movements, one with its origins in the law, the other with its origins in the technology, represent two philosophies. The first, which began with a concentration on commercial law issues, has focused on keeping commercial laws generic and supportive. The goals have been to remove barriers to electronic commerce, treat electronic communications on a par with paper communications, and not to favor one technology over another (technology neutrality) nor one business model over another (implementation neutrality). As between different technologies or implementation schemes, the choice was to be that of the parties. This approach exhibits a degree of confidence in the marketplace to make suitable options available to parties, allowing them to make intelligent choices. The second movement has the philosophy—and the express goal—of supporting and promoting specific technologies, or, more correctly, one specific technology and one implementation model. The theory is that the technology and implementation offer such benefits to the users of the Internet that legislation should recognize those benefits and enshrine them in the law. Despite their different orientations, both movements ended up dealing with the same issue: the satisfaction of legal requirements of writings and signatures through technological means in an electronic environment.

At the outset, the two movements were relatively separate; those revising the commercial laws and those building PKI infrastructures represented two different constituencies: law revisionists and technology supporters. To a large extent, however, the "digital signature" movement was the more visible of the two. Commercial law does not tend to have inherent appeal to either the public or to legislators. On the other hand, mere mention of certain buzzwords, such as "Internet," "security," or "technology," immediately piques the interest of both the public and the legislature. Among the public, the digital signature movement quickly gained two distinct bodies of followers. The first consisted of those who saw digital signatures as the answer for Internet security.[53] Because of their belief in the security aspects of digital signatures, the desire was to build a structure, a business structure as well as a legal structure, to support the technology. The second body of followers were those business people attracted to the digital signature movement not because of any interest in the

52. UTAH CODE ANN. § 46-3-406 (1998).

53. Some of these participants were in fact representing businesses that were marketing digital signature technology; others were simply focused on the merits of the technology.

technology itself but because of concerns about the ability of the law in its current state to recognize and validate online business transactions. Their desire to gain legal recognition of electronic communications contributed to their support for digital signature legislation. That support, driven out of a desire to establish the validity of electronic commerce, was given in the absence of a recognition that other efforts would establish that validity without the need for a complicated, legal, and regulatory structure for digital signatures.

Ultimately, the law revision and technology "movements" joined issue on the question of the legal effects to be given to certain uses of the technology to "sign" or otherwise authenticate messages. In one regard, the dispute is between the "removal" of barriers to electronic commerce through the development of generic rules and the "support and promotion" of electronic commerce through the creation of rules geared to promoting its use. In another regard, the dispute is whether specific types of technology implementations should be given special treatment under the law.

IV. SURVEYING THE BATTLE FRONT

The war between the law revision and technology movements is being waged on many simultaneous fronts: within the individual states, at the federal level in Congress, at the uniform law level within the United States, at the national level abroad, and on the international level as well. On the individual state level, state legislatures have acted in a variety of ways to accommodate electronic commerce, but four patterns of statutes have emerged over time, reflecting the influence of the two movements. Initially, Utah was the first state to adopt a full-fledged digital signature statute supporting a public key infrastructure,[54] legislation which was based on efforts of the American Bar Association's Information Security Committee, which published a set of *Digital Signature Guidelines.*[55] The approach used by Utah and the *Digital Signature Guidelines*, however, of setting forth a highly structured, prescriptive, regulatory environment only for digital signatures, has not been widely followed by the states.[56] California quickly

54. *See* UTAH CODE ANN. § 46-3-101 (1996). The 1996 legislation was a revision of legislation which originally became effective in 1995.

55. ABA COMM. ON INFORMATION SECURITY, *Digital Signature Guidelines* (1996). It is interesting to note that, while the *Guidelines* were developed within a committee of the American Bar Association, that committee consisted of a substantial number of individuals who were not lawyers but were drawn from various segments of the technology industry.

56. For an excellent survey, see Internet Law and Policy Forum, *Survey of State Electronic & Digital Legislative Signature Initiatives*, submitted Sept. 12, 1997 <http://www.ilpf.org/digsig/digrep.htm>, *updated*, Internet Law and Policy Forum, *UPDATE: Survey of State Electronic & Digital Signature Legislative Initiatives*

followed on the heels of Utah by enacting legislation that did not follow the Utah statute in its adhesion to public key cryptography. Rather, it drafted a technology-neutral law.[57] It provided that an electronic signature[58] would have the same legal effect as a manual signature if it has these attributes: it is unique to the person using it, it is capable of verification, it is under the sole control of the person using it, it is linked to the data in such a manner that, if the data are changed, the electronic signature is invalidated, and it conforms to regulations adopted by the Secretary of State.[59] Later regulations permitted either digital signature using a certification authority or signature dynamics.[60] The California approach has proven to be more popular in the United States than the Utah focus on digital signatures alone.[61] While it is more generalized, a person using a certain security procedure must demonstrate that either it fits within the regulations or within the generalized criteria set forth in the statute before the digital signature is given effect.

Florida followed a third approach when, in 1996, it enacted the Electronic Signature Act.[62] Florida represents the enabling approach, emphasizing the elimination of artificial barriers to electronic commerce. Under the Act, the term "writing" is defined to include information created or stored in any electronic medium that is also retrievable in perceivable form.[63] Any such writing containing an electronic signature, defined to include any letters, characters, or symbols, manifested by electronic or

---

<http://www.ilpf.org/digsig/UPDATE.HTM>. Another source of current information on state and other legislation is the McBride Baker Coles site, <http://www.mbc. com/>.

57. California was influenced, in part, by international legislation, the Model Law on Electronic Commerce, being drafted by the United Nations Commission on International Trade Law. *See supra* note 6.

58. California used the expression "digital signature" to cover more than just signatures using public key cryptography. To avoid confusion in the text, the term "electronic signature" is used to emphasize that the legislation applies to any signatures in electronic form, whether or not they are technically dual key encryption "digital" signatures.

59. *See* CAL. GOV'T CODE § 16.5 (West 1995). The first four criteria were first established in a decision of the Comptroller General of the United States in *Matter of National Institute of Standards and Technology (NIST)—Use of Electronic Data Interchange Technology to Create Valid Obligations*, Comp. Gen. File VB-245714 (Dec. 13, 1991) <http://www.softwareindustry.org/issues/docs-org/cg-opinion.pdf>.

60. Signature dynamics is associated with PenOp, a system of signing manually using computer-recorded strokes. *See* PenOp, *Welcome to PenOp, the World's Leading Electronic Handwritten Signature* <http://www.penop.com/>.

61. *See* ILPF Survey, *supra* note 57.

62. Electronic Signature Act of 1996, 1996 Fla. Laws ch. 96-224 (codified as amended at FLA. STAT. § 282.72 (1996)).

63. This formulation tracks the definition of a "record" in uniform legislation proposed by the National Conference of Commissioners on Uniform State Laws. *See supra* note 39.

similar means, with intent to authenticate a writing, may be used to sign a writing and is given the same force and effect as a written signature. This enabling approach has become increasingly popular among the states that have considered the question.[64] It does not require an extensive set of regulations, does not set forth specific technologies and implementations that it sanctions, nor does it set forth "criteria" for judging whether electronic signatures will be given legal effect.

A fourth approach developed in Illinois as a "middle ground" between digital specific statutes and mere enabling statutes: the concept of a hybrid statute that enabled the use of electronic signatures by validating their use, but at the same time recognized a category of "secure electronic signatures."[65] Anyone may use an electronic signature in electronic commerce and be assured that legal writing and signature requirements are no obstacle. However, if a signature qualifies as a secure electronic signature by meeting criteria similar to that found in the California statute, rebuttable evidentiary presumptions arise as to the authenticity and integrity of the signature.

The lack of uniformity among the various state enactments has led to activity on two fronts. Pressure is being placed on Congress to take action, both from the fear that states will delay in responding to the needs of electronic commerce and from the fear that their responses will be non-uniform in character. Thus, the push is on to: 1) develop standards for use of electronic and digital signatures in transactions with the government; 2) develop a federal standard for recognition of electronic and digital signatures; and 3) preempt state law. Several bills have been introduced over the past few years to deal with electronic commerce, although none have yet been enacted. The scope and approach of the proposed legislation has differed drastically. At one end of the spectrum is proposed legislation merely giving effect to "electronic signatures" as a method of signing;[66] this type of legislation would best be characterized as enabling legislation. Other proposed legislation, within the banking context, proposed to validate "secure" electronic techniques of authentication adopted pursuant to agreement or system rules;[67] to the extent this legislation would merely

64. ILPF Survey, *supra* note 57.

65. The Illinois statute was enacted in 1998. 205 ILL. COMP. STAT. § 705/10 (West 1998).

66. *See* Government Paperwork Elimination Act of 1998, S. 2107, 105th Cong. (1998) (sanctioning electronic signing of forms submitted to federal agencies); Paperwork Elimination Act of 1999, H.R. 439, 106th Cong. (1999) (following Government Paperwork Elimination Act); Millennium Digital Commerce Act, S. 761, 106th Cong. (1999).

67. The Digital Signature and Electronic Authentication Law of 1998, S. 1594, 105th Cong. (1998) (validating electronic authentication under relevant "agreements" or "system

reinforce the ability of the parties to govern their transactions by agreement, it would be consistent with an enabling and validating approach. A bit further down on the scale is proposed legislation providing that close-up electronic signatures meeting certain criteria are acceptable as signatures.[68] To the extent that legislation begins to set additional hurdles for electronic commerce, it begins to move from merely enabling and starts to introduce a channeling function—that of telling businesses what technologies they should adopt. One piece of proposed federal legislation, in the context of federal tax filings, would create a presumption that the person on whose behalf a return was filed did indeed subscribe to and submit the return.[69] As will be discussed below, presumptions have become a fertile battleground on the uniform law level; this proposed federal legislation, however, deals solely with communications, i.e., tax filings, with the government and relieves the Internal Revenue Service of proving in each instance that a particular taxpayer did indeed file the return under consideration. The proposed bill that goes the furthest in establishing a more regulatory approach would establish a federal panel to develop a national digital signature infrastructure.[70]

The primary thrust of the federal push is the need for immediate uniform national legislation. There are other efforts on a state-by-state basis that should fill that need. The National Conference of Commissioners on Uniform State Laws will be taking final action in July 1999 on two pieces of proposed uniform legislation that will address the concerns of at least those who want to validate and enforce electronic transactions by removing

---

rules" and authorizing their use by financial institutions pursuant to agreement or pursuant to a "banking, financial, or transactional system using electronic authentication").

68. Electronic Financial Services Efficiency Act of 1997, H.R. 2937, 105th Cong. (1997) (stating all forms of electronic authentication meeting certain standards "shall have standing equal to paper-based, written signatures"). Those standards are: 1) the identification method be unique to the person sending the communication; 2) the identification technology be capable of verification; 3) the identification method be under the sole control of the person using it; and 4) that the identification method be linked to the data in such a way that if the data is altered, the authentication becomes invalid. *Id.* This follows the approach begun in the California legislation—borrowing the standards from NIST, *supra* note 36, and subsequently picked up in several states.

69. Internal Revenue Restructuring and Reform Bill of 1997, H.R. 2676, 105th Cong. (1997) (sanctioning tax returns filed electronically and stating that any return filed electronically shall be presumed to have been submitted and subscribed to by the person on whose behalf it was filed).

70. Computer Security Enhancement Act of 1997, H.R. 1903, 105th Congress (1997) (also authorizing National Institute of Standards and Technology to assist private sector in developing voluntary standards and guidelines for a public key infrastructure).

barriers to electronic commerce.[71] Driven in large part by concerns about nonuniformity among the states, these efforts have benefitted greatly from the "experimentation" that has already occurred on the state level. The need for uniformity should be achieved, without federal preemption, if either of these measures gain sufficient enactment by the states.[72]

On the international scale, a similar pattern is beginning to emerge, although developments internationally are lagging somewhat behind those in the United States. Following the lead of Utah, and inspired in large part by the *Digital Signature Guidelines,* several countries, including Germany,[73] Italy,[74] Malaysia,[75] and Argentina,[76] have enacted legislation relating to electronic authentication and adopting to some degree the approach pioneered by Utah. By contrast, Singapore has adopted an approach loosely based on the Illinois hybrid approach, drawing a distinction between electronic signatures on the one hand, which it enables, and secure electronic records and signatures on the other, including digital signatures.[77] Similarly taking a hybrid approach is the recently released EU Directive on Digital Signatures[78] and several drafts considered by the United Nations Commission on International Trade Law.[79]

---

71. *See supra* note 5 and accompanying text.

72. Indeed, recent federal legislation would *not* preempt state laws in those states that have enacted uniform state law such as the Uniform Electronic Transactions Act. *See* Millennium Digital Conference Act, 1999 S. 761 (Mar. 26, 1999), section 6(c).

73. German Digital Signature Law (Aug. 1, 1997) <http://www.iid.de/rahmen /iukdgbt.html>, *available in English at* <http://www.kuner.com/data/sig/digsig4.htm>.

74. *See* Italian Law N. 59, Art. 15, c. 2 (enacted Mar. 15, 1997), *available in Italian at* <http://www.interlex.com/testi/attielet.htm>, and regulations promulgated Nov. 10, 1997 (Presidential Decree No. 513), *available in Italian at* <http://www. notariato.it/forum/dpr_513.htm> .

75. *See* Malaysia Digital Signature Act, Law No. 59 of 15 Mar. 1997 <http://www.mycert.mimasmy/digital.html.>.

76. Legislation has also been passed in Italy. Argentina has also adopted digital signature legislation by presidential decree. Presidential Decree No. 427/98 <http://www.sfp. gov.ar/firma.html>, *available in English at* <http://www.sfp.gov.ar/decree427.html>.

77. Singapore Electronic Transaction Act (adopted June 29, 1998), *available at* <http://www.ech.ncb.gov.sg/>.

78. European Commission, *Proposal for a European Parliament and Council Directive on a Common Framework for Electronic Signatures* (May 13, 1998) <http://www.ispo. cec.be/eif/policy/com98297.html>. The articulated goal of the directive was to "[ensure] the proper functioning of the Internal Market in the field of electronic signatures by creating a harmonized and appropriate legal framework for the use of electronic signatures within the [European] Community and establishing a set of criteria which form the basis for legal recognition of electronic signatures." *Id.*

79. *See* the Preparatory Documents for the UNCITRAL Working Group on Electronic Commerce <http://www.un.or.at/uncitral/>. For many years, UNCITRAL adhered to the

Several other nations, however, have refused to legislate detailed standards for the use of different authentication techniques or one particular technique, urging instead a simple enabling approach. In March 1998, the Australian Electronic Commerce Expert Group issued its report on the laws of electronic commerce, in which it concluded:

> It is our view that the enactment of legislation which creates a detailed legislative regime for electronic signatures needs to be considered with caution. There is the risk, particularly given the lack of any internationally uniform legislative approach, that an inappropriate legislative regime may be adopted without regard to market-oriented solutions. Given the pace of technological development and change in this area, it is more appropriate for the market to determine issues other than legal effect, such as the levels of security and reliability required for electronic signatures. Accordingly, we have recommended that legislation should deal simply with the legal effect of electronic signatures. While a number of articles in the Model Law deal with electronic signature issues that go beyond legal effect, it is our view that these issues should be left to the existing law in Australia. Whether the existing Australian law deals with these issues adequately or not, the same situation should apply to both paper based commerce and electronic commerce. At this stage we are not persuaded of the need to give a legislative advantage to electronic commerce not available to traditional means of communication. If a clear need to deal with these issues appears in the future the recommended legislation can be amended.[80]

Similarly, the New Zealand Law Commission, in its October 1998 report on Electronic Commerce, rejected the approach of technology specific legislation as found in Utah and Germany and adopted as one of its guiding

---

notion that it was important to maintain technology in its rules, and therefore pursued the dual approach. At its February 1999 meeting, however, the Working Group backed away from the attempts to develop a "media neutral" set of rules and opted for the moment to pursue development of public key infrastructure ("PKI") or digital signature specific rules.

80. Australian Electronic Commerce Expert Group, *Electronic Commerce: Building the Legal Framework*, Executive Summary <http://www.law.gov.au/aghome/advisory/eceg /summary.html>. Legislation has since been proposed which would follow the provisions of the UNCITRAL Model Law and therefore have no special recognition given to digital signatures nor any presumptions attaching beyond those provided for in the Model Law. *See Australian Draft Electronic Transactions Bill* <http://law.gov.au/ ecommerce/>.

principles "technological neutrality."[81] The Law Commission recommended merely that legislation be passed to ensure that electronic signatures would be acceptable under law.[82]

V. ENABLING VERSUS PROMOTING: THE DEBATE IN THE UNIFORM LAW PROCESS

The debate within the uniform law process, as it is currently proceeding, highlights the controversy between those who view the appropriate role of law revision as simply removing barriers to electronic commerce—with the marketplace providing other necessary incentives and support—and those who feel that security on the Internet is and should be promoted by legislation that gives advantages to those who adopt the appropriate technology. In August of 1999, the National Conference of Commissioners on Uniform State Laws will be presented with two pieces of proposed uniform legislation: a new Uniform Electronic Transactions Act ("UETA")[83] and an addition to the Uniform Commercial Code, Article 2B, that deals with computer information transactions.[84] Despite the worthy goal of uniformity and the original mandate to the drafting committees to be consistent, these two products are not uniform in their treatment of security procedures and their use. Indeed, their lack of uniformity exemplifies the tension between those dedicated to removing barriers to electronic commerce and those wishing to support and promote by creating confidence in the systems themselves.

VI. UNIFORM ELECTRONIC TRANSACTIONS ACT

The Uniform Electronic Transactions Act Drafting Committee, created in 1997 by the National Conference of Commissioners on Uniform State Laws, initially explored various means of providing security in electronic commerce, offering strong presumptions where certified digital signatures

81. New Zealand Law Commission, Report 50, *Electronic Commerce Part One: A Guide for the Legal and Business Community*, at ¶¶ 334–335 (Mar. 15, 1999) <http://www.lawcom.govt.nz/pub_index.html>.

82. "In our view, the needs of the market can be met by making a change to the proposed Interpretation Act by including a definition of the term 'signature' to ensure that electronic signatures are acceptable. This could follow the intent of article 7 of the UNCITRAL Model Law on Electronic Commerce." *Id.* at ¶ 344.

83. *See supra* note 5 and accompanying text.

84. *See supra* note 2. On April 7, 1999, after this article went to press, the National Conference of Commissioners on Uniform State Laws announce that the final form of these rules would be in the Uniform Computer Information Transactions Act, and not a part of the Uniform Commercial Code.

were involved.[85] Thus, in the beginning of the UETA deliberations, the philosophy of the digital signature legislation was pursued: identifying certain technological implementations and giving them special legal effect. Serious skepticism was expressed at the first meetings, however, about the appropriateness of this approach, and in particular about presumptions, for many reasons, ranging from concerns about the implementation of digital signature technology,[86] to the lack of acknowledged standards of care of a private key, to uncertain certification practices by CAs, and to unfairness of the presumptions to less sophisticated parties. On the theory that market practices were not sufficiently developed to permit evaluation of the presumptions, the presumptions were weakened drastically,[87] and the special treatment for digital signatures was replaced with special treatment for secure signatures. By July of 1998, however, the presumption language was eliminated.[88] No heightened effect was given to a message or record because of its status as either a digital or "secure" signature.

There was, however, special treatment given where security procedures were implemented. Under the provisions dealing with attribution, an electronic message would be attributed to a person if another person, through the application of a commercially reasonable security procedure, concluded that it was that of the purported sender.[89] Gone was any reference to specific technologies, or criteria those technologies need to satisfy; as long as the procedures were commercially reasonable, they were given special legal effect. In essence, what started as a technological construct (specified security procedures) evolved into a semi-technological construct (security procedures satisfying specified criteria) and eventually into a commercial law construct (commercially reasonable security procedure). Even that

85. The preliminary draft of the UETA was prepared in the spring of 1997 and considered at an organizing meeting of the drafting committee in Dallas in May. *See* Uniform Law Commissioners, *Drafts of Uniform and Model Acts Official Site*, <http://www.law.upenn.edu/bll/ulc/uecicta/ecomm.htm>. It reflected some of the thinking in both UNCITRAL's deliberation and the Utah Act, offering strong presumptions that certified digital signatures bound the purported signer (the person named in the certificate) to the electronic record. Similar provisions appeared in the August 1997 draft.

86. *See* Cem Kaner, *The Insecurity of the Digital Signature* <http://www.badsoftware.com/digsig.htm>.

87. The November 1997 draft of the UETA weakened the presumptions drastically; it had borrowed concepts from Illinois, as had UNCITRAL at about the same time. Continued concern about the presumptions led to the inclusion in the March 1998 draft of the UETA three alternative definitions of a presumption, ranging from a "bursting bubble" approach, where the proffering of any credible evidence destroys the presumption, to a shifting of the burden of persuasion. *See* UETA § 102(a)(15) (Revised Draft Mar. 1998).

88. *See* Uniform Electronic Transactions Act (Proposed Draft July 1998).

89. *See id.* § 202. In turn, a security procedure was defined as a procedure required by law, established by agreement, or knowingly adopted by each party. *See id.* § 102(a)(17).

provision raised concerns, in large part for the same reasons that the presumption language did, but in addition because of the vagueness and uncertainty inherent in a "commercially reasonable" standard. Eventually, this special treatment for commercially reasonable security procedures was also eliminated by the February 1999 draft.[90]

Although, generally, the UETA eliminated presumptions, the February 1999 draft did contain one vestige of presumptions arising in the security procedure context that proved to be controversial and was ultimately eliminated. Under that provision, if one party required the use of a security procedure, that "requiring party" would be precluded from denying any messages sent pursuant to that security procedure. In other words, an irrebuttable presumption was created that the message came from the requiring party.[91] The other party, however, would not be precluded from denying any messages under similar circumstances and would retain the right to deny the message as its own.[92] The theory of the section was to "cast[ ] the risk of misattribution, and informational error on the party that is responsible for a particular security procedure being used in a transaction."[93] The unintended consequence of this provision, however, was to *discourage* a party from resorting to security procedures: it would appear to a party's advantage *never* to require a security procedure—a result fundamentally at odds with the type of behavior, i.e., the use of security procedures, one would otherwise want to encourage. Even if a party were acting reasonably, prudently, and in good faith in setting out security procedures, it could not

90. A memorandum prepared by the Chair and Reporter of the UETA Drafting Committee outlined the reasons for eliminating the presumptions: "certainty and stability regarding the predicate facts giving rise to the presumption" inherent in creation of statutory presumptions is lacking; the vague formation of "commercially reasonable procedures" led to uncertainty; and uncertainty was inherent in the development of the technologies. Memorandum from Patricia Brumfield Fry and D. Benjamin Beard to NCCUSL Commissioners (July 18, 1998) <http://www.webcom.com/legaled/ETAForum>. Technology changes so rapidly that it is difficult to say, two years after a given transaction occurred, what procedures were "commercially reasonable" at the time. Other considerations that were cited include: the relative weakness and therefore meaninglessness of the "bursting bubble" presumption (the presumption exists until denied by the other party), the concern about creating a regime in which parties selected the medium for their transaction based on their differing legal effects; the fact that presumptions would operate against the interests of consumers and other unsophisticated parties; and the fact that presumptions might become a rationale for other governments to regulate. *Id.* For a summary of the discussions at the Uniform Electronic Transactions Act Drafting Committee meetings, see *id.*

91. UETA § 107(a) [Alternative 1] (Proposed Draft Feb. 1999). The other party must have relied upon that message to trigger the presumption. *Id.*

92. *Id.* An alternative proposal would provide simply that "an agreement to be bound by the results of a security procedure is unenforceable." *Id.* § 107(a) [Alternative 2].

93. *Id.* Reporter's Note.

escape liability under this provision, even by contract.[94] Consequently, a provision intended to encourage the use of security procedures arguably did just the opposite, and it was eliminated by the UETA Drafting Committee at its February 1999 meeting.

The current draft of the UETA, as it may be expected to be presented to the National Conference, treats attribution in a very simple, straightforward manner. An electronic message is attributed to a person "if the electronic record resulted from the act of the person, or its electronic agent."[95] Once it is found that a message or record is attributable to a person, attribution "has the effect provided for by law, regulation, or agreement regarding the security procedure."[96] Under this approach, attribution clearly is a factual matter;[97] no preference is given to any particular method of authentication or any particular security procedures, and at the same time, freedom of contract is recognized. Thus, at least within the context of the UETA, the view that there should not be any rule which would provide a specific effect for any security procedure,[98] whether it be an identified security procedure, e.g., digital signatures, a security procedure agreed to by the parties, or a security procedure which meets some predefined criteria, has carried the day with regards to attribution.[99]

VII. ARTICLE 2B OF THE UNIFORM COMMERCIAL CODE

The proposed new Article 2B to the Uniform Commercial Code, whose scope is limited to computer information transactions, was intended to forge

94. UETA § 107(b) (Proposed Draft Jan. 29, 1999) (stating the "provisions of this section may not be varied by agreement"). *Id.*

95. *Id.* § 109(a).

96. *See id.* § 109(b). "'Security procedure' means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person." *Id.* § 102(a)(18).

97. As a result, a certain security procedure may be effective to prove attribution at a given point in time but will lose its efficacy with advances in technology, or with the ability of hackers to demonstrate the vulnerability of systems.

98. *See* Letter from the Bank Working Group to D. Benjamin Beard and Patricia Brumfield Fry (Feb. 12, 1999) (on file with the author). The Bank Working Group includes Citigroup, The Chase Manhattan Bank, Visa International, Independent Bankers Association of America, Consumer Bankers Association, The New York Clearing House Association, L.L.C., and the Keybank National Association.

99. Under a parallel provision, § 111, an electronic signature "may be proven in any manner, including by showing that the electronic signature was signed in conformity with a security procedure for validating electronic signatures, or that a procedure existed by which the person . . . must have engaged in conduct or operations that signed the record or item in order to proceed further in the processing of the transaction." UETA § 111 (Proposed Draft Jan. 1999). Again, any presumptions arising from the use of a particular security method are removed. *Id.*

the rules for electronic contracting that would provide the base for the remaining articles of the Code.[100] Although the UETA has gone to great lengths to eliminate presumptions and to eliminate any special treatment arising from the use of security procedures, the Article 2B Drafting Committee has taken the position that such treatment is important and that if security procedures are present, that treatment encourages the use of security procedures and promotes electronic commerce.

Article 2B begins with the traditional rule that the person asserting that a record is that of another person has the burden of proof of attribution.[101] Special legal effect is given, however, to the implementation of security procedures, or what Article 2B calls an "attribution procedure."[102] If the parties agree to, *or otherwise adopt,* an attribution procedure[103] which is used by the parties, the attribution procedure is commercially reasonable, and the recipient "relies on or accepts" the message, then the recipient has met its burden of attributing the message to the sender.[104] The only way the purported sender may avoid attribution is to prove the message was not caused by: 1) someone entrusted by the sender with the right to act on its behalf; 2) someone who gained access to the transmitting facilities of the sender; or 3) someone who obtained, from a source controlled by the purported sender, information facilitating breach of the attribution procedure.[105] Even if the purported sender is able to overcome this hurdle, it might still be held liable under negligence-type principles.[106]

The foundation, then, of Article 2B's rules is the presence of a "commercially reasonable"[107] attribution procedure, a concept that had its

100. Although that was the intent, the Article 2 Drafting Committee voted at its February 1999 meeting to adopt a minimalist approach, more akin to Article 2B, rather than following Article 2B's approach. That decision was ratified by the Article 2 Drafting Committee at its last meeting in March of 1999. Thus, the Article 2 Drafting Committee has stopped short of adopting the Article 2B provisions discussed above.

101. *See* U.C.C. art. 2B-116(c) (Proposed Draft Feb. 1, 1999), *available at* <http:www.law.upenn.edu/bll/ulc/ulc.htm>.

102. An attribution procedure is defined as "a procedure established by law, regulation, or agreement, or a procedure otherwise adopted by the parties, [to verify] that an electronic message . . . is that of a specific person." *See id.* at § 2B-102(a)(3).

103. *See id.* at § 2B-116(c). At its February meeting, the Article 2B Drafting Committee discussed a clarification that the attribution procedure must have been "knowingly" adopted. *Id.*

104. *Id.*

105. *See id.* at § 2B-116(c)(3) (Proposed Draft Feb. 1, 1999) *available at* <http:www.law.upenn.edu/bll/ulc/ulc.htm>.

106. Under U.C.C. § 2B-116(e), a purported sender is liable for reliance losses if those losses occurred as a result of the purported sender's failure to exercise reasonable care with regard to the attribution procedures. U.C.C. § 2B-116(e).

107. *See, e.g., id.*

genesis in the "security procedure" provisions of Article 4A on funds transfers.[108] Once the presence of such a procedure is established, then the recipient of the message has carried its burden of establishing that the message originated with the identified sender. The theory is that such a standard makes it easier for recipients of messages to "prove up" those messages in court, and as a result, more people will implement commercially reasonable security procedures, and confidence in the systems will increase.

Those favoring presumptions[109] of this nature frequently invoke the precedent of Article 4A and its treatment of commercially reasonable security procedures. Crucial differences exist between the two formulations, however. First, Article 4A applies only where there has been an "agreed" security procedure. Indeed, under Article 4A, the notion of a "commercially reasonable security procedure" acts as a limitation on the ability of the parties to alter traditional rules governing proof of attribution: a contractual agreement will be recognized only if the agreed procedure is commercially reasonable. Thus, Article 4A is *not* a recognition that certain security procedures should be given special legal effect, but a recognition that the ability of the parties to agree—and, in particular, the ability of a bank to shift the liability for an unauthorized message to its customer—is limited.

While Article 4A only applies where there has been an "agreed" security procedure, Article 2B applies to any attribution procedure "otherwise [knowingly] adopted by the parties."[110] According to the drafters of Article 2B, the provision on attribution "enables electronic commerce in an open environment, while stating reasonable standards to allocate risk."[111]

---

108. *See* Boss, *supra* note 4. Article 4A on funds transfers defines a security procedure as "a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or canceling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication." U.C.C. § 4A-201. For the definition of an "attribution procedure," see *supra* note 102. The relevance of Article 4A as a precedent in other areas of electronic commerce has, however, been called into question in large part because of distinctions between the types of transactions subject to Article 4A and those subject to the provisions of either Article 2B or the UETA. *See* Boss, *supra* note 9, at 1079–80, 1083.

109. The February 1999 draft of § 2B-116 spoke in terms of use of attribution procedures "creat[ing] a presumption" of attribution. U.C.C. § 2B-116 (Proposed Draft Feb. 1, 1999). At its February meeting, the Drafting Committee accepted a proposal put forward by Chair Carlyle C. Ring, Jr. and Reporter Raymond Nimmer to modify the language to speak in terms of who has the burden of establishing attribution or non-attribution. *See* <http://www.2Bguide.com/docs/299t4.html>. The effect of the proposal was to remove the problem of characterizing the type of presumption (bursting bubble, burden of going forward, burden of persuasion), but in effect, the language utilizes the strongest of rebuttable presumptions: the burden is that of establishing the negative.

110. U.C.C. § 2B-102(a)(3) (Proposed Draft Feb. 1, 1999).

111. *Id.* § 2B-116, Reporter's Note 1.

It is clear that the Article 2B drafters were concerned about parties who were not otherwise in privity with each other: "Electronic commerce is anonymous in character and depends upon such procedures and their recognition in law and practice."[112] The absence of any requirement of an agreement has important ramifications. At least where there is an agreement between the parties as to the relevant procedures to be followed, a party is arguably on notice that all parties to the transaction will rely on those procedures. Because of the vague reference in Article 2B to procedures "otherwise adopted by the parties,"[113] such notice is arguably lacking. Moreover, under the required agreement under Article 4A, the customer unwilling to assume fraud risks had the ability to protect itself by shifting the burden back to the bank or requiring the bank to take additional procedures,[114] an ability lacking under Article 2B.

A second crucial difference is the practical ability of the alleged sender of a message to overcome the presumption in light of the nature of the transaction and in light of the state of technology. If a person adopts a PIN or other attribution method for doing business on the Internet, it will find that if a message is sent utilizing that PIN, the person will be liable for that message unless it can invoke the provisions setting forth how the presumption is overcome. Consequently, rather than the burden being on the recipient to prove who sent the message, the burden is now on the alleged sender to prove it did not send the message and that the message did not originate from anyone who gained access through the alleged sender.

Proving a negative is difficult. In the context of Article 4A, however, the rationale was explained as follows:

> Because of bank regulation requirements, in this kind of case [wire transfer fraud,] there will always be a criminal investigation as well as an internal investigation of the bank to determine the probable explanation for the breach of security. Because a funds transfer fraud usually will involve a very large amount of money, both the criminal investigation and the internal investigation are likely to be thorough. In some cases there may be an investigation by bank examiners as well. Frequently, these investigations will develop evidence of who is at fault and the cause of the loss. The customer will have access to evidence developed in these

112. *Id.* § 2B-102, Reporter's Note 2.

113. *Id.* § 2B-102(a)(3).

114. *See* U.C.C. § 4A-203, cmt. 3 ("A customer may want to protect itself by imposing limitations on acceptance of payment orders by the bank"). *Id.* "Some customers may be unwilling to take all or part of the risk of loss with respect to unauthorized payment orders even if all of the requirements of Section 4A-202(b) are met." *Id.* § 4A-203, cmt. 6.

> investigations and that evidence can be used by the customer in meeting its burden of proof.[115]

Unfortunately, access to such rigorous investigation and proof will be lacking in the typical transactions covered by Article 2B.[116]

Third, Article 2B adopts an additional ground for shifting risks: if the person alleged to have sent the message can nonetheless prove that it did not send the message—a somewhat difficult task to begin with—that person may still be liable for losses "in the nature of the cost of performance of the other party"[117] if the loss occurred because: 1) the purported sender failed to exercise reasonable care; 2) the other party reasonably relied on the belief that the purported sender sent the message; and 3) the fraudulent third party who used the attribution procedure gained access to it from a source under the control of the purported sender.[118] The net result is that it may well be impossible for an alleged sender to avoid attribution under Article 2B.[119]

VIII. INTO THE BREACH: LEGISLATING FOR SECURITY

When the UETA Drafting Committee was first established, the assumption, and, indeed, the mandate given to that committee, was to avoid inconsistency with the revisions being proposed to the Uniform Commercial Code, and, in particular, Article 2B. Theory, however, has diverged from practice, as illustrated by Article 2B's adoption of a presumption approach, and its not-so-hidden desire to go beyond mere removal of barriers to

115. U.C.C. § 4A-203, cmt. 5.

116. The difficulties in proving a negative raise another issue: the burden on the party attempting to avoid liability arguably is the same (to prove the message did not come from a source controlled by that party) regardless of the security procedure at issue. Yet not all technological security procedures are created equal; what they involve, what they prove, and the strength of their proof vary. Even "digital signatures" come in different strengths: the longer the number used to generate the key pair, the harder it is to crack the code, and the shorter the number, the easier it is. Yet all commercially reasonable security procedures are treated equally with respect to the presumption.

117. U.C.C. § 2B-116 (Proposed Draft Feb. 1, 1999).

118. *Id.* For a history of the evolution of this provision and its source in both Article 4A and the UNCITRAL Model Law on Electronic Commerce, see Boss, *supra* note 4, at 1961–63.

119. Take the situation of a person who has attribution procedures resident on an office computer and locks the office to attend a weekend meeting, where there are ample witnesses to confirm that it was physically impossible to send the message at issue. Proof that it was physically impossible for that person to send the message would not be sufficient to satisfy the burden of establishing that the electronic message was not caused by anyone entrusted by that person with the office, someone who gained access to the office, or someone who gained information facilitating breach from that person.

actively supporting electronic commerce, and the rejection of that approach in the UETA. According to the Chair and the Reporter for the UETA, "perhaps the most significant difference between the UETA and Article 2B relate[s] to the creation of presumptions when security procedures are employed by parties to an agreement."[120]

These differences continue despite attempts to harmonize the approaches between those two drafts; the only agreement is continued disagreement.[121] "In light of the different character and scope of the respective drafts, it was agreed that the different approach in the two drafts can be justified."[122] What is far from evident[123] is what differences in character and scope justify the difference in approach to presumptions. Although it is true that Article 2B has a narrower scope than the UETA in that it applies only to certain informational contracts while the UETA potentially applies to any contracts entered into online, the reality is that under both, there is a wide range of sophistication in the parties potentially subject to their provisions, and under both, identical arguments may be made about the need to support electronic commerce. The only conclusion that can be drawn is that each Drafting Committee has a different view about the relationship between the law and security.

On one hand, the philosophy of the UETA is the minimalist approach: as long as the law recognizes and enforces electronic transactions, businesses gain some "security" in their commercial dealings. The role of law in technology is enabling, not promotional of certain technologies, nor channeling, encouraging certain procedures. This approach recognizes that "technological security" is not monolithic: there are many technological methods of security, with different strengths and weaknesses, and technology is in a constant stage of development.[124] Thus, promoting certain technologies or certain implementations would be counterproductive. This approach also recognizes that the law is of limited utility in encouraging

120. Memorandum, *supra* note 90.

121. Each Drafting Committee reaffirmed its own approach, and rejected that of the other, in its last meeting in February 1999.

122. Memorandum from Patricia B. Fry, UETA Drafting Committee Chair, and Carlyle C. Ring, Jr., U.C.C. Article 2B Drafting Committee Chair, to the UETA and Article 2B Drafting Committees (Jan. 29, 1999) <http://www.2Bguide.com/docs/199pfcr.html>.

123. This is true even to one who is both on the Article 2B Drafting Committee and the official American Bar Association Advisor to the UETA Drafting Committee. The statement may simply be a recognition that different drafting committees, dealing with different subject matters, came up with different solutions.

124. "While a number of participants argued that *fairly strong presumptions are necessary to promote electronic commerce*, others felt that the state of technology and current market are still too underdeveloped to warrant the creation of any presumptions." Memorandum, *supra* note 90.

certain types of behavior: people will use security procedures because it is good business, not because the law gives special legal effects if they are used. The marketplace, rather than the legislature, provides the incentives and support. The UETA does not view the law as the sole or even primary source of security; instead, it recognizes that the entire technological, legal, and social structure contributes to that security.

On the other hand is the view that the law has an important role in providing "security" in electronic commerce; that the law can indeed "legislate" security by providing certain benefits to those who use the available technology. Article 2B, following the lead of Article 4A,[125] represents the position that statutory provisions that recognize those security procedures can encourage use of security procedures.[126] By assuring parties involved in "electronic commerce" of the ability to enforce transactions in which reasonable security procedures are used, the law creates user confidence and ultimately supports and promotes the use of electronic commerce.

Each approach has its critics. The minimalist approach, limited to the removal of barriers, has been criticized as not giving the user of technology the degree of assurance necessary. Critics emphasize that simply saying electronic messages "may" suffice or are equivalent to writings and signatures is insufficient; users want to know what *will* suffice. Consequently, it is asserted that the legislation must lay out the indicia of assurance and certainty necessary for the electronic messages to be deemed reliable.[127]

The question, however, is whether the Article 2B approach gives any greater certainty or any greater assurances than the minimalist approach. In giving special effect when commercially reasonable security procedures are present, what must be asked is whether Article 2B has met the goals of

---

125. Article 4A theorized that losses due to fradulent payment orders can best be avoided by the use of commercially reasonable security procedures, and that the use of such procedures should be encouraged. U.C.C. § 4A-203, cmt. 3. The rules designed to "protect both the customer and the receiving bank," were aimed at providing such encouragement. *Id.* Thus, the customer may not be held liable *unless* commercially reasonable security procedures are agreed to, and the bank is protected if they are agreed to and are implemented. *Id.*

126. As one letter put it: "Given the limited experience with electronic commerce, NCCUSL should gravitate towards general legal principles that provide incentives for, and reward the use of, *commercially reasonable* and *agreed* procedures that give courts a basis to select and adjust to the facts of individual cases." Memorandum from Business Software Alliance to Article 2B Drafting Committee (Jan. 20, 1999) <http://www.2Bguide.com/docs/0119bsa.html>. Of course, as discussed, Article 2B goes well beyond agreement.

127. *See* Michael S. Baum, *Linking Security and the Law of Computer-Based Commerce* <http://www.verisign.com>.

"security:" more certainty and predictability in the application of the law; greater assurances of the validity of the transaction; encouragement of the use of security procedures; and more faith or trust in the systems.

It is questionable whether, as currently articulated, Article 2B contributes to the certainty and predictability in the application of the law. The factual nature of the commercially reasonable standard[128] renders it vague and subjective in nature,[129] a result which "could hardly have been more inconsistent with the drafters' statement that 'the parties . . . transfer need to be able to predict risk with certainty.'"[130] It is true that in the context of funds transfers, the same test has been used, but the funds transfer situation differs.[131] Determining what is "commercially reasonable" in an industry where there is a developed body of commercial practices, where the

128. U.C.C. § 2B-114 (Proposed Draft Feb. 1, 1999) ("commercial reasonableness is [to be] determined in light of the purposes of the procedure and the commercial circumstances at the time the parties agree to or adopt the procedure."); *id* ("How one gauges commercial reasonableness depends on a variety of factors, including the agreement, the choices of the parties, the then current technology, the types of transactions affected by the procedure, sophistication of the parties, volume of similar transactions engaged in, availability of feasible alternatives, cost and difficulty of utilizing alternative procedures, and procedures in general use for similar types of transaction."). *Id.*, Reporter's Note 4.

129. This objection has been made on both the domestic level as well as on the international level (where the concepts of "reasonableness" and "commercial reasonableness" generally do not have the same level of acceptance as they do within the United States). *See* letter from Paul Shupack, Paul S. Turner, and Jane K. Winn (Jan. 20, 1999) <http://www.2Bguide.com/>.

130. *Id.* (citing Official Comment to Section 4A-102).

131. In the Article 4A context, the use of the phrase was justified on the grounds that to the extent one goal of Article 4A was to shield banks from potential catastrophic losses by shifting some wire fraud risks to customers, the "commercially reasonable security procedure" requirement was one way of achieving a balance by limiting the bank's ability to shift the risk in egregious circumstances. According to that line of argument, the national interest of protecting recipients of messages from catastrophic losses (which was present in the bank regulation arena) is absent in the more generic area of electronic commerce. Thus, a device (the requirement of a commercially reasonable security procedure) which was originally adopted to protect customers from a rule of absolute liability is now being invoked to impose liability. *See* Letter from Shupack, Turner, & Winn, *supra* note 126.

This description of the intent of the "reasonable security procedure" requirement of Article 4A has been disputed by the Chair of the Article 2B Drafting Committee, who also chaired the Article 4A Drafting Committee. Memorandum of Carlyle C. Ring, Jr. (Jan. 25, 1999) <http://www.2Bguide.com/>. His account points out that, in its application, Article 4A places the risk of unauthorized orders on the bank; the bank is only able to shift that risk to the customer if it finds that commercially reasonable security procedures are used. While his argument correctly interprets the language and structure of Article 4A as it currently existed, it does not respond to the argument that the alternative in Article 4A was to shield banks from liability by placing all risks on the customer.

parties belong to a relatively closed community of players, and where the major participants are either large, sophisticated commercial parties or banks subject to strict regulatory oversight[132] is a different burden than proving what is "commercially reasonable" when such factors are absent. In other words, although benefits are intended to flow from the use of "commercially reasonble" security procedures, the introduction of notions of "commercial reasonableness" is a serious qualification on the legal construct that weakens its usefulness as a guiding beacon for business.[133] Thus, according benefits when "commercially reasonable" security procedures are used may not provide the type of "security" that the industry is seeking, given the vagueness and uncertainty inherent in the formulation and the difficulty in determining whether a particular procedure may be commercially reasonable under the circumstances.

Just as it is questionable whether the goal of "certainty" is met, it is also questionable whether Article 2B gives the user any greater assurances than would exist under the UETA. To get the benefit of the beneficial treatment accorded by the statute, the proponent would still have to prove that there was a method adopted by the parties to authenticate the message as that of the sender, that the method adopted did operate as an authentication device, and that under the circumstances of the transaction, it in fact operated reasonably as an authentication device. In other words, to get the benefit of the statute, the recipient would have to prove essentially the same set of facts one would normally need to prove attribution directly.[134] Thus, it is doubtful

---

132. Boss, *supra* note 9, at 1079–80, 1083.

133. Of course, to the extent a vague standard of "commercial reasonableness" falls far short of laying out the indicia of assurance and certainty necessary for reliability, one could argue for more specificity in the type of security procedures sanctioned by the law. To the extent a specific technological implementation does indeed provide assurances of reliability, it is argued that implementation should be given greater efficacy under the law. This can be accomplished through statutory or legal provisions treating these more secure methods as conclusively satisfying signature and writing requirements and as providing evidence of source and identity of the sender, as well as the integrity of the content of the message. The more detail and "indicia," however, one lays out in a statute, the more regulatory and binding the scheme becomes. Also, there is less flexibility with respect to emerging technologies and implementations and the needs of the parties.

134. That is not the case where there is an agreement: then all the recipient would need to prove was the agreement itself and compliance with its procedures. Similarly, where there is a specific statute or regulation validating a specific technological method of authentication, all that the recipient would need to prove is that the specified method was used. The proof issues become complicated when the recipient must prove "commercially reasonable attribution procedures," as is the case with Article 2B, or when it must prove that the method used qualifies as a "secure electronic signature," the approach followed in Illinois and in the proposed UNCITRAL legislation.

whether the "commercially reasonable security procedure" standard at all helps the litigant with her burden of proof.

The goal of encouraging the use of security procedures is also troublesome, and the risk exists that the statutory scheme may actually operate as a disincentive. As was observed in the context of the UETA, a rule placing the risk of loss on the person requiring use of a specified security procedure might indeed discourage people from designating certain procedures;[135] a variation of this provision in Article 2B[136] was deleted at the Drafting Committee's last meeting for this very reason. The same question can be raised about the other provisions in Article 2B with regard to attribution: does adopting presumptions that make it easier for one party to prove a transaction in court, while at the same time making it difficult, if not impossible, for the other party to disprove the transaction, result in encouraging or discouraging the use of security procedures? No special proof rules exist, for example, in the context of phone orders or mail orders, yet those businesses thrive. Article 2B's rule encourages recipients of messages to use "commercially reasonable attribution procedures" by giving them statutory incentives, but it does not provide similar incentives to potential senders of electronic messages. Indeed, the rules may arguably discourage potential senders from adopting certain methods of communication for fear of having liability imposed, in actions with strangers, where the alleged sender did not send the message.[137] If, indeed, part of the problem is that people are concerned about the "unknown" and the potential of unintended liability, rules such as this feed rather than assuage their fears.

Additionally, Article 2B takes the view that by providing those benefits, one in turn *increases* the confidence of those doing business electronically because they can now reasonably rely on receipt of electronic messages from strangers. This view of security and its relationship to the law assumes that the value and security added to electronic commerce in this manner is both appropriate and acceptable. As noted above, however, that security may be illusory. First, to the extent that potential users of the technology are discouraged from its use because of fear of potential liability, their confidence in the system is *decreased.* More importantly, however, whatever confidence flows from the use of security procedures in electronic commerce arguably comes *not* from the knowledge that the law gives the

135. *See supra* notes 91–94 and accompanying text.

136. U.C.C. § 2B-115 (Proposed Draft Feb. 1, 1999).

137. Consumer representatives, for example, have pointed out that the credit card scheme that currently exists protects consumers in the case of fraud or unauthorized use of their cards, while in contrast, an Article 2B approach in the consumer context would protect the merchant. The UETA approach is to favor neither party.

users benefits but from the knowledge that the technological implementations themselves are trustworthy.

On the federal level, several agencies have noted the need to avoid allocations of risk at a time when electronic commerce is still evolving. Thus, the Federal Reserve Board, considering the question of stored value cards, noted:

> Economic theory and empirical evidence suggest that government regulation has the potential to foster or hinder technological progress and the development of new products by influencing private sector incentives to invest in research and development activities and private sector choices among alternative technologies. In deciding whether and, if so, how to regulate . . . policymakers must carefully assess the potential effect of their decisions on the evolution of these new products and the extent to which they achieve market acceptance.[138]

In similar words, the White House, which had previously urged governments to avoid undue regulation of the market,[139] urged flexibility in the drafting of electronic commerce laws, in large part to prevent unwarranted market distortion. This is expressed in the following:

> The market is very much in the early stages of experimentation with respect to business models for electronic commerce. The United States believes it is not wise at this time to attempt to identify a single model that these transactions will use or to develop a legal environment using a single model. Indeed, such an approach would prevent the market from testing different possible approaches and prematurely impose a particular model on all electronic commerce, inevitably limiting its growth. Therefore, at the current state of development, the legal framework should support a variety of business models so that the market is able to experiment and select the models that best fit particular types of electronic commerce.[140]

---

138. Board of Governors of the Federal Reserve System, *Report to the Congress on the Application of the Electronic Funds Transfer Act to Electronic Stored-Value Products* (Mar. 1997) <http://www.bog.frb.fed.us/boarddocs/RptCongress/efta_rpt.pdf>.

139. *See supra* note 30.

140. U.S Government Working Group on Electronic Commerce, First Annual Report (Nov. 1998) <http://www.doc.gov/ecommerce/E-comm.pdf>.

IX. CONCLUSION

No one disputes the fact that security issues in electronic commerce, both of the technological and non-technological kind, are extremely important. This is true even of those who adhere to the notion that the law should, at this stage, simply *remove* barriers but otherwise stay neutral on the subject. Indeed, security is one of the primary concerns that should be addressed by businesses migrating to electronic communication and businesses online.[141] Thus, in the case of agreements between businesses doing electronic commerce, it makes sense to go beyond merely requiring "reasonable security procedures" to explain in specific detail what procedures are required,[142] and where the agreement is specific as to the effects to be given to the use of those procedures, it makes sense to give deference to that agreement. Similarly, the development of industry standards and codes of conduct addressing security is of extreme importance.[143] Industry codes and standards operate to inform business people as to the variety of technological security means at their disposal, thereby empowering them to make intelligent choices. This type of education clearly gives the businesses a sense of security.

The real questions go to the relationship between the law and these "security" issues: what type of "legal security" is necessary? Should the law set forth a legal regime specific to certain technologies or implementations, providing certain benefits when that technology is used? While it may be true that certain technological security procedures are "uniquely suited to the needs of secure e-commerce,"[144] two key points

141. *See supra* note 21, cmt. 1 (1990) ("Adequate security procedures are recognized . . . as critical to the efficacy of electronic communication. . . . The use of adequate security enhances the reliability of those records and enhances the ability to prove the substantive terms of any underlying commercial transaction.").

142. *See, e.g., Model Electronic Payments Agreement and Commentary* at § 7, cmt. 5; 32 JURIMETRICS J. 601, 654 (1992) ("in certain situations a lack of specificity in defining 'reasonable' security procedures may provide inadequate guidance causing such security procedures to fail in their intended purpose. Specificity may help the parties implement and comply decisively and unambiguously with security procedures, reduce confusion and offer better expectations of reliability and certainty. Security procedures should be sufficiently precise so that they are not subject to discretionary, self-serving interpretation").

143. *See* Information Security Committee, Section of Science and Technology, *American Bar Association, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* (1996) <http://www.abanet.org/scitech/ec/isc/home.html/ >.

144. This claim, often made of digital signatures within a public key infrastructure, *see* Baum, *supra* note 46, has been disputed both because it assumes all implementations of the technology are the same when they are not, and it ignores other technological security procedures such as biometrics.

remain. First, while certain types of technology today may be considered sufficiently secure to merit special treatment, future technological advances raise the possibility that: 1) methods of security currently used may cease to be secure in the future; and 2) other methods of security and other modes of technological implementation will provide comparable or even better means of security. Given the time lags inherent in the updating of laws,[145] drafting a technology-specific or implementation-specific body of rules may not be prudent.[146] Drafting a more general body of rules that depend upon such concepts as "commercially reasonable security procedures" or that set out criteria that security procedures must satisfy present a different problem: the creation of a legal regime lacking the certainty desired by many business people.

The theory that these laws "encourage" the use of security procedures is questionable. If indeed certain technological security techniques are uniquely situated to the needs of secure electronic commerce, they may well be implemented without the adoption of specific rules. "One compelling example of the dramatic success of open PKI is the ubiquitous use of the SSL (Secure Sockets Layer) protocol over shared paths such as the Internet for e-commerce."[147] That proposition, while asserted as evidence of the need for PKI specific legislation, arguably proves the opposite: if there is a good, secure method of doing electronic commerce, that method will be implemented as a matter of sound business practices, not as the result of PKI specific legislation. In other words, the technology implementation itself provides the necessary security and certainty necessary for electronic commerce without the need for legislative intervention.[148]

145. The need to revise our domestic and international laws to accommodate electronic commerce has been a theme for well over a decade, yet we are still attempting to address that need through statutory enactment.

146. *Cf.* C. Bradford Biddle, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace*, 34 SAN DIEGO L. REV. 1225 (1997).

147. Baum, *supra* note 124, at 38. According to Baum, the total number of sites using SSL has risen from 486 in the third quarter of 1996, to 104,760 in the third quarter with a projected rise in the fourth quarter of 1999 to 307,206. The total number of sessions, as opposed to sites, has similarly increased during that period from 291,600 to 134,775,517, and is projected to rise to 636,335,396. *Id.*

148. An example lies within the development of the SET protocol, which involves the use of digital signatures in the credit card system. MasterCard and Visa, who under current arrangements potentially bear the risk of fraudulent transactions, charge their participating merchants a percentage based on the risk involved in particular transactions, e.g., the rate assessed for telephone order charges is much higher than the rate assessed in transactions evidenced by both the card imprint and card holder signature. They have announced, however, that when the SET protocol is implemented in the credit card system, and, presumably, the risks of fraud drop, they will lower their merchant discount rate by several percent. Thus, the benefits of security implementation are being realized not through the

The difficulty with much of this debate over whether or not to recognize specific means of technological security is that the discussion is misplaced. If the technology provides reasonable means of security, people will implement the technology for that reason, not because the law says so. A person who installs locks on his or her door does not do so because greater legal protection is afforded those who use the technology; a person installs locks because experience has shown that locks are one means of stopping intruders. A business that requires checks to be signed by more than one officer does so not because the law requires but because it is a good business practice that reduces risks of fraud, and a bank which institutes the practice of manually examining the signatures on checks over a given amount does so not because the law requires it but because it is a prudent banking practice to reduce risk of fraud. The economic and other benefits to be gained from implementation of secure systems is not disputed; what is disputed is the need for the law to enact legislation saying that these secure systems are secure and therefore are entitled to special treatment. Such legislation may be neither needed nor wise.

There is no doubt that "security" in electronic commerce is an important issue, but the debate over electronic signature legislation is misleading in that it fails to recognize that security is more than merely the legal effects to be given to certain technological security techniques. Once we recognize that fundamental point, we can place the discussions about what type of legislation is necessary and appropriate in perspective and evaluate the claims for what they are worth.

---

enactment of any legislation but through marketplace recognition of the risk reduction additional technological security brings.

Ira Glasser
Executive Director – American Civil Liberties Union

Mr. Glasser has served as Executive Director of the American Civil Liberties Union since 1978. Previously, he was executive director of the New York Civil Liberties Union.

Prior to his affiliation with the ACLU, Mr. Glasser was a mathematician and a member of the science and mathematics faculties of Queens College and Sarah Lawrence College. He was also editor of *Current Magazine*.

Mr. Glasser authored a book, *Visions of Liberties: The Bill of Rights for All Americans*, published in November 1991. An insightful analysis of how our rights developed, written to commemorate the 200th anniversary of the Bill of Rights, *Visions* was published by Arcade Publishing, Inc., in New York City.

In addition to *Visions*, Mr. Glasser is a widely published essayist on civil liberties principals and issues, whose writings have appeared in *The New York Times*, *The Village Voice*, *Harper's*, *The New Republic*, *The Nation*, and *Christianity and Crisis*, among other publications. He is also the co-author of *Doing Good: The Limits of Benevolence*, published by Pantheon in 1978.

Mr. Glasser received a B.S. degree in Mathematics and graduated with honors in Literature and the Arts from Queens College in 1959. He has a master's degree in mathematics from Ohio State University and also studied sociology and philosophy on the graduate level at the New School for Social Research.

Born and raised in New York, Mr. Glasser is married and the father of four children.

The Struggle for a New Paradigm: Protecting Free Speech and Privacy in the Virtual World of Cyberspace

Ira Glasser

TABLE OF CONTENTS

I. INTRODUCTION

Constitutional struggles are, of necessity, most frequently fought out in terms of law and legal principles. While this is inevitable, it often obscures the underlying moral issues, the debate over values that always precedes the formation of constitutional principles and always infuses the effort to implement and interpret them.

For example, it is often, though mistakenly, said that we support free speech because of the First Amendment, when the truth is the reverse: we support the First Amendment because we believe in free speech. If opponents of free speech succeeded in repealing the First Amendment, it would not alter support of free speech by those who believed in it. However, they would be less able to protect it. The First Amendment was the invention of those who believed in free speech and thought it required constitutional protection, enforceable in the courts.

Similarly, the belief in the value of privacy preceded the Fourth Amendment, the latter having been invented by those who thought that a man's home was his castle[1] and that the castle required a constitutional moat to inhibit

1. The founders, sensitive as they were to the notion of natural rights, were not yet so sensitive as to recognize that a woman's home was her castle as well.

the state's unwarranted trespasses.[2] Therefore, in evaluating and adapting the values of the Constitution to modern conditions, we need to place ourselves in the position of the framers, who found themselves without a Bill of Rights and endeavored to decide, without reference to a prior constitution, what values should be protected and what rights needed to be legally enforced through the Constitution. This is not meant to suggest that constitutional adjudication requires, in any simplistic way, a preconstitutional exploration of original intent. Rather, it is to argue that in debating what values a constitution should protect, we need first to identify and debate those values apart from, and prior to, their constitutional formulations. It may well be, for example, that certain values like free speech or privacy can be adequately protected by current, properly interpreted provisions of the Constitution. Or it may be that they cannot, and constitutional amendments to do so should be proposed. But, that is a different question from what values we want the Constitution to protect and it is the latter question that takes precedent.[3]

The unexamined premise of this article is that the values of free speech and privacy, as commonly understood today, are believed by most Americans to be worth protecting and that it is our task to find ways of doing so, either by adapting through reasonable interpretations the Constitution we have or by amending it to include the protections we desire. At the very least, this article assumes, *arguendo*, that the rights of free speech and privacy that we already have should not be eroded by the unintended effects of technological developments.

Inevitably, technological advances always change the circumstances under which basic values exist, sometimes nourishing those values and sometimes threatening them. Both occur at the same time more often than one would expect, rendering the debate over such values especially complex, and altering the paradigms that were previously understood to govern constitutional constraints.

II. THE INVENTION OF THE PRINTING PRESS AND HOW IT AFFECTED THE LAW OF FREE SPEECH

For example, the invention of the printing press had a revolutionary impact on the value of free speech in fifteenth century England by both

2. *See generally* IRA GLASSER, VISIONS OF LIBERTY: THE BILL OF RIGHTS FOR ALL AMERICANS, (1991) and in particular, Ch. 1, at 21; Ch. 3, at 114–18; and Ch. 4, at 165–66.

3. The reference in this context to "values" the Constitution should protect refers not to all values, but rather to those that define the proper boundaries between what John Stuart Mill called "individual sovereignty" and the police power of the state. *See generally* JOHN STUART MILL, ON LIBERTY AND OTHER ESSAYS 14 (John Gray ed., 1991).

nourishing it and threatening it. Indeed, it is fair to say that the threats to freedom of speech arose out of its nourishment, out of a fear by the British government that this new technological device, which made speech more indiscriminately accessible, required legal curbs not previously thought to be necessary.[4]

Thus, in 1456 when the printing press was invented, fewer than 15,000 books existed in all of Europe.[5] Books were a rare commodity, as were people who were able to read them. Access to the printed word was not widespread. Suddenly, with the invention of the printing press, speech and opinion could be widely disseminated. Before the invention of the printing press, speech and opinion had been audible only to listeners in the immediate vicinity of a speaker or, if in written form, accessible only to a very limited number of readers. However, after the invention of the printing press, ideas and opinions could be spread relatively cheaply by anyone with access to a printing press to anyone who could read. Moreover, the widespread access to the printed word meant that people had an incentive to learn how to read.

Although the effect of this change was not immediate—just as the broad effect of radio, television, and the Internet could not be immediate—the potential of this means of communication was incendiary, and the British government was not slow to recognize the threat and take steps to put out the fire of unfettered thought. Thus, if the printing press would ultimately nourish the development of free speech, it would also, and more immediately, provoke governmental restrictions.

Relatively swiftly, Parliament enacted laws to control what could be published. Censorship was imposed through various mechanisms. For example, printing presses were required to be registered with the government as if they were dangerous weapons,[6] the number of printers was limited, books could not be sold without a government license, and broad powers to search for illegal publications were established.[7] In short, a tissue of legal

4. This is similar to the dynamic that in 1996 led Congress to pass, and President Clinton to sign, the Communications Decency Act of 1996. Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133 (codified as amended at 47 U.S.C. § 223 (Supp. II 1997)). This Act consists of legal restraints designed to curb speech on the Internet that would have been constitutionally impermissible to curb in other forms of media, such as newspapers, books, magazines, or leaflets. *Id.*

5. *See generally* JAMES MORAN, PRINTING PRESSES; HISTORY AND DEVELOPMENT FROM THE FIFTEENTH CENTURY TO MODERN TIMES (1973).

6. An interesting analogy is the current effort by the Clinton administration to construe strong encryption as a weapon and bring it under the legal constraints of laws restricting the export of weapons.

7. *See* MORAN, *supra* note 5.

constraints was created so that nothing of consequence could be printed, unless approved in advance, by either the government or the church.

These laws were harshly enforced by special courts called the High Commission, which was the supreme ecclesiastical tribunal, and the Star Chamber, which was the highest royal court. The Star Chamber in particular came to be used to punish critics of the king, and those who published or circulated unorthodox literature. Playwrights were heavily fined for plays that made fun of the church. But fines were the least of the punishments meted out; other punishments included ruinous and torturous physical mutilations.

This assault by the government was so massive that those who championed freedom of the press could hardly imagine resisting the substantive restrictions of the new laws. Instead, free speech advocates limited themselves to the goal of abolishing those laws requiring advance approval of printed matter by the government. Freedom of the press thus became synonymous, not with the freedom to print what one wanted without fear of government punishment, but rather with the limited idea that no advance government approval should be required. The goal of ending prior restraints was the leading edge of the free speech movement. Eventually, that goal was reached. In 1695, the English licensing law expired and was not renewed.[8] The system of prior censorship was ended.

This, of course, left the substantive restrictions intact. People could now go ahead and publish without prior approval, but at considerable risk. It remained illegal to criticize the crown, the government, and the church and it was perilous to do so. This was called seditious libel and it was nearly universally believed to be a category of speech legitimately restricted by law.[9] As late as the end of the seventeenth century, violating these laws was regarded as treason, and was punishable by death, which was often gruesomely executed. By the eighteenth century, seditious libel remained illegal, but was no longer considered treason. Therefore, the punishment for this crime was reduced. For 150 years after the licensing laws requiring prior approval were abandoned, people in England were prosecuted, convicted, and punished for their words.[10] They were free to speak and publish, but they risked punishment *afterward*. Virtually everyone accepted

8. *See* Thomas I. Emerson, *Freedom of the Press*, *in* 2 ENCYCLOPEDIA OF THE AMERICAN CONSTITUTION 798 (Leonard W. Levy et al. eds., 1986).

9. *See id.*

10. *See* David A. Anderson, *Seditious Libel*, *in* 4 ENCYCLOPEDIA OF THE AMERICAN CONSTITUTION 1644 (Leonard W. Levy et al. eds., 1986). *See also* LEONARD A. LEVY, ORIGINAL INTENT AND THE FRAMERS' CONSTITUTION 197 (MacMillan 1988).

this as the proper boundary between freedom of speech and government restraint. In 1769, only a few years before the American Revolution, the most influential legal scholar of his time, William Blackstone, put it this way:

> The liberty of the press is indeed essential to the nature of a free state; but this consists in laying no *previous* restraints upon public actions, and not in freedom from censure for criminal matter when published. Every free man has an undoubted right to lay what sentiments he pleases before the public; to forbid this, is to destroy the freedom of the press; but if he publishes what is improper, mischievous or illegal, he must take the consequences of his own temerity.[11]

Blackstone's view continued to reflect the prevailing view of what was legally proper at the time the First Amendment was drafted in America. However, the practice of free speech in America at first exceeded the legal concept of what constituted a free press. The law in early America prohibited criticism of the government.[12] Seditious libel laws were common among the thirteen original states.[13] Yet, as a matter of practice, the press vigorously criticized public officials, often in terms that resembled modern-day tabloid talk radio shows.[14]

Then, in 1798—scarcely seven years after the First Amendment was ratified—a major event transformed the early Americans' understanding of what it took to protect the right to criticize the government. This event undermined the Blackstonian view that had dominated legal thought during that time. At the time, John Adams was President, and his administration and its followers seemed intent upon encouraging a war with France and, perhaps, reestablishing an alliance with England. This was a matter of such hot dispute that some newspapers of the day were intensely engaged in a harsh criticism of the Adams Administration, even attributing to it a desire to

---

11. Thomas I. Emerson, *Freedom of the Press, in* 2 ENCYCLOPEDIA OF THE AMERICAN CONSTITUTION 798 (Leonard W. Levy et al. eds., MacMillan 1986) (citing William Blackstone, *Commentaries* (1769)).

12. *See* LEONARD W. LEVY, ORIGINAL INTENT AND THE FRAMERS' CONSTITUTION 195-228 (1988).

13. *See generally* LEVY, *supra* note 12.

14. *Id.*

undo the Constitution and restore a monarchy.[15] The government's effort to quash this criticism resulted in the first federal sedition act being passed by Congress.[16] The Sedition Act made it a crime, punishable by both a fine and prison, to publish "false, scandalous and malicious" criticism of the government, Congress, or the President, "with intent to defame" them or to heap contempt upon them or damage their reputations.[17]

The war with France never came, but the Sedition Act was widely enforced against American citizens, all of which were Democratic-Republicans (Thomas Jefferson's party) and political opponents of President Adams and his followers. Editors, scientists, pamphleteers, and even one member of Congress were arrested.[18] While all were fined and imprisoned, some died in jail awaiting trial. Despite the First Amendment,[19] the Sedition Act was passed by the Senate 18 to 6, and by the House, 44 to 41.[20]

Democratic-Republicans were shocked by this. They learned for the first time how insufficient the Blackstonian view was. The Sedition Act, after all, was a model of civil libertarian principles, as commonly understood at the time. It punished speech only after publication, imposed no prior censorship, and even authorized truth as a defense, which was a great advance. It thus permitted critics of the government to win acquittal of the charges against them by proving the truth of their criticisms. Only false criticisms would be punished, which was what even Jefferson said he wanted.[21] What could be wrong with permitting the government to punish false criticism while leaving truthful criticism immune?

The Sedition Act of 1798 showed Jefferson and his political colleagues why truth as a defense was a trap, not a safeguard. A government seeking to suppress criticism could indict anyone it wished to silence, exposing him to the cost of a trial and the risk of a serious penalty. Moreover, who would

---

15. For a general history of this turbulent period written from the point of view of the Adams administration and utilizing verbatim newspaper accounts from that time, see RICHARD ROSENFELD, AMERICAN AURORA (1997).

16. Sedition Act of 1798, Ch. 74, 1 Stat. 596 (1798) (expired in 1801).

17. Merrill D. Peterson, *Alien and Sedition Acts*, *in* 1 ENCYCLOPEDIA OF THE AMERICAN CONSTITUTION 43-44 (Leonard W. Levy et al. eds., 1986). Sedition Act of 1798, Ch. 74, 1 Stat. 596 (1798) (expired in 1801).

18. *See* Merrill D. Peterson, *Alien and Sedition Acts*, *in* 1 ENCYCLOPEDIA OF THE AMERICAN CONSTITUTION 43 (Leonard W. Levy et al. eds., 1986).

19. The First Amendment states: "Congress shall make no law . . . abridging the freedom of speech, or of the press; or [of] the right of the people . . . to petition the Government for a redress of grievances." U.S. CONST. amend. I.

20. WILLIAM O. DOUGLAS, AN ALMANAC OF LIBERTY 12 (1954).

21. LEVY, *supra* note 12, at 199–200.

decide what was true and what was false? These were necessarily highly subjective judgments, vulnerable to precisely the kind of prejudice that led to the prosecutions in the first place. Judges and juries, who would reflect the general hysteria as often as they would be likely to curb it, would have the power to decide what was true and what was not. As the convictions mounted, it became clear that the power to prosecute speech itself was the problem. The defense of truth was no defense at all.

A new idea of freedom of expression began to emerge. If the right to free speech was to be protected against government attempts to suppress criticism, legal limits on government power would have to extend to punishment after publication as well as to previewing and censorship before the material was published. People began to see that a law allowing the government to impose punishment after publication would have precisely the same effect as a law allowing the government to censor speech before publication. James Madison expressed this growing idea pungently: "'It would seem a mockery to say that no laws shall be passed preventing publications from being made, but that laws might be passed for punishing them in case they should be made.'"[22]

That the government should not be able to punish speech after publication meant that even scurrilous speech, including false accusations and misrepresentations of fact, would not only be tolerated, but would be protected by law; a radical departure.[23] Before this, even advanced libertarians had assumed that freedom of the press meant only the legal freedom to publish the truth, whereas falsehoods could and should be punishable. However, after the experience with the Sedition Act of 1798 people began to realize that if the government had the power to punish false speech, it would inevitably use that power to silence its critics.

John Thomson expressed this new idea in a book he wrote in 1801 called *An Enquiry into the Liberty and Licentiousness of the Press, and the Uncontrollable Nature of the Human Mind.*[24] Any laws prohibiting "licentious" speech, he wrote, would inevitably be used by those who wished "nobody to enjoy the Liberty of the Press but such as were of their own opinion."[25] That was what occurred in 1798 when, under the pretext of protecting America against a foreign menace, the Adams administration used

22. LEVY, *supra* note 12, at 215.

23. LEVY, *supra* note 12, at 215–18.

24. JOHN THOMSON, AN ENQUIRY, CONCERNING, THE LIBERTY, AND LICENTIOUSNESS OF THE PRESS, AND THE UNCONTROLLABLE NATURE OF THE HUMAN MIND (photo. reprint 1970) (1801).

25. *Id.*

the Sedition Act of 1798 to target its domestic political critics: all ten men convicted under this Act were Republicans who had criticized the Adams administration and its policies, and all were pardoned by the next Republican president, Thomas Jefferson.[26]

It may have seemed abstractly logical to protect truthful criticism while allowing the law to punish false or malicious criticism, but in the world of political power, that was not the way it worked. Often, the very purpose of criticism was to damage the reputation and undermine the credibility of the party in power. Permitting the target of criticism to prosecute his critics would inevitably destroy freedom of expression. In practice, there was no way to neatly separate truth from error. Political truth was often a matter of subjective judgment, not scientific determination. How would a jury evaluate political truths? It was, said John Thomson, rather like letting a jury decide which was the most tasty food or the most beautiful color, and then allowing it to punish anyone who had a different view.[27] If the government was given the power to punish false or malicious speech, would it not naturally use that power to punish any speech it found too critical? That was exactly what had just happened with the Sedition Act—why should it ever be any different?

Furthermore, how could the accused prove to his accusers that what he said was true? The experience with the Sedition Act had shown beyond doubt that the defense of truth, long thought to be a safeguard, was no safeguard at all. It could never protect a critic against prosecution, and it would hardly ever protect him against conviction. Republicans who were sent to jail by the Adams administration for their malicious speech came to understand that the only important question was who had the power to decide the truth of their statements. Since they could not be certain of always holding political power, they began to believe that the best way to protect their own freedom of expression was to prohibit *any* government from prosecuting *any* speech.

The Republicans initially developed this theory out of blatant self-interest. They were a political minority trying to gain political power by first persuading people of the folly of the party in power, and second persuading them of their own virtue. When they did this, they were prosecuted for seditious libel for maliciously criticizing the government. Therefore, they championed the right to freedom of speech because they *needed* it to defend

26. Merrill D. Peterson, *Alien and Sedition Acts*, *in* 1 ENCYCLOPEDIA OF THE AMERICAN CONSTITUTION 43–44 (Leonard W. Levy et al. eds., 1986).

27. *See generally* THOMSON, *supra* note 24.

themselves. They were not political philosophers so much as practical politicians, activists hoping to advance their own cause. It is also unlikely that they would have behaved any more magnanimously toward their opponents had they themselves been in power. Indeed, when they gained power a few years later, they did not always respect the free speech rights of their opponents. Even Jefferson himself, when he became president, urged that his opponents be prosecuted under state sedition laws.[28]

III. CHALLENGING THE IDEA OF SEDITIOUS LIBEL

For the first time, as a result of the experience under the Sedition Act of 1798, the concept of seditious libel itself was challenged.[29] The truly radical idea that in a democracy the people must have the same right as the government to voice any opinion and express any thought without fear of prosecution was advanced. However harsh, however unjust, however "false," speech had to be legally protected because the power to prosecute any opinion was the power to prosecute all opinion. There could be no such thing as a verbal crime. This new idea advocated nothing less than an absolute right to freedom of political expression. The line between what should be legally protected and what could be criminally punished was no longer to be drawn between categories of speech, such as true or false, but between speech and overt acts.

Not only was this a radical *libertarian* idea at the time, it was also a radical *democratic* idea. It meant that the government could never tell a citizen what to think or to say, or punish him for his words. It implied an equality between citizens and their government: a king might insulate himself from criticism by his subjects, but in a democracy, the concept of seditious libel was a contradiction because *citizens are not subjects*; their relationship to the government is, or ought to be, a legally egalitarian one. Unlike in a monarchy, where political power was permanently vested in a single family, political power in a democracy was fluid. It was intended to pass from party to party, as the people saw fit. Furthermore, how were the people to decide, if not by being exposed to the full flow of competing ideas, opinions, and even to competing views of the facts? If the party in power was allowed to skew a debate by punishing its critics and controlling which views became available to the public, could it not then manipulate public opinion and entrench its own political power?

---

28. *See generally* LEVY, *supra* note 12.

29. Sedition Act of 1798, Ch. 74, 1 Stat. 596 (expired in 1801).

Thus, the idea that democracy itself required absolute freedom of political expression grew. As a practical matter, since this was not possible without also protecting false and malicious speech, all political speech would have to be protected from government restriction. Jefferson said that error could be tolerated, so long as truth was left free to combat it,[30] and, he might have added, so long as government was not permitted to decide which was which. Therefore, what began as an idea rooted in the narrow self-interest of the Republican minority grew into a general theory of free expression that today broadly protects all Americans.

However, this idea did not grow quickly, at least not as enforceable constitutional law. The Sedition Act of 1798 was never challenged in the United States Supreme Court because the political turmoil it helped to create resulted in Thomas Jefferson being elected president, replacing John Adams. The Sedition Act was repealed and those convicted under it were pardoned by President Jefferson before any of the cases reached the Supreme Court.[31] As a result, state sedition laws stayed on the books and were mainly used to prosecute antislavery opinions in the South and labor activists in the late nineteenth and early twentieth centuries. Then, in 1917, in the midst of substantial dissent over the propriety of America's entrance into World War I, the first federal sedition law since the Sedition Act of 1798 was passed.[32] Once again, it became a federal crime to print, speak, write, or publish any words that heaped contempt or scorn upon the government.[33] Over 2,000 prosecutions were brought and more than a thousand convictions obtained, almost all of them for expressing criticism of the war.[34] One man was sentenced to prison for reading the Declaration of Independence in public;[35] a minister was sentenced to fifteen years for saying that the war was unchristian.[36] Additionally, a newspaper editor was convicted for questioning the constitutionality of the draft.[37]

As late as the early 1920s, more than 130 years after the First Amendment was ratified and 120 years after Jefferson and his colleagues

30. Speech by Thomas Jefferson (Jun. 13, 1779), *in* WILLIAM O. DOUGLAS, AN ALMANAC OF LIBERTY 362 (1954).

31. *Id.*

32. *See generally* WILLIAM O. DOUGLAS, AN ALMANAC OF LIBERTY 124, 193 (1954). *See also* Paul L. Murphy, *Espionage Act*, *in* 2 ENCYCLOPEDIA OF THE CONSTITUTION 653 (Leonard W. Levy et al. eds., 1986).

33. *See generally* DOUGLAS, *supra* note 32; Murphy, *supra* note 32.

34. *Id.*

35. *Id.*

36. *Id.*

37. *Id.*

realized what was wrong with the Sedition Act of 1798, the Supreme Court had still never struck down any such law or overturned any prosecution on First Amendment grounds. It would take many more years, well into the 1960s, before the First Amendment rights most Americans today take for granted would finally be enforceable in the courts.

What does all of this have to do with the Internet and with protecting free speech in cyberspace? First, it is clear that the invention of a radical new medium, the printing press, though it eventually allowed free speech and democracy to flourish, at first provoked laws designed to control speech and which gave the government broad powers to suppress and punish disfavored speech. Second, once the rules of restriction were set into place they became reified and legitimate, so that even advocates of free speech accepted limitations that few Americans, and no current Supreme Court Justice, would accept today. Third, the impact of these early restrictions were incredibly enduring, having a substantial impact for centuries, and a residual impact extending into our own lifetime.

Therefore, it is critically important to the future of free speech on the Internet that the rules of freedom, not censorship, govern from the outset. Once established, early rules are likely to determine for many years whether free speech prevails in what is likely to become the major medium of American democracy, or whether the new medium instead becomes the occasion to restore speech restrictions we no longer tolerate in print media.[38]

IV. THE INVENTION OF THE TELEPHONE AND HOW IT AFFECTED THE LAW OF PRIVACY

The invention of the telephone in the late nineteenth century, and its intersection with the traditional paradigm of the constitutional law of

38. Although it is beyond the scope of this article to examine the intermediate case of broadcast media , i.e., radio and television, it is worth pointing out that today Americans live with greater restrictions on radio and television than are constitutionally permissible in print media because of the early rules established at the emergence of radio. These early restrictions were rooted in the notion of the scarcity of broadcast airwaves and the subsequent need to regulate access to and control of such limited channels of communication. Although cable television and the likely merging of computer technology and the Internet with television has altered the original reality of scarcity and may alter it more in the years to come, the laws regulating television and radio have been slow to shed their original restrictions. Although this is a complex issue not possible to address fully here, it does illustrate the basic theme of this article, which is that early rules endure and that the early rules governing speech on the Internet will likely determine the degree to which Americans enjoy free speech in cyberspace for years to come.

privacy, also had, and continues to have, a profound transformational effect on rights the Fourth Amendment was designed to protect.

It is often, though mistakenly, claimed that no right to privacy can be found in the Constitution, and it is true that the word "privacy" does not appear anywhere in the Bill of Rights. But, there can be little doubt that maintaining privacy was a fundamental concern of early Americans or that the Fourth Amendment was explicitly designed to protect it.

Before the American Revolution, British soldiers and customs agents entered homes and offices at will and searched any person or place they wished. It is doubtless that the victims of those intrusions came to quickly value the right to privacy, and to believe that liberty could not be sustained unless the government was prevented from engaging in such intrusions at its discretion. Indeed, no less a witness to the cause of the trouble between England and its American colonies than Samuel Adams said that he regarded the unrest over general searches "as the Commencement of the Controversy, between Great Britain and America."[39]

After the Revolution, there was a strong public demand to prohibit general searches and to establish constitutional protection for "[t]he right of the people to be secure in their persons, houses, papers, and effects."[40] The Fourth Amendment represented a fundamental repudiation of traditional English law and created a presumptive right to privacy against government intrusion.[41] The right to privacy was protected by creating a legal barrier to physical intrusion. Security was established by the physical walls of one's home or place of business and the Fourth Amendment prohibited general searches of such private premises. What conversations took place there, and what papers and effects were stored there, would safely remain private except under the narrow, limited circumstances permitted by the Fourth Amendment. Privacy would be protected by the Fourth Amendment's limitation against physical trespass.

The invention of the telephone eroded this premise. Before the telephone, private conversations could take place only if the participants were physically contiguous. Additionally, conversations within the four walls of one's home or place of business were private because the government had no effective way to listen in. However, the telephone changed all that. With this invention two people could have a conversation while each stayed in his own home. The wire through which such

39. LEVY, *supra* note 12, at 227–28.

40. U.S. CONST. amend. IV.

41. This right was at first applied only against the federal government, a problem that would require 170 years to fully resolve. *See* Mapp v. Ohio, 367 U.S. 643 (1961).

conversations would pass, was initially thought to be opaque and impenetrable, like an envelope that no one could open. Thus, it was not believed to be necessary to construct special legal safeguards against listening in on telephone conversations to parallel those that protected the privacy of sealed paper letters. It was clear though that no one had anticipated wiretapping.

The first constitutional issue involving the telephone surfaced during the days of alcohol prohibition.[42] During the days of alcohol prohibition, Roy Olmstead, a suspected bootlegger whom the government wished to search, was the subject of a government wiretapping operation.[43] Utilizing this brand-new technique, the government placed taps in the basement of the building where his office was located and on wires in the streets near his home.[44] No physical trespass that breached the walls of his office or home took place; none was necessary.

Olmstead was convicted entirely on the basis of evidence from those wiretaps. In his appeal to the Supreme Court of the United States, Olmstead argued *inter alia* that the taps constituted a search conducted in violation of the Fourth Amendment, in that no warrant was issued and no probable cause existed, and so the evidence that had been admitted into evidence against him should have been excluded.[45] In a narrow but fateful 5 to 4 decision, the Court rejected Olmstead's arguments and upheld the federal government's power to wiretap without limit, and without any Fourth Amendment restrictions on the grounds that no actual physical intrusion of the premises had taken place and that physical intrusion of the premises was what the Fourth Amendment restricted.[46]

Justice Louis D. Brandeis dissented.[47] He said that the Fourth Amendment was designed to protect privacy and that the Fourth Amendment's restrictions on physical trespass were merely instrumental, not primary.[48] Brandeis warned against allowing the "progress of science [to furnish] the Government with means of espionage."[49] He said that such electronic methods would become more sophisticated and ubiquitous and

42. Olmstead v. United States, 277 U.S. 438, 442 (1928).
43. *Id.* at 455–56.
44. *Id.* at 456–57.
45. *See generally id.*
46. *Id.* at 469.
47. *Olmstead*, 277 U.S. at 471 (Brandeis, J., dissenting).
48. *Id.* at 474.
49. *Id.*

would render Fourth Amendment rights meaningless unless the Court ruled that they were not immune from Fourth Amendment restrictions.[50]

Brandeis not only argued that the Fourth Amendment should apply to wiretapping, he thought that if it did, it must bar wiretapping instead of merely restricting it.[51] He felt that no wiretap warrant could be limited, as the Fourth Amendment required, to describing particularly the conversations to be overheard, seized, and recorded.[52] Wiretaps, he said, indiscriminately picked up *every* conversation over the wires that were tapped, not only every conversation of the target, many or most of which would be personal and not germane to the investigation, but also every conversation of anyone else who lived in the house, as well as anyone else who phoned in.[53] Wiretaps, Brandeis argued, could not be precise, as the Fourth Amendment required, but were instead like vacuum cleaners, sweeping up everything.[54] In this respect, he concluded, wiretaps constituted the kind of general search prohibited by the Fourth Amendment.[55] Referring to colonial history, he said that the old British "general warrants are but puny instruments of tyranny and oppression when compared with wiretapping."[56]

But Brandeis did not prevail. By the margin of one vote, the Supreme Court failed to meet the challenge of adapting the Fourth Amendment's protection to emerging new technology.[57] If the Court had focused on the *right* the Fourth Amendment was designed to protect, and not upon the *instrumentality* of that right—the limitation upon physical trespass—electronic communication might have enjoyed the same privacy protections as paper mail. But by protecting the four walls of the home, when the private conversation no longer took place there, the Court allowed such conversation to be prey to government intrusions. This early decision was enduringly consequential because, just as the early laws governing the printing press restricted free speech for centuries, the *Olmstead* decision restricted privacy for decades and in some essential respects restricts it still.[58]

---

50. *Id.*
51. *Id.* at 438.
52. *Olmstead*, 277 U.S. at 438.
53. *Id.* at 476.
54. *Id.* (Brandeis, J., dissenting).
55. *Id.* at 479.
56. *Id.* at 476.
57. *Olmstead*, 277 U.S. at 476 (Brandeis, J., dissenting).
58. *See generally* Katz v. United States, 389 U.S. 347 (1967).

For forty years the Court's decision in *Olmstead* totally exempted wiretapping and other forms of electronic spying from any constitutional restrictions. Then in 1967, in a similar case involving gambling, the Court overruled *Olmstead* by an 8-1 margin, and recognized that the Fourth Amendment applied to wiretapping and electronic surveillance.[59]

Even then, Brandeis was only partially vindicated. The Court, in *Katz v. United States*,[60] did rule that warrants were required before wiretaps could be authorized, and that warrants could be issued only if there was evidence sufficient to satisfy the Fourth Amendment's requirement of probable cause.[61] However, Brandeis' view, that wiretapping was necessarily a general search because it inevitably recorded many innocent conversations and should therefore be entirely prohibited by the Fourth Amendment, was rejected by *Katz*.[62]

To a substantial extent, the failure of the *Katz* Court to take the second part of Brandeis' dissent into serious consideration can be said to have been a result of the reification over time of *Olmstead*. By the time *Katz* was decided, wiretapping and electronic surveillance (as the result of *Olmstead*) had been institutionalized in America for forty years. In fact, it was part of the landscape at both the federal and state level, and had become too habitual to stop. Just as even the avant-garde of free speech advocates in the eighteenth century could not see their way clear to challenge the government's prerogative to enforce substantive limits on dissent and criticism but were instead content to challenge the doctrine of prior restraint, leaving postpublication speech vulnerable, so even the avant-garde of privacy advocates in 1967 could not see their way clear to challenge *Katz* but instead celebrated it, content to have the warrant requirement now apply to wiretapping and electronic surveillance but remaining oblivious to what a nearly empty victory that turned out to be.

Following the *Katz* decision in 1967, Congress passed the *Omnibus Crime Control and Safe Streets Act of 1968*.[63] This new law authorized law enforcement officials to conduct wiretaps and other electronic surveillance under court ordered wiretaps.[64] It required that records be kept to show how many taps were authorized, how many conversations and people were

59. Katz v. United States, 389 U.S. 347 (1967).

60. *Id.*

61. *Id.*

62. *Id.*

63. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 236 (codified as amended at 18 U.S.C. § 2518 (1994)).

64. 18 U.S.C. § 2518 (1994).

overheard, how many interceptions led to arrests and convictions, and for which crimes.[65]

From the beginning, these statistics showed how right Brandeis had been when he dissented in *Olmstead* and how *Katz* had overruled *Olmstead* only formally, while leaving the underlying intrusion intact. For example, only a few years after the 1968 law was passed, government reports showed that wiretaps were indeed a vacuum cleaner, sweeping many innocent people and conversations into its net. Every incriminating conversation captured produced huge violations of the privacy rights of the innocent for only meager returns in criminal convictions.[66]

> * In 1968, when there was no federal eavesdropping, state officials listened in on 66,716 conversations.[67]
>
> * In 1969, when both federal and state officials eavesdropped, 173,711 conversations were overheard.[68]
>
> * In 1970, the amount of eavesdropping doubled to 381,865 conversations.[69]
>
> * In 1971, at least 498,325 conversations were overheard, a jump of 30 per cent [sic] over 1970.[70]

What were the results of all this expanded surveillance?

> * In 1968, out of 66,716 overheard conversations, *no* convictions were reported.[71]
>
> * In 1969, out of 173,711 conversations, 294 convictions [were obtained].[72]
>
> * In 1970, out of 381,865 conversations, 538 convictions resulted.[73]

---

65. *Id.* § 2519.

66. Ira Glasser & Herman Schwartz, *Your Phone is a Party Line*, HARPER'S MAG., Oct. 1972, at 108.

67. *Id.* at 108.

68. *Id.*

69. *Id.*

70. *Id.*

71. Glasser & Schwartz, *supra* note 66, at 108.

72. *Id.* at 111.

> * In 1971, out of at least 498,325 conversations, 322 convictions [were obtained].[74]

In the first four years after the 1968 bill was passed, 1.1 million conversations were overheard, 93,080 people were spied upon, 6131 people were arrested and a total of 1154 were reported convicted—barely more than one percent.[75] Moreover, it is not clear, because the government reports do not say, how many of those convictions depended upon wiretapping evidence.

In 1970 and 1971, there was not a single federal tap involving either a homicide or kidnapping. On the state level, from 1968 to 1971, only three taps involved kidnapping and only a few involved homicide.[76] The overwhelming bulk of court ordered wiretaps were for gambling and drugs.[77] "In 1971, gambling alone accounted for [ninety] per cent of federal tapping," drugs, six percent, and all other offenses combined, four percent.[78] Most of the gambling taps were on bookies and their customers.[79]

In subsequent years, these results did not significantly vary. For example, according to statistics released by the Administrative Office of the United States Courts and the Department of Justice, of the 2.2 million conversations captured by the government in 1996, 1.7 million—more than three-quarters—were deemed not incriminating by prosecutors.[80] Moreover, most of those conversations that were incriminating were in cases involving drugs or gambling, much of it petty.[81] In 1996, *none* of the wiretap orders were issued for investigations involving arson, explosives, or weapons, and in thirty years the vast majority of wiretaps and other forms of electronic surveillance have occurred in vice crimes, like gambling and drug offenses.[82] Over the past eleven years, eighty three percent have occurred in such cases,

---

73. *Id.*
74. *Id.*
75. *Id.*
76. Glasser & Schwartz, *supra* note 66, at 111.
77. *Id.*
78. *Id.*
79. *Id.*
80. American Civil Liberties Union, *Big Brother on the Wires: Wiretapping in the Digital Age* <http://www.aclu.org/issues/cyber/wiretap_brother.html> [hereinafter *Big Brother*] (as of Feb. 5, 1999 this site had changed).
81. *Big Brother, supra* note 80.
82. *Id.*

and hardly ever in crimes involving bombings, arson, firearms, homicide, assault, rape, robbery, or burglary.[83]

If as many homes had been intrusively entered, and three-quarters of the targets had turned out to be innocent, while most of the others where incriminating evidence was found were in cases involving gambling and drugs and not those involving crimes of violence, most modern Americans, and certainly most of the early Americans, would have felt violated. It was precisely the purpose of the Fourth Amendment to target searches narrowly so that when warrants were issued the privacy rights of innocent people would be minimized. Wiretapping stands that purpose on its head, as Brandeis predicted at its dawn.

Here again, as in the area of free speech, the lesson is that when new technologies develop the law must develop along with them to maintain a proper balance between individual rights and government power. Just as the invention of the printing press ushered in new laws that upset the balance and weakened the right of free speech for centuries, so did the invention of the telephone when the law failed to keep pace at the outset, permanently altering the balance of power between the government and the individual, and ushering in an era of declining privacy rights that has not yet ended. It is therefore critically important to the future of privacy at the dawn of the era of cyberspace that the rules be drawn now in a way that insulates privacy from government intrusions, because those early rules, once established, are likely to determine for many years whether the value of privacy prevails in a digitalized world of electronic communication.

V. THE COMMUNICATIONS DECENCY ACT AND ITS PROGENY

The Communications Decency Act of 1996, ("Act"),[84] presented the United States Supreme Court with its first opportunity to decide, in a fundamental way, how the First Amendment would apply to cyberspace. A detailed analysis of the Act and of the Supreme Court decision that struck it down is beyond the scope and purpose of this article.[85] What is significant, and what this article proposes to examine, is the way in which this Act presented both Congress and the President on the one hand, and the Supreme

83. *See generally* BRUCE SCHNEIER & DAVID BANISAR, ELECTRONIC PRIVACY PAPERS: DOCUMENTS ON THE BATTLE FOR PRIVACY IN THE AGE OF SURVEILLANCE, Ch.10, at 463 (1997). *See also Big Brother*, *supra* note 80.

84. Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133 (codified as amended at 47 U.S.C. § 223 (Supp. II 1997)).

85. Reno v. ACLU, 521 U.S. 844 (1997).

Court on the other, with an early opportunity to adapt the traditional paradigms of First Amendment case law to the startling new technology of the Internet. Because these early decisions are likely to endure and to set the terms of the intersection of the law with rapidly emerging new technology, they are especially interesting and, in all probability, disproportionately significant.

As the Internet developed, it began to come to the attention of a wide variety of interest groups and eventually of governments worldwide, many of whom were alarmed by the decentralized, uncontrolled, and unlimited nature of the communication taking place.[86] In a reprise of the alarm like that which caused Parliament to impose comprehensive censorship schemes on the then-new printing press four centuries ago, Congress moved swiftly to pass the Act, thereby making it a crime to "publish" or communicate by means of a telecommunications device or through the use of an "interactive computer service" certain content described in some sections of the law as "indecent" and in other sections as "patently offensive."[87]

The statute also barred communications that were obscene, but this part of the statute was less legally interesting because it essentially sought to transfer to the Internet legal standards that already were embedded in longstanding constitutional case law as it applied to print media, films, etc.[88] On the other hand, in extending criminal bans to material that was "indecent"[89] or "patently offensive" even if not legally obscene, the statute sought to criminalize speech and expression that it clearly could not constitutionally prohibit in books, magazines or films. This squarely raised

86. The Internet grew from its experimental origins in 1969 as a project linking computers and computer networks owned by the military, defense contractors, and university laboratories conducting military research to include without limit networks and computers throughout the world. *Id.* at 849–50.

87. *Id.* at 849.

88. Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133 (codified as amended at 47 U.S.C.§ 223 (Supp. II 1997)). Even with respect to obscenity law, however, the new technology presented challenging new problems for the law to resolve. A key element of current obscenity laws, as governed by *Miller v. California*, rests on the notion of "community standards." 413 U.S. 15 (1973). Thus, what is legally obscene in Tupelo, Mississippi may be different than what is obscene in San Francisco, California. But how can the idea of local community standards be maintained in the world of cyberspace, where something can be posted in San Francisco, or, for that matter, in Finland, and downloaded by someone in Tupelo?

89. The statute banned "indecent" communications without anywhere defining the term. Communication Decency Act of 1996, Pub. L. No. 104-04, 110 Stat. 133 (codified as amended at U.S.C. § 223 (Supp. II 1997)).

the question of whether the Internet could be governed by different substantive constitutional standards than those that governed print and film.

Those who believed that the Internet would in the not too distant future become the principal means of mass communication well understood the significance of the answer to this question. Advocates of free speech sought to have the standards currently applying to books and newspapers applied to the Internet. Those who were frustrated by their inability to restrict sexual content in print media saw in the Internet a rare occasion to embed more restrictive constitutional standards in a new and emerging means of communication. Central to the outcome of this constitutional contest was the struggle over the appropriate metaphor. What exactly was the Internet? Was it what one judge called "a never-ending worldwide conversation" which, as "the most participatory form of mass speech yet developed" deserved "the highest protection from governmental intrusion"?[90] Was it like broadcast television because communications were received visually on a screen? Or was it more like an electronic version of a book or newspaper? Because the law had long permitted government restrictions of content on radio and television that it had not permitted in books, magazines, or newspapers, this factual question, this struggle over the correct analogy, was critical to the outcome of the litigation that challenged the Act. Thus, at the trial, expert witnesses were exhaustively presented; the contest over what the applicable legal standards should be was preceded by, and was based upon, a contest over the facts. In the end, both the trial court and the Supreme Court rejected the analogy of broadcast television and applied the traditional First Amendment standards governing print media to Internet communications, thus striking down as unconstitutional those provisions of the Act that expanded the law's restrictive reach.[91]

The Court also ruled that the state's interest in protecting minors from certain sexually explicit content could not, in a situation where minor audiences could not effectively be segregated from adult audiences, justify restricting access by adults to constitutionally protected content if less restrictive alternatives were available.[92] The Court stated that the availability of user based blocking software by parents is one such alternative.[93] This led to a rapid and explosive growth of such software[94] as

90. ACLU v. Reno, 929 F. Supp. 824, 883 (E.D. Pa. 1996).
91. Reno v. ACLU, 521 U.S. 844 (1997).
92. *Id.* at 855–56.
93. ACLU v. Reno, 929 F. Supp. at 883.

parents exercised their prerogative to guide their children's Internet access in much the same way that they might wish to guide their access to books, magazines, and films. The use of blocking software has also become an instrument of government. An increasing number of city and county library boards began to require public libraries to install such blocking software, over the objection of the American Library Association and library users. The struggle over such government-mandated blocking software has now become the biggest free speech controversy in cyberspace since the legal challenge to the Act. Lawsuits challenging the required use of blocking software by local libraries are now pending, and a battle looms in Congress, where a bill has been introduced that would require all public libraries and schools to use blocking software in order to qualify for a federal funding program designed to promote and assist universal Internet access.[95]

To some extent, the controversy over the constitutionality of government blocking schemes once again turns on the facts. Blocking software that was able to narrowly limit its reach to unprotected speech, e.g., obscenity, might be at least presumptively constitutional. But such narrowly targeted software is now quite impossible and is likely to remain so. Some blocking software relies on key words and phrases, such as "xxx" (meant to block triple x-rated pornography) "which blocks out Superbowl XXX sites; "breast," which blocks websites and discussion groups about breast cancer; and the consecutive letters 's,' 'e' and 'x,' which block sites containing the words 'sexton' and [even] "Mars exploration," among many others".[96] Any blocking software that relies on key words and phrases will inevitably be overbroad. Ironically, at the same time that it blocks benign sites, such software often lets targeted material through. According to a recent survey, one software vendor's own test showed that its software blocked fifty-seven sites containing nothing objectionable while failing to block a number of pornographic sites.[97] The definitional problems inherent in this filtering approach are thus both under- and over-inclusive.[98]

Blocking software also relies on the judgment of individuals hired by software vendors who browse the Internet for sites to block according to the manufacturer's criteria, which may include such imprecise categories as

---

94. Sales were estimated at $14 million in 1997 and are projected to increase to $75 million over the next three years. American Civil Liberties Union, *Censorship in a Box* <http://aclu.org/issues/cyber/ box.html/> [hereinafter *Censorship in a Box*].

95. Internet School Filtering Act, S. 1619, 105th Cong. (1998).

96. *Censorship in a Box*, *supra* note 94.

97. *Id.*

98. *Id.*

"hate speech," "criminal activity," "sexually explicit speech," "adult speech," "violent speech," "religious speech," and even "sports." Using such criteria, the vendor maintains lists of unacceptable sites, and makes judgments that update such lists. These methods are inevitably subjective and vague, often surprising their supporters with unanticipated results. The American Family Association ("AFA") a strong advocate of blocking software, was angered to learn that their own site had been blocked by software that blocked discussion of homosexuality because of the AFA's *opposition* to homosexuality![99]

Thus, the censorship offered by such software is often like poison gas: it seems like a good idea when aimed at a target you oppose, but the wind has a way of shifting. Ultimately, the First Amendment considerations are no different from traditional problems of vagueness and overbreadth that are inherent in any language attempting to define categories of impermissible speech. The Internet has therefore become the locus for the replay of traditional struggles between censorship and First Amendment rights. Between 1995 and 1998, twenty-five states considered or passed one form or another of Internet censorship laws. This year alone at least seven states plus Congress are considering bills that require libraries and/or schools to use blocking software.[100] The struggle over the application of First Amendment principles to this new medium is unlikely to abate anytime soon.[101]

VI. BIG BROTHER IN THE WIRES: DIGITAL TELEPHONY, ENCRYPTION, AND COMPUTER PRIVACY

The values of privacy articulated by Justice Brandeis in *Olmstead* are now at stake as never before in our history.[102] Electronic communications, including telephone conversations, fax messages, e-mail, fund transfers, commercial transactions, trade secrets, and health records are all floating in the air, waiting to be scooped up by governments, private groups, and individuals. The black strips on the backs of our credit, ATM, and identification cards, the electronic wands being distributed by gasoline companies to make purchases easier, the E-Z passes for paying tolls

99. *Id.*

100. *Id.*

101. Currently, this author's research reveals that federal district courts in New York, Georgia, New Mexico and Virginia have found Internet censorship laws unconstitutional on First Amendment or other constitutional grounds, and that other cases are pending.

102. *See* Olmstead v. United States, 277 U.S. 438 (1928).

effortlessly and electronically, and the imminent arrival of a new generation of compact digital PCS phones that also function as wireless computers, e-mailers, pagers, and data transmitters compound the problem.[103] Americans are on the edge of a degree of vulnerability to both governmental and private sector spying and surveillance that was unimaginable only a decade ago. One can scarcely contemplate how the new potential for total surveillance of the most personal details of our private lives would have stunned those who valued privacy, like Justice Brandeis in 1928, or like the majority of citizens who supported the Fourth Amendment in the late 18th century, fueled by their rage against the intrusions of British soldiers.[104]

Strong encryption of all such data is the modern electronic equivalent of the door that blocked the King of England from entering the tenements of British subjects.[105] It is also the equivalent of the opaque envelope that provides a constitutionally mandated shield to paper communications. Without an individual, constitutionally-based right to strong encryption, there will be no way to prevent private communications from being swept up. The King of England, and all other governments and private sector entities, will be empowered to enter any data door at will, to join any conversation, to monitor and record any communication. Without an enforceable right to strong encryption, the general search our ancestors so justifiably hated will be resurrected to a degree unimagined by those who value personal privacy.

Most countries in the world today do not have legal controls on the use of encryption, which may be used, manufactured, and sold without restriction.[106] "There are a small number of countries where strong domestic [legal] controls on the use of cryptography are in place."[107] These include countries that are not noted for their traditional respect for individual rights:

---

103. *Big Brother, supra* note 80.

104. "Thus our houses and even our bed chambers, are exposed to be ransacked, our boxes chests [and] trunks broke open ravaged and plundered by wretches, whom no prudent man would venture to employ even as menial servants." BERNARD SCHWARTZ, 1 ROOTS OF THE BILL OF RIGHTS 206 (Leon Friedman ed., 1980) (citing THE RIGHTS OF THE COLONIES (1772)).

105. "The poorest man may, in his cottage, bid defiance to all the forces of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England may not enter." William Pitt, *Opposing a Bill to Authorize General Searches, Speech Before Parliament* (1763) *in* LEONARD W. LEVY, ORIGINAL INTENT AND THE FRAMERS' CONSTITUTION 222 (1998).

106. Wayne Madsen, *Cryptography and Liberty: An International Survey of Encryption Policy* <http://www.gilc.org>.

107. *Id.*

Belarus, China, Israel, Pakistan, Russia and Singapore.[108] A few other countries are currently considering the adoption of new controls, limiting the right to encryption and therefore threatening the right to privacy; among these is the United States.

The debate in the United States regarding whether encryption will be limited, though of immense consequence to citizens, has yet to engage the general public.[109] On one side of this debate are law enforcement and national security agencies, i.e., the Department of Justice, the Federal Bureau of Investigations ("FBI"), the National Security Council, the Drug Enforcement Administration, and many state and local law enforcement agencies—those who typically and traditionally seek wider powers to penetrate zones of personal privacy. On the other side are privacy and civil liberties advocates, those who typically and traditionally seek to limit the powers of government by legally enforceable rights, joined in this instance by leading cryptographers and computer scientists, and also by much of the communications industry, whose products depend upon their ability to guarantee security of information to users.

Conceptually, modern techniques of encryption are not difficult to understand. Computers generally transmit data in digital form, that is, data translated into strings of ones and zeroes.[110] Encryption programs scramble those numbers using a mathematical formula that can be reconverted only with the proper "key."[111] "Thus, only an authorized person with the secret key can convert a scrambled message back to its original state or readable form."[112] If one sends an encrypted e-mail message to a friend or colleague and the sender and the recipients are the only ones with the key code, that message is effectively inaccessible to any third party who may intercept it. Encryption thus provides, in effect, an electronic opaque envelope.

But just as paper envelopes may be steamed open, so encrypted messages may be decoded. The strength of encryption generally depends on the length of the mathematical formula or key that is required to decrypt the data.[113] This key is measured by its "bit length."[114] Generally, the longer the

108. *Id.*

109. KENNETH W. DAM, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY xvi–xvii (1996). Professor Dam chaired the National Research Council's Committee to Study National Cryptography Policy, and has warned that a "policy crisis" is upon the nation. *Id.* at xv.

110. AMERICAN CIVIL LIBERTIES UNION, *Wiretapping in the Digital Age* (as of Feb. 5, 1999, this site had changed).

111. *Id.*

112. *Id.*

113. *Id.*

114. *Big Brother*, *supra* note 80.

bit length, the more difficult it is to crack the code.[115] Thus, a 56-bit length key, which is fairly weak, could quickly be decoded by a hacker or thief, whereas a 128-bit length key is exponentially more difficult and could be impossible to decode within a lifetime.[116] Although the powerful series of computers available to governments and some private-sector corporations could shorten the time needed to unlock longer keys, the use of still longer keys is an effective barrier to most unauthorized interceptions. Thus, the right to manufacture, sell, and use such strong encryption becomes the key to protecting the right to privacy of data and communications. Thus, it is no surprise that the government has sought to pass laws banning strong encryption or, in the alternative, demanding access to the keys that unlock it. The arena in which this struggle is taking place is Congress.

In 1993, the Clinton administration announced its so-called "Clipper Chip"[117] proposal, which would have, in effect, "required every encryption user (that is, every individual or business using a digital telephone system, fax machine, [e-mail,] the Internet, etc.)" to provide their decryption keys to the government, "giving it access to both stored data and real time communications."[118] That would have been the equivalent of a law requiring all home and office builders to embed microphones or cameras in the walls of homes and offices.[119] As soon as this proposal became known, opposition was fierce; a Time/CNN poll conducted soon after the proposal was made found that eighty percent of the public was opposed, and the Clinton administration withdrew the proposal.[120]

Shortly thereafter, the Clinton administration proposed "Clipper II,"[121] which required anyone using encryption to leave the key with a government approved "escrow agent," a third party that would give the government the key upon the issuance of a warrant by a court, but without the knowledge of the user.[122] That, too, provoked substantial public opposition and was

115. *Id.*
116. *Id.*
117. DAM, *supra* note 109.
118. *Id.*
119. *Big Brother*, *supra* note 80.
120. *Id.*
121. *Id.*
122. *Id.*

withdrawn. Later, a subsequent version, dubbed "Clipper III,"[123] was proposed but did not differ significantly.[124]

In addition to these proposals, none of which has thus far been enacted, the FBI has pushed for sweeping expansions of its wiretapping powers in numerous bills. Some have passed, including the so-called anti-terrorism legislation passed in 1996.[125] Perhaps the best example of the current policy conflict is the Communications Assistance for Law Enforcement Act ("CALEA") passed in 1994.[126] This law requires telecommunications carriers and manufacturers to build special wiretap capabilities into its new digital telephones. Among the FBI's demands was one that would require every cell phone to be able to transmit information about the location of users to police, in effect turning the phone into a homing device. In response to objections by opponents, CALEA, which was scheduled to be implemented by October of 1998, has now been delayed by the Federal Communications Commission.

In contrast, in 1996, a bill was introduced to protect the right to strong encryption.[127] The FBI has strongly opposed this bill. FBI Director Louis Freeh has justified his position by claiming that the FBI only seeks to maintain the balance between privacy and government power that the Fourth Amendment set 200 years ago.[128] According to Freeh, the bills to protect the right to strong encryption:

> will dramatically shift that balance for the first time in 200 years. What it means is that with probable cause, the judge signs the order for me to access the conversations, but I cannot understand it . . . because no one has . . . required that there be some key safely placed somewhere, only attainable with a court order. That

123. *Id.*

124. *See generally The Rights of Key Recovery, Key Escrow and Trusted Third-Party Encryption*, a report by eleven prominent cryptographers and computer scientists (1997) (source on file with author).

125. Anti-terrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1214 (codified as amended in scattered sections of 28 U.S.C., 18 U.S.C., and 42 U.S.C.).

126. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as assembled in sections of 18 U.S.C. & 47 U.S.C.).

127. The Security and Freedom Through Encryption Act, H.R. 3011, 105th Cong. (1997). *See also* The Encrypted Communications Privacy Act, S. 376, 105th Cong. (1997).

128. FBI Director Louis Freeh's testimony on June 26, 1997 at a closed briefing session of the House International Relations Committee on the subject of encryption. *See generally*, <http://www.netltynews.com> (as of Feb. 5, 1999, this site had changed). The transcript of this session was obtained by Netlynews, an online news service, pursuant to the Freedom of Information Act. *Id.*

> dramatically changes the balance of the Fourth Amendment to the detriment of public safety.[129]

Freeh poses the public policy question precisely, but he is wrong on several counts. First, the claim that the right to strong encryption would alter the balance struck by the Fourth Amendment 200 years ago ignores the fact that the balance was fatally altered in 1928 when the *Olmstead* decision permitted government wiretaps upon the fictional claim that the Fourth Amendment did not protect the privacy of citizens but rather only barred the government from physical trespass of their homes and offices.[130] It was Justice Brandeis who, at that time, argued for maintaining the balance struck by the Fourth Amendment in 1791.[131] If Freeh truly advocated the original balance he would, like Brandeis, have to oppose wiretapping, which, of course, he does not. The balance Freeh wishes to maintain is not the original balance of 1791 but the dramatically altered balance of 1928, an alteration that expanded the government's surveillance power at the expense of the individual privacy of millions of innocent citizens not even suspected of any crime.[132]

Second, because the expansion of electronic communication now and into the future dwarfs the communication that used to take place along telephone wires, and already includes or will soon include the wireless digital transmission of virtually all data and communications, commercial, political and personal, the vacuum cleaner sweep of government wiretapping powers will, if not curtailed, be infinitely greater than anything seen before with respect to traditional wiretapping. In the pre-digital era, communications over telephone wires was limited and data transmissions minimal. Moreover, the labor-intensive cost of wiretaps, conducted by human agents listening to and transcribing conversations, tended to limit its use. Even so, between 1985 and 1995, more than twelve million conversations were tapped and all but a relative few were completely innocent.[133] In 1995 alone, two million *innocent* conversations were intercepted.[134] Digital surveillance, on the other hand, will mean massive

129. *Id.* (this testimony was delivered on June 26, 1997 at a closed briefing session of the House International Relations Committee on the subject of encryption. A declassified and redacted transcript of this session was obtained by Netlynews, an online service, pursuant to the Freedom of Information Act).

130. Olmstead v. United States, 277 U.S. 438 (1928).

131. *Id.* at 471–85 (Brandeis, J., dissenting).

132. *See supra* Part III.

133. *See generally* Glasser & Schwartz, *supra* note 66.

134. *Id.*

scanning of many more conversations and data transmissions, by computers coded to look for digital representations of key words like "drugs," "bombs," "civil rights," etc. Like software filters, these scans will necessarily capture more than they intend, rendering puny by comparison the overbroad sweep of traditional wiretapping.

The dragnet quality of electronic eavesdropping, which Brandeis first noted in *Olmstead*, will turn out to be a prophecy of exponential proportions. Allowing the government to rummage through all the data transmissions sent or received by any warranted target will necessarily capture immense amounts of unrelated data and a substantial number of innocent people. This has, according to the government's own statistics, been precisely the result of wiretapping since 1968,[135] and it will necessarily be substantially more so in the world of ubiquitous electronic communications we are rapidly entering.

Third, the claim frequently made by Freeh and his superiors that a right to strong encryption will "devastate our ability to fight crime and prevent terrorism"[136] is demonstrably disproved by the government's own statistical evidence.[137] The plain facts are that even traditional wiretapping has been used overwhelmingly in cases involving drugs and gambling,[138] only negligibly in cases involving bombing, arson, or firearms[139] and hardly at all in cases of homicide, rape, assault, robbery, or burglary. The record of wiretapping over the past three decades is a record that justifies Justice Brandeis' concern. It is fair to say that electronic surveillance is of some value to law enforcement. However, it is hyperbole to claim that it is an "indispensable" tool to prevent serious crimes of violence, crimes for which, in fact, it is rarely used. Government surveillance through wiretapping has, as Brandeis predicted, always picked up far more innocent conversations than incriminating ones. In this light, the prospect of permitting the government to widen its surveillance as the amount of electronic communication and data transmission widens promises nothing but an immolation of the right to personal privacy. Without an individual right to strong encryption, the right to personal privacy for which our ancestors fought a revolution will be in great peril.

---

135. *See supra* Section II.

136. Letter from Janet Reno, Attorney General, to Congress, (July 18, 1997) (on file with author) [hereinafter Letter from Janet Reno].

137. *See supra* Section III.

138. Letter from Janet Reno, *supra* note 136 (83% over the past 11 years).

139. Letter from Janet Reno, *supra* note 136 (2% over the past 11 years).

VII. ADAPTING OLD VALUES TO NEW MEANS OF COMMUNICATION

The values of free speech and privacy have been fundamental to what has distinguished America from the rest of the world. Our nation began not only by inventing a new form of government but also by declaring a new purpose for government. That new purpose was the protection of individual rights. No government had ever before been created with that as one of its primary purposes.

The early Americans fundamentally redefined the proper legal relationships between the individual and the government. They did not endorse anarchy nor abandon the need for government to protect the safety of the community. But they meant to draw the lines of government power in such a way as to legally and constitutionally prevent the government from interfering with individual rights. "Over himself, over his own body and mind, the individual is sovereign," John Stuart Mill would write more than a half-century later.[140] Once, the concept of "sovereignty" was meant only to include the unlimited powers of the king; later, it described the powers of nations and governments. In America, it came to describe the rights of individuals. "To secure these rights," wrote Thomas Jefferson in the Declaration of Independence, "governments are instituted among men."[141]

Primary among those rights were the rights to free speech and to personal privacy, what Brandeis called "the right to be let alone."[142] It is our task to protect those traditional rights under the conditions and circumstances of a new world never imagined by our founders.

140. JOHN STUART MILL, ON LIBERTY AND OTHER ESSAYS 14 (John Gray ed., 1991).

141. THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776).

142. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

Trotter Hardy
Professor - College of William & Mary

Professor I. Trotter Hardy was graduated Order of the Coif from Duke University, where he served as Articles Editor for the *Duke Law Journal.* After graduation, he clerked for the Honorable John D. Butzner, Jr., on the Federal Court of Appeals for the Fourth Judicial Circuit. Following that clerkship, he joined the law faculty at the College of William & Mary, where he teaches intellectual property, torts, and legal issues of the Internet.

Professor Hardy is the author of articles on the design of computer command languages, international data flows, health law, law and computers, copyright law, and the law of the Internet.

His current research interests include copyright and new technologies; governmental regulation of the Internet; electronic journals; and personal computer networking and electronic communication in legal education. He is the moderator of an Internet discussion list called "CYBERIA" dealing with the law and policy of computer networks.

He also founded and is the current editor of the *Journal of Online Law*, an electronic journal dealing with computer communications legal issues.

Professor Hardy was on leave during the summer and fall of 1996 when he worked for Copyright Register Marybeth Peters as Scholar in Residence and Technical Advisor. While at the Copyright Office, he was in charge of project "Looking Forward," an effort to predict the evolution of the Internet and the possible consequences for copyright law.

Copyright and "New-Use" Technologies

I. Trotter Hardy

TABLE OF CONTENTS

Today's copyright concerns often center on the new digital technologies, especially the Internet and its friendly interface, the World Wide Web ("the Internet"). Even though the Internet is relatively new and poses new challenges for copyright law, "technology," as such, and a constant change in technology are certainly not new. To the contrary, inventors, innovators, and entrepreneurs have been changing the landscape of American life ever since the country's founding. Not surprisingly, copyright law—having existed for almost as long[1]—has repeatedly had to accommodate new technologies over the two centuries of its existence.

Congress has repeatedly stated its intention to make the Copyright Act[2] flexible enough to adapt to new technologies over time without requiring repeated amendments. Much of the talk in hearings for the 1909 Copyright

1. The first Copyright Act was enacted in 1790. *See generally* Act of May 31, 1790, ch. 15, 1 Stat. 124.

2. Copyright Act of 1976, Pub. L. No. 94-553, 90 Stat. 2541 (codified as amended at 17 U.S.C. §§ 101–118 (1976)).

Act[3] focused on this goal, and even more of the hearings for the 1976 Copyright Act[4] focused on it as well. Yet, since its effective date of 1978, the most recent major copyright revision has been amended at least twenty-eight times,[5] more than once every year on average, and as of this writing, has just undergone some very significant amendments relating to new technology.[6]

Something is out of kilter here. On the one hand, Congress has tried to make the Copyright Act flexible enough to survive technological change; on the other hand, every new technological change seems to lead to further amendments to the Copyright Act. Why is it so hard to make the Copyright Act flexible, particularly when Congress has declared that doing so is a signal value?

Two reasons account for the failure of Congress to craft an enduring Copyright Act, though only the second of these is addressed here. The first reason is essentially a matter of politics: a Copyright Act written to survive significant technological change would necessarily be very broadly and generally worded. But broad and general language neither clearly requires the imposition of liability nor clearly renders a potential defendant immune

---

3. Copyright Act of 1909, Pub. L. No. 60-349, 35 Stat. 1075 (codified as amended at 17 U.S.C. §§ 101–914 (1994)).

4. Copyright Act of 1976, Pub. L. No. 94-553, 90 Stat. 2541 (codified at 17 U.S.C. § 101 (1994)).

5. *See Preface to the Copyright Act* <http://lcweb.loc.gov/copyright/title17/preface.html> (the U.S. Copyright Office World Wide Web site). *See also* H.R. REP. No. 104-554, at 6 (1996) (stating "[s]ince 1976, Congress regularly has had to address new issues, especially those raised by new technologies or new methods of exploitation. Each session of Congress has produced at least one major amendment to the Copyright Act").

6. *See* The Digital Millennium Copyright Act ["DMCA"], H.R. 2281, 105th Cong. (1998), signed into law by President William Clinton in the fall of 1998 as Pub. L. No. 105-304, 112 Stat. 2860 (1998) (to be codified at 17 U.S.C. 101). The Copyright Office summarized the law as follows:

> The DMCA is divided into five titles:
> Title I . . . implements the WIPO treaties.
> Title II . . . creates limitations on the liability of online service providers for copyright infringement when engaging in certain types of activities.
> Title III . . . creates an exemption for making a copy of a computer program by activating a computer for purposes of maintenance or repair.
> Title IV contains six **miscellaneous provisions**, relating to the functions of the Copyright Office, distance education, the exceptions in the Copyright Act for libraries and for making ephemeral recordings, "webcasting" of sound recordings on the Internet, and the applicability of collective bargaining agreement obligations in the case of transfers of rights in motion pictures.
> Title V . . . creates a new form of protection for the design of vessel hulls.

U.S. Copyright Office, *The Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary* <http://lcweb.loc.gov/copyright/legislation/dmca.pdf> (emphasis in original).

from liability in a given context. Political interest groups therefore seek legislative provisions not only favorable to their interests, but provisions that clearly and unambiguously favor those interests. To accomplish the latter goal, those groups press Congress for narrow and specific statutory wording, wording that cannot be expected to survive much technological change. Conversely, the more general the language of an act—and hence the more likely that it is to survive a long while—the greater the incentive of interest groups to oppose it.[7]

The second reason for Congress's failure is a matter of policy, however, and is within the scope of this article: Congress has perceived and hence tried to solve only one-fourth of the problem of copyright and new technologies—the other three-fourths have never been adequately addressed, let alone solved. The one-fourth of the problem that has been reasonably well solved is the issue of copyright's subject matter. At times, new technologies create new media for recording the creative expression of authors, such as photography, motion pictures, laser-etched disks, and so on. This kind of technological evolution has often in the past given rise to the corresponding issue of whether those new media should be protected by copyright. By and large, the 1976 Copyright Act avoided the questions—and the need for repeated Copyright Act amendments—for future media by defining copyright's subject matter to be "works of authorship", something that is by definition an abstraction and independent of any particular medium of fixation. The three-fourths of the problem that has not been addressed makes up an enormous portion of the issues that surround new technology and copyright. Those issues, first proposed in a report written for the United States Copyright Office,[8] include the following.

---

7. For more on the politics of copyright revision, see Professor Litman's excellent analysis in Jessica Litman, *Copyright Legislation and Technological Change*, 68 OR. L. REV. 275, 277 (1989), written 10 years ago and more timely than ever:

> Throughout its history, copyright law has had difficulty accommodating technological change. Although the substance of copyright legislation in this century has evolved from meetings among industry representatives whose avowed purpose was to draft legislation that provided for the future, the resulting statutes have done so poorly. The language of copyright statutes has been phrased in fact-specific language that has grown obsolete.... Whatever copyright statute has been on the books has been routinely, and justifiably, criticized as outmoded. In this article, I suggest that the nature of the legislative process we have relied on for copyright revision is largely to blame for those laws' deficiencies.

Id. at 277 (citations omitted).

8. I. TROTTER HARDY, PROJECT LOOKING FORWARD: SKETCHING THE FUTURE OF COPYRIGHT IN A NETWORKED WORLD-FINAL REPORT 238 (1998) [hereinafter HARDY I] (source on file with author).

New subject matter. First, new technologies sometimes allow new forms of creative expression that are independent of any particular medium.[9] These new forms of expression raise questions of copyright's subject matter that are not solved by the current Copyright Act's separation of copyrightable "works" from particular media because the issue has nothing to do with the particular medium of fixation.[10] For example, the hierarchy of menu commands that is part of many computer programs is a form of expression that can be fixed in a variety of media.[11] Yet, in early 1996 the Supreme Court split four-to-four on the question of the copyrightability of menu command hierarchies.[12]

Decentralized infringement. Second, technologies like photocopying and computers sometimes allow widespread noncommercial uses of copyrighted works in ways that would clearly be infringing if done on a large scale for commercial purposes.[13] When they are done on a small scale, typically for noncommercial purposes, the issue arises whether these "decentralized infringements" should be legitimized as a fair use, considered to be infringements even if they are largely undetectable by copyright owners, declared to be non-infringing by Congress, or dealt with in some other way.[14]

New uses. Finally, new technologies often create new ways of using existing copyrighted works.[15] Radio in the early 1920s raised the issue whether music broadcasts infringed composers' performance rights, for example.[16] Cable television in the 1960s similarly raised the issue whether retransmitting copyrighted television programs or movies infringed the copyright owner's performance rights.[17]

This article will summarize these three issues of copyright and new technologies, and then concentrate on the last, the "new-use" issue from the perspective of copyright as an incentive to creative efforts. The article will demonstrate that much of the affected parties' and Congress's understanding of the new-use issue is faulty because it is heavily biased toward the then present state of the technology in issue. A proper analysis of the issue requires thinking ahead. Some new-use technologies will eventually grow to supplant "old use" technologies and should therefore be required to pay

9. *Id.* at 238.

10. *Id.*

11. *See* Lotus Dev. Corp. v. Borland Int'l, Inc., 49 F.3d 807 (1st Cir. 1995), *aff'd by an equally divided court* 516 U.S. 233 (1996).

12. *Id. See also infra* text accompanying notes 31–34.

13. HARDY I, *supra* note 8, at 240.

14. *Id.* at 241.

15. *Id.* at 240.

16. *Id.*

17. *Id.*

royalties to preserve authors' incentives at their previous level. Other new-use technologies may not grow to any particular importance, and consequently need not be required to pay royalties to preserve authors' incentives. Unfortunately, neither courts nor Congress can predict the future growth of a new technology in order to make this determination. The issue is then how to make a determination about a new-use technology's royalty obligation that depends on foretelling the future when the future cannot be foretold.

This article proposes one answer to this apparently intractable problem by analyzing the issue in terms of the statistician's "Type I" and "Type II" errors. Essentially, this approach asks: "How bad could it be" if the copyright decision-maker (court or Congress) guesses wrongly about a new technology's future? If one type of wrong guess is likely to be less harmful than other types, than absent information to the contrary, that is the guess about the future that the decision-maker ought to make. Finally, this same analysis implies that in the absence of other information to the contrary, when courts or Congress face the issue of whether a copyright royalty obligation applies to a new-use technology, they should find that it does apply.

I. NEW MEDIA AS SUBJECT MATTER

The way we view copyright's "subject matter" has evolved over the two centuries of copyright law's existence. In 1790, the first copyright statute included "maps, charts, and books" within its protection.[18] Although not expressly confined to tangible media—a court could always interpret "map" or "chart" or "book" in a broad and nonliteral way were the occasion to do so arise[19]—this statute nonetheless seemed to focus on tangible media as the object of copyright's protection.

Over the succeeding two hundred years, the focus of copyright's subject became more varied, including some subject matters defined or phrased as tangible objects, and others suggesting more abstract types of works. In an 1853 case, for example, the Supreme Court said clearly that copyright was an abstract right, thoroughly separate from any tangible embodiment:

> But from the consideration we have given to the case, we are satisfied that the property acquired by the sale in the engraved plate, and the copy-right of the map secured to the author under the

18. Act of May 31, 1790, ch. 15, 1 Stat. 124.

19. *See* Holmes v. Hurst, 174 U.S. 82, 89 (1899) (stating "the word 'book' as used in the statute is not to be understood in its technical sense of a bound volume, but any species of publication which the author selects to embody his literary product").

> act of Congress, are altogether different and independent of each other, and have no necessary connection. The copy-right is an exclusive right to the multiplication of the copies, for the benefit of the author or his assigns, disconnected from the plate, or any other physical existence. It is an incorporeal right to print and publish the map, or, as said by Lord Mansfield in Millar *v.* Taylor (4 Burr. 2396) "a property in notion, and has no corporeal tangible substance."[20]

Yet when Congress added photography to copyright's subject matter in 1865, it used words that focused on the medium itself: protection applied to "photographic prints."[21] On the other hand, musical compositions were for years registered by the Copyright Office in the category of "books,"[22] a practice that implied a recognition of "music" as a more abstract entity, capable of being fixed in a variety of forms. Congress only expressly added "musical compositions" to copyright's subject matter in 1831.[23] "Dramatic works" were added to the statute as a category in 1856,[24] another phrase suggesting a focus on the abstract work regardless of its medium of fixation. Yet, this abstract sounding focus was not so broad that it was thought expressly to include "operatic compositions," a subject matter only added to the statute in 1894.[25] Moreover, in 1908 the Supreme Court declared without reservation that copyright's subject matter consisted only of tangible media:

---

20. Stephens v. Cady, 55 U.S. 528, 530 (1852).

21. Act of March 3, 1865, ch. 126, 13 Stat. 540. Interestingly, the issue of photography as a new type of copyrightable subject matter was litigated a year *later*, in 1866, on facts that had arisen before passage of the 1865 Act. *See* Wood v. Abbott, 30 F. Cas. 424, 425 (S.D.N.Y. 1866) (No. 17,938). The court concluded that photographs did not fit within any of the existing categories of protectible subject matter and hence were not copyrightable. *Id.*

22. *See Revision of Copyright Laws: Hearings Before the Joint Comm. on Patents*, 60th Cong. (1908) (statement of Albert H. Walker), *reprinted in* E. FULTON BRYLAWSKI & ABE GOLDMAN, LEGISLATIVE HISTORY OF THE 1909 COPYRIGHT ACT (1976) [hereinafter BRYLAWSKI] Part K at 46 (noting that English courts had protected sheet music as "books" since 1777, and that American courts had always followed that precedent).

23. Act of Feb. 3, 1831, ch. 16, 4 Stat. 436.

24. *See* Act of Aug. 18, 1956, ch. 169, 11 Stat. 138 (1856).

25. *See* H.R. 6835, 53d Cong. § 4966 (1894). Apparently Congress omitted "operatic compositions" from the category of "dramatic works" from simple oversight. *See* JAMES W. COVERT, AMENDING THE COPYRIGHT LAW, H.R. REP. NO. 1191, at 1 (stating "the omission to include protective provisions for operatic compositions in the law sought to be amended [in 1856] was, doubtless, the result of oversight").

> The statute has not provided for the protection of the intellectual conception apart from the thing produced, however meritorious such conception may be, but has provided for the making and filing of a tangible thing, against the publication and duplication of which it is the purpose of the statute to protect . . . .[26]

Finally, in the 1976 Copyright Act, Congress formally adopted the "meritorious conception" that was rejected sixty-eight years earlier by the Supreme Court, namely that copyright's subject matter is abstract "works of authorship" regardless of the medium of a work's fixation.[27] By "generalizing" copyright's subject matter that way, Congress hoped to permit copyright law more gracefully to accommodate technological change—to apply to new media of fixation, whether "now known or later developed."[28] Relative to other issues of copyright and new technology, Congress has succeeded reasonably well in that endeavor.[29] To the author's knowledge, no issues of copyright subject matter have arisen over "video

---

26. White-Smith Music Publ'g Co. v. Apollo Co., 209 U.S. 1, 17 (1908). Apparently *contra* is the ten-years' earlier opinion in *Holmes v. Hurst*, 174 U.S. 82, 89 (1899) (stating: "It is the intellectual production of the author which the copyright protects and not the particular form which such production ultimately takes" though the Court may have intended "form" to refer to some form of paper publication).

27. 17 U.S.C. § 102(a) (1994).

28. *Id.*

29. *But see* HARDY I, *supra* note 8, at 246 stating:

> Even under the 1976 Act, subject matter issues that spring from new media of fixation have not always been resolved as cleanly and simply as the statutory language suggests. Notably in the 1980's, it took a major, highly contested case, *Apple Computer v. Franklin Computer Corporation*, [714 F.2d 1240 (3rd Cir. 1983)], to determine that although computer programs written on paper or on a disk were the subject matter of copyright, so were computer programs fixed in read-only memory. One would have thought that the "medium-neutral" design of the 1976 Act would have made this an easy answer to reach.

Id. See also Matthew Bender & Co., v. West Pub. Co., 158 F.3d 693 (2d Cir. 1998), where despite its claims to the contrary, the Second Circuit returned to putting copyright's subject matter focus on the particular medium of fixation instead of the abstract work that results from "selection and arrangement." *Id.* at 703.

> But the relevant statutory wording refers to material objects in which "a work" readable by technology "is fixed," not to another work or works that can be created, unbidden, by using technology to alter the fixed embedding of the work, by rearrangement or otherwise. The natural reading of the statute is that the arrangement of the work is the one that can be perceived by a machine without an uninvited manipulation of the data.

Id.

cassettes," "audio CDs," "CD-ROMs," "laser disks," "DVD disks," "DIVX videos," three-dimensional photographs in holograms, or over any other modern developments in media technology. That such disputes have not arisen is a tribute to Congress's wisdom in abstracting copyright's subject matter away from the medium of fixation.

II. NEW WORKS AS SUBJECT MATTER

Tributes pretty much have to stop with Congress's handling of the medium-of-fixation issue, alas. Less successfully treated in the Copyright Act is the issue of whether new types of *works* should be treated as copyrightable subject matter.[30] The First Circuit's decision in *Lotus Development Corp. v. Borland International, Inc.*,[31] a case involving the question of extending protection to the menu command structure of a computer program, illustrates the problem.[32]

Lotus had developed the widely used computer spreadsheet program known as "Lotus 1-2-3."

> Lotus 1-2-3 is a spreadsheet program that enables users to perform accounting functions electronically on a computer. Users manipulate and control the program via a series of menu commands, such as "Copy," "Print," and "Quit." Users choose commands either by highlighting them on the screen or by typing their first letter. In all, Lotus 1-2-3 has 469 commands arranged into more than 50 menus and submenus.[33]

Competing software company Borland developed its own spreadsheet program, "Quattro," which could make use of the same menu commands—indeed, Quattro had implemented "'a *virtually identical* copy of the entire 1-2-3 menu tree'" though with a different on-screen appearance.[34] Lotus sued Borland, arguing that Borland had infringed Lotus's copyright in hierarchy

30. 17 U.S.C. § 103 (1994).

31. 49 F.3d 807 (1st Cir. 1995), *affirmed by an equally divided Court*, 516 U.S. 233 (1996).

32. *Id.* at 810.

33. *Id.* at 809.

34. *Id.* at 810 (quoting Lotus Dev. Corp. v. Borland Int'l, Inc., 831 F. Supp. 202, 212 (D. Mass. 1993) (emphasis in original)).

of menu commands. The First Circuit concluded that the menu hierarchy was a "method of operation"—something not copyrightable by definition.[35]

A more useful way of looking at the case, though, is to see it as an issue of new subject matter. Personal computers and the software sold for them constituted a new technology that led to a new type of authorial effort, the creation of a computer program's "menu hierarchy." The fundamental issue in the case was whether copyright law should recognize that type of authorship as an appropriate type of subject matter for protection.[36]

The issue arises because of ambiguity in the statutory language. Section 102 defines two things: things that copyright protects as subject matter, *and* things that copyright does not protect as subject matter.[37] These twin provisions, intended no doubt to serve as an abundance of caution in ensuring that the Copyright Act withholds copyright protection from ideas, facts, and the like, actually open up a middle ground of uncertainty. If there were but a single definition of what is copyright's subject matter, courts would focus on new types of works with but a single question: Does this type of work fall within that definition of subject matter? With two definitions, one inclusive and one exclusive, the *Lotus* court understandably felt obliged to ask three questions: Does the new type of work fall within the definition of copyrightable subject matter? Does the work also fall within the definition of non-copyrightable subject matter? And finally, what is the effect of a work's falling within *both* categories of expressly protected and expressly unprotected subject matter? *Lotus* apparently concluded that a computer program's menu hierarchy did in fact fall within both categories:

> [W]hile original expression is necessary for copyright protection [that is, falls within copyright's *included* subject matter], we do not think that it is alone sufficient. Courts must still inquire whether original expression falls within one of the categories foreclosed from copyright protection by [section] 102(b) [that is, falls within copyright's *excluded* subject matter], such as being a "method of operation."[38]

35. *Id.* at 815. The Copyright Act, section 102(b), notes: "'In no case does copyright protection for an original work of authorship extend to any . . . method of operation.'" *Lotus*, 49 F.3d at 815 (quoting 17 U.S.C. § 102(b) (1994)).

36. *Id.* at 813.

37. 17 U.S.C. § 102(a), (b) (1994).

38. *Lotus*, 49 F.3d at 818.

The court implicitly found that falling within both categories meant that the new type of work, menu command hierarchies, was not eligible for copyright's protection.[39]

III. THE "DECENTRALIZED INFRINGEMENT" ISSUE

One major problem in copyright enforcement today is the fact that many modern communications technologies exhibit very low reproduction costs. Low costs mean that small firms, or even individuals, can make low volume copies without coming to the attention of copyright holders. When copying costs are high, infringement tends to be "centralized" because economies of scale dictate that a business enterprise—a store, a copy center—provide the copying equipment. Business enterprises are few enough in number, and visible enough through advertising, that copyright holders can locate and bargain with them.

Before the invention of mimeography and xerography, for example, the copying of books or other printed matter would have to be undertaken by hand, a severe practical limit, or by a printer. Printing required typesetting, an expensive and time-consuming process. Because of the high initial overhead of printing, copying would not be worth undertaking unless a fairly large run of books was envisioned. A large run of books by a commercial printer would constitute a "centralized" infringement and would be relatively visible to a copyright holder:

> The unauthorized publication of a copyrighted book may ordinarily be adequately punished through civil proceedings and under the provisions of existing law. The offender in such case is ordinarily a person of fixed habitat, and has a press and the implements of his business. The ordinary processes of the courts may readily be served upon him, and he may be compelled to respond in damages for his wrongdoing.[40]

When technology reduces the costs of copying, the phenomenon of "decentralized infringement" results: individuals can duplicate copyrighted works in a way that is not easily detected by the copyright holder. Today, high quality copies can be made in low volume by ubiquitous photocopy machines. Such copying takes no overhead, little time, and even the machinery is priced low enough for home use, where the copying is essentially invisible to a copyright holder.

---

39. *Id.* at 819.

40. *See* COVERT, *supra* note 25, at 2.

The photocopier and the video recorder are obvious examples of dramatically lowered costs over printing presses and television studios for the making of copies of paper documents and television programs. Similarly, the falling cost of home audio taping equipment in the form of tape cassettes during the 1960s and 1970s allowed individuals to make high quality copies of sound recordings that previously could only be made with expensive reel-to-reel tape machines in professional sound studios. Making such copies was lawful under federal law until 1972.[41]

Decentralized infringement is not confined to physical reproduction of copyrighted materials. The distribution right[42] can also be affected by technology. Today's computer networks and electronic mail provide an easy way to distribute information to literally millions of Internet users. In spite of recent amendments to the Copyright Act[43] to deal with digitized music, new developments in digital audio and the Internet raise the familiar issue of decentralized infringement once again.

Music has been available in a digital format in the form of audio "compact disks" or "CDs" for many years.[44] For some years, it was far from easy for home users to make a copy of the digital audio data resident on a CD. CD players and computers with CD-ROM drives converted the digital format to analog immediately upon use. Consequently, home audio taping equipment that was used to copy a CD produced an analog tape recording, one that would decline in quality with multiple generations of subsequent copies. Both home audio equipment and computer CD-ROM drives today, however, are commonly able to copy the digital format directly, without conversion to analog form. Readily available software can read the digital files from a CD and copy them onto a personal computer's hard disk.[45]

---

41. *See* Pub. L. No. 92-140, 85 Stat. 391 (1971) (codified as amended at 17 U.S.C. § 1(f)); *see also* Goldstein v. California, 412 U. S. 546 (1973) (discussing California's state-law approach to the problem).

42. The Copyright Act confers several defined rights on copyright owners: reproduction, distribution, public performance, public display, and the preparation of derivative works. *See* 17 U.S.C. § 106 (1994).

43. *See* 17 U.S.C. §§ 1001–1010 (1994) (codifying the Audio Home Recording Act of 1992, Pub. L. No. 102-563, 106 Stat. 4327 (1992)).

44. The Philips Corporation introduced the first CD system in 1979. Sony followed with improvements to the Philips design in 1983. RUSSELL SANJEK & DAVID SANJEK, AMERICAN POPULAR MUSIC BUSINESS IN THE 20TH CENTURY 241 (1991).

45. *See, e.g.*, *Audiograbber* <http://www.audiograbber.com-us.net> (stating:

> Audiograbber is a beautiful piece of software that grabs digital audio from cd's. It copies the audio digitally - not through the soundcard - which enables you to make perfect copies of the originals. It can even perform a test to see that the copies really are perfect. Audiograbber can also automatically normalize the music, delete silence from the start and/or end of tracks . . . .).

However, the resulting computer files are quite large.[46] For most home users, wide-spread distribution of such files electronically over the Internet would be impracticably time consuming.[47] However, a compression technology called "MP3" has arisen that reduces the sizes of such files by a factor of ten, with little or no noticeable loss in music quality.[48] This combination of copying and compression technologies has resulted in the rapid spread of nonprofessional Internet sites that feature digitized music for downloading, typically copied from CDs.[49] This development now threatens to decentralize the formerly highly centralized system for the distribution of recorded music.[50]

---

46. CD music occupies roughly 10 million bytes of computer storage per minute of playing time. A three minute song, for example, copied to one's computer hard disk would take up roughly 30 megabytes of disk storage.

47. A typical home-to-Internet connection today operates at 28.8 kilobits per second. At that speed, downloading or uploading a three-minute song, about 30 million bytes (which at eight bits per byte equals 240 million bits), would take roughly 140 minutes or over two hours (that is 240 million bits divided by 28,800 bits per second which equals 8333 seconds). Obviously, anything that speeded up such downloading—other things being equal—would increase the amount of such downloading. Faster modems or other access technologies would do it; smaller file sizes would also do it. It happens that the latter came first.

48. *See* Jason Chervokas, *Music Industry Fears Digital Music Pirates* <http://search.nytimes.com/books/search/bin/fastweb?getdoc+cyber-lib+cyberlib+20671+3+wAAA+mp3> (source on file with author). *See also* David Thom, *MPEG Audio FAQ Version* 9 <http://www.tnt.uni-hannover.de/project/mpeg/audio/faq/> (source on file with author).

49. The Recording Industry Association of America ("RIAA") refers to these non-professional sites as "Music Archive Sites," defining them as sites that

> host an inventory of full-length sound recordings for Internet users to download and play and in some cases upload as well. Music Archive Sites may contain hundreds of full-length sound recordings that, for the most part, are of near CD quality. The sites often actively encourage -- sometimes require -- users to upload additional full-length sound recordings to the site in exchange for being able to download.

RIAA, *Record Industry Protects Copyrighted Sound Recordings On the Internet: Enforcement Campaign Expands, Music Archive Sites Targeted* <http://www.riaa.com/antipir/releases/maslit.htm>.

50. *See, e.g.*, Jon Pareles, *With A Click, A New Era of Music Dawns*, N.Y. TIMES, Nov. 15, 1998, at AR-1 (stating: "Digital distribution is likely to revolutionize the economics of the music business. Some advantages of large recording companies, like their *centralized manufacturing and distribution* and their domination of retail display space, vanish if the Internet becomes the main outlet for music") (emphasis added). These new music distribution technologies have strong analogies to jukeboxes, radio, retail CD stores, and so on, suggesting that courts will find that distributing music in this particular form will be infringing. Yet, on October 26, 1998, federal district court Judge Audrey B. Collins denied the recording industry's motion for a preliminary injunction against the sale of a device for storing music in

These previous illustrations feature changing costs making certain uses of works so cheap that they are no longer centralized and hence no longer "visible" or readily controllable by copyright owners. This phenomenon can arise even without sophisticated technology. Early in the twentieth century, witnesses in copyright hearings testified about the difficulty of finding and suing professional play pirates, who operated in this fashion:

> An expert stenographer secretes himself somewhere in the theater and he takes down word for word everything that is spoken in the play .... After he has gotten all that, he takes down the makeup of the actor, everything he wears, the arrangement of the face, the beard or wig if he wears one, the costume. Then he comes down to the scenery; the properties that are used. All of the play is stolen in that way.
>
> ....
>
> How does he get that stolen manuscript on the market? He does not put out a sign "Play broker," "Play agent," as a reputable vendor of manuscripts would do. But he has in front a beer saloon. You enter ostensibly to get a glass of beer. What you go for is to get the play. By knocking on a door or by some other means you obtain access to the manuscript room, and you get a copy for $5.[51]

Another witness similarly complained about the difficulty of enforcing play copyrights when unauthorized "performances are usually given at points remote from the location or headquarters of the dramatic author or producer, and by irresponsible persons, who jump their companies nightly from town to town."[52] Obviously, modern digital technology had nothing to do with these nineteenth to early twentieth century play performances. Rather, the

---

its MP3 format. *See* Recording Indus. Ass'n of Am., Inc. v. Diamond Multimedia Sys., 29 F. Supp. 2d 624 (C.D. Cal. 1998). Actions against private individuals for "decentralized infringement" in the form of copying MP3 files may be foreclosed by the digital audio amendments to the Copyright Act made in 1992. *See* 17 U.S.C. § 1008 (1994).

51. *Revision of Copyright Laws: Hearings Before the Joint Comm. on Patents*, 60th Cong. (1908), *reprinted in* BRYLAWSKI, *supra* note 22, Part K at 22 (statement of Harry P. Mawson, representing the American Dramatists' Club).

52. *Id.* at 24 (statement of Ligon Johnson, representing the National Association of Theatrical Managers). Similarly, the 19th century saw the wide-spread unauthorized reproduction and distribution of sheet music. Canadian music publishers maintained secret publishing houses in the United States. They sent thousands of salesmen out with trunks of sheet music, keeping only a few sheets at recognized warehouses so that they could not be caught with much on hand. *See* H.R. REP. NO. 1289-55.

problem grew from the fact that the performances, at least when done with limited props and scenery, had only small economies of scale and could therefore be produced with a small number of people and equipment and hence in a decentralized fashion.

Courts and Congress have responded to the decentralized infringement issue in a variety of ways. At times, stiff penalties have been imposed on the conduct;[53] at times, Congress has adopted a compulsory license with prescribed payments;[54] at times, private parties have worked out their own arrangements in the form of "guidelines;"[55] at times, Congress has rendered the activities immune, perhaps in exchange for a tax/royalty on some related activity;[56] at times, one who facilitates decentralized infringement has been found liable for contributory infringement;[57] at times, a court has declared the activity to be a fair use.[58] And doubtless, at times, the activity in question continues, undetected, without litigation, and hence without any definitive resolution of the infringement question.

IV. THE NEW-USE ISSUE

All three problems so far discussed—new media of fixation, new types of works, and decentralized infringement—raise challenges for copyright law and merit thoughtful analysis. But the fourth problem is perhaps the most vexing of all: new technologies that create a new way of using existing copyrighted works. In short, these technologies raise the new-use question: Does the new-use of an existing copyrighted work infringe the author's rights? An abundance of illustrations has emerged from copyright cases over the last century or so.

For example, musical compositions as such were copyrightable after 1831, well before the advent of radio in the 1920s. When radio stations began playing musical compositions "on the air," however, litigation soon arose over whether such a playing constituted a "performance for profit" of

53. *See* Act of January 6, 1897, ch. 4, 29 Stat. 482 (amending 60 R.S. ch. 3) (imposing prison sentences for unauthorized play performances).

54. *See* 17 U.S.C. § 115(c) (compulsory license for the making of "cover records").

55. *See* Ad Hoc Committee on Copyright Law Revision, Authors League of America, and Association of American Publishers, Inc., Agreement on Guidelines for Classroom Copying in Not-For-Profit Educational Institutions with Respect to Books and Periodicals, *reprinted in* HOUSE REPORT ON COPYRIGHT ACT OF 1976, H.R. REP. NO. 94-1476, at 159–60, *reprinted in* 1976 U.S.C.C.A.N. at 5775–76 [hereinafter House Report].

56. *See* 17 U.S.C. §§ 1003, 1004 (1994) (tax on digital recording devices and media).

57. *See, e.g.*, Princeton Univ. Press v. Michigan Document Servs., Inc., 855 F. Supp. 905 (E.D. Mich. 1994), *rev'd*, 74 F.3d 1512 (6th Cir. 1996), *reh'g en banc and opinion vacated*, 74 F.3d 1528 (6th Cir. 1996), *aff'd* 99 F.3d 1381 (6th Cir. 1996).

58. *See, e.g.*, Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984).

the composition—and hence a copyright infringement under the 1909 Copyright Act.

The same question arose after the arrival of cable television in the 1960s. Cable television began as a means of strengthening the signal of distant broadcast stations, especially in the valleys of mountainous areas. These cable stations picked up broadcast signals from the airwaves and passed them along to cable subscribers without seeking permission from the broadcast stations or paying royalties. Again, litigation arose over whether such retransmission by cable constituted a "public performance for profit" within the scope of the copyright owner's rights.

A. *Phonograph Recording*

Composers of the 1900s era wanted to be able to collect royalties from phonograph and piano roll companies that hired orchestras to record their compositions. Most copyright scholars know that the Supreme Court rejected that desire in 1908, when the Court decided the *White-Smith Music Publishing. Co. v. Apollo Co.*[59] case. *White-Smith* held that the use of copyrighted music on piano rolls, a popular technology of the day,[60] did not infringe the composer's copyright rights.[61] Less well-known, perhaps, is that the Supreme Court rested its decision partly on that fact that a number of earlier lower court cases had declined to offer copyright protection to recorded sound; Congress, with presumed awareness of those decisions, had not acted to change that result.[62]

---

59. 209 U.S. 1 (1908).

60. *Id.* at 9.

> The record discloses that in the year 1902 from seventy to seventy-five thousand of such instruments were in use in the United States, and that from one million to one million and a half of such perforated musical rolls . . . were made in this country in that year.
>
> It is evident that the question involved in the use of such rolls is one of very considerable importance, involving large property interests, and closely touching the rights of composers and music publishers.

Id.

61. *Id.* at 18.

62. *Id.* at 12–14.

> [I]t must be admitted that the decisions, so far as brought to our attention in the full discussion had at the bar and upon the briefs, have been uniformly to the effect that these perforated rolls operated in connection with mechanical devices for the production of music are not within the copyright act.

White-Smith, 209 U.S. at 12.

> Since these cases were decided Congress has repeatedly had occasion to amend the copyright law. The English cases, the decision of the District

The real story was a bit more circular. True, the early cases of recorded music found no infringement. In 1888, a Massachusetts case, *Kennedy v. McTammany*,[63] found that the reproduction of music in the form of perforated paper rolls for "organette" hand organs[64] did not infringe composers' copyrights because it was not a "copy" of the composition for copyright purposes.[65] A similar case in 1901, *Stern v. Rosey*,[66] relied on *Kennedy* to conclude that a phonograph record was similarly not a copy of the musical composition it recorded.[67] Within just a few years of that decision, Congress began considering a major revision of the Copyright Act. By the time the first Congressional hearings began in June, 1906,[68] a bill had already been introduced that provided music composers the right to control the reproduction of their works in the form of recorded sounds:

> [T]he copyright secured by this Act shall include the sole and exclusive right . . .
>
> (g) To make, sell, distribute, or let for hire any device, contrivance, or appliance especially adapted in any manner whatsoever to reproduce to the ear the whole or any material part of any work published and copyrighted after this Act shall have gone into effect, or by means of any such device or appliance

---

> Court of Appeals, and Judge Colt's decision must have been well known to the members of Congress . . . the omission of Congress to specifically legislate concerning them might well be taken to be an acquiescence in the judicial construction given to the copyright laws.

Id. at 14.

63. 33 F. 584 (C.C.D. Mass. 1888).

64. For a brief history of organettes, see Peter Schmidt, *History of Organettes* <http://www.actionwebcreations.com/smr/history.htm>, where one learns that John McTammany—presumably the defendant in the case cited—was the inventor of the devices. *Id.* Schmidt himself is evidently a collector of antique organettes. *Id.*

65. *Kennedy*, 33 F. at 584.

66. 17 App. D.C. 562 (1901).

67. *Id.* at 565.

68. Three hearings took place: in June of 1906; again in December of that year; and finally, in March of 1908. *See Revision of Copyright Laws: Hearings Before the Joint Comm. on Patents*, 59th Cong. (1906), *reprinted in* BRYLAWSKI, *supra* note 22, Part H at 102; *Revision of Copyright Laws: Hearings Before the Joint Comm. on Patents*, 59th Cong. (1906), *reprinted in* BRYLAWSKI, *supra* note 22, Part J at 276; *Revision of Copyright Laws: Hearings Before the Joint Comm. on Patents*, 60th Cong. (1908), *reprinted in* BRYLAWSKI, *supra* note 22, Part K at 46.

> publicly to reproduce to the ear the whole or any material part of such work . . . .[69]

The bill proved controversial, with the "authors" (composers and publishers) favoring it, and "users" (piano roll and phonograph manufacturers) opposing it. In classic fashion, though, both sides to the debate focused on the effect of the new technology on the market for the old technology, without so much as a nod to the possibility that the new technology might itself become a major market one day. In the case of recorded sound, the old market was for the sale of sheet music to individuals and to orchestras and bands for live performances.[70] Accordingly, much testimony centered on sheet music sales: Whether a composer's right to control the making of recordings would help or hurt the composer's income from the sale of sheet music.[71] As it turned out, in a very few years several phonograph recording companies would earn phenomenal amounts of money

---

69. *Revision of Copyright Laws: Hearings Before the Joint Comm. on Patents*, 59th Cong. (1906), *reprinted in* BRYLAWSKI, *supra* note 22, Part H at v (1976).

70. KERRY SEGRAVE, PAYOLA IN THE MUSIC INDUSTRY: A HISTORY, 1880–1991 3 (1994). "In those days [the late 19th century], of course, it was the sale of sheet music that was the sole source of income for the [music publishing] companies . . . . Records would not become a major factor for several more decades." *Id.*

71. *See, e.g.*, BRYLAWSKI, *supra* note 22, Part H at 325 (statement of Paul H. Cromelin, representing the Columbia Phonograph Company). Mr. Cromelin stated that the operators of a penny arcade that featured coin operated player pianos:

> are being paid by certain music publishers for displaying ads of certain compositions over the automatic piano or piano player which is used to attract the public.
>
> It seems to us that this would amply demonstrate the fact that publishers and composers consider the piano player an advantageous medium to increase the sale of their compositions.

Id. at 325 (statement of Paul H. Cromelin, representing the Columbia Phonograph Company)

> Why does [one of several well known music publishers], who claim that we are stealing the product of the composers' brains, use . . . us and paying [sic] for 250 to 300 records of every song as soon as they publish it? For the purpose of selling the records? No—absolutely not—but to give them away to the owners of penny arcades in consideration of their putting them on their automatic graphophones, so that the public will become acquainted with the tune and buy the sheet music.

Id. at 326. "We claim, gentlemen, that there has been no more potent influence than the talking machine and the piano player and these various mechanical devices in bringing about an increase in sheet music sales of 163 percent in six years." *Id.* at 333.

from record sales;[72] however, this possibility was remote from the discussions.

In any event, Congress and various industry representatives continued to thrash the music issue throughout the hearings, initially without sign of any resolution. By the last round of hearings, in March of 1908, the Supreme Court had just a month earlier issued its decision in the *White-Smith* case.[73] As already noted, the Court—relying heavily on the fact that Congress itself had not amended the statute—concluded that under the statute as it then stood, composers had no right to control recordings of their works.[74]

The Court had deferred to Congress—which then deferred back to the Court.[75] Representative Currier observed that composer Victor Herbert, whose views doubtless represented a great many other composers, was "asking us to create for him an absolutely new property right, *which the Supreme Court says has absolutely no existence.*"[76] Representative Barchfeld added that "[y]ou are coming to Congress and asking for additional legislation to give you a right which the law does not now give you. *The Supreme Court has declared that you have no standing in court.*"[77]

The issue had become a mutual finger-pointing exercise, with the Supreme Court unwilling to create or recognize rights that Congress had not chosen to create or recognize, and the Congress apparently unwilling to create or recognize rights that the Supreme Court had not chosen to create or recognize. Whereas at an earlier point, a bill to grant rights to composers might have seemed unremarkable, after the Supreme Court's decision, such a bill seemed to fly in the face of established authority. With this posture, the hearings took on the quality of a stalemate.

---

72. Between 1902 and 1917, assets of the Victor Talking Machine Company, predecessor to the RCA Victor company, went from $2.7 million to $33.2 million, a twelve-fold increase. The company's founder, Eldridge Johnson, "had become a tycoon; and several of the men whose careers dated back to the founding of the company were millionaires, or well on their way." ROLAND GELLATT, THE FABULOUS PHONOGRAPH: FROM EDISON TO STEREO 151 (1965). And this was at a time, 1910, when *one* dollar "would buy a seven-course dinner at a first-class restaurant." *Id.* at 149. The British recording company, Gramaphone, saw its *net* profits rise from £79,348 in 1901 to £137,268 in 1902 and to £252,285 (over $1 million) in 1903. *Id.* at 122.

73. *See* White-Smith Music Publ'g Co. v. Apollo Co., 209 U.S. 1 (1908).

74. *Id.* at 14.

75. *Id.*

76. *Revision of Copyright Laws: Hearings Before the Joint Comm. on Patents*, 60th Cong. (1908), *reprinted in* BRYLAWSKI, *supra* note 22, Part K at 193 (comment of Representative Currier) (emphasis added).

77. *Id.* (comments of Representative Barchfeld) (emphasis added).

A stalemate leads Congress to compromise. In the final round of hearings, members and witnesses seized on the proposal to establish a "compulsory license" as a compromise between full copyright rights and none.[78] A compulsory license meant that composers would receive a non-negotiated, statutorily prescribed royalty when their compositions were recorded more than once.[79] Hearings participants finally struck an agreement on a compulsory license some time after the hearings closed. In short order, it became law.[80]

History now shows us that notwithstanding the vigorous discussion at the hearings about how recorded music would boost the sale of sheet music, the sheet music market soon withered under the dual onslaught of the phonograph and later the radio.[81] Today, music in the home almost

78. In addition to the Supreme Court's ruling in the *White-Smith* case, the compulsory license provision in the 1909 Copyright Act was also inspired by fears of a recording industry monopoly. A leading piano roll company of the day, the Æolian Company, had signed contracts with many music publishers that would have granted Æolian exclusive rights to the music for which copyright was held by the publishers. These contracts were conditioned upon either the Supreme Court or Congress declaring that recording music without permission was an infringement of the composers' rights. By the end of 1906, about 500 publishers had signed such contracts. A number of music publishers, in other words, had signed contracts that would be ineffective if copyright were found not to apply to sound recordings, but would automatically transfer copyright permissions to Æolian if copyright were found to apply. *See Revision of Copyright Laws: Hearings Before the Joint Comm. on Patents*, 59th Cong. (1906), *reprinted in* BRYLAWSKI, *supra* note 22, Part J at 277–80 (statement of Albert H. Walker).

79. Composers were not obliged to permit any recording of their compositions. However, having once voluntarily negotiated with a recording company to permit recording, composers were then subject to the compulsory license provision: other recording companies could record the same composition on payment of the statutorily prescribed fee whether the composer liked it or not.

80. Representative Currier introduced a bill that included the compulsory license provision on March 2, 1909. *See* H.R. 28192 § 1(e), *included in* H.R. REP. NO. 2222, 60th Cong. (1909), *reprinted in* BRYLAWSKI, *supra* note 22, Part S at 22–24 (1976). The bill specified a compulsory royalty of two cents per record for anyone to record compositions that had already been licensed by the composer for recording. The next day it passed in both the House and the Senate. *See* 43 CONG REC. 3768-69 (1909) (House version); 43 CONG REC. 3744 (1909) (Senate version). President Roosevelt signed it the following day, March 4. *See* 43 CONG REC. 3831-32 (1909).

81. A turning point of sorts was around 1921, when music publishing companies first began releasing compositions to phonograph recording companies before exhausting sheet music sales. *See* SANJEK & SANJEK *supra* note 44, at 20. By 1924, roughly seven to eight million phonographs were in use, compared with about five million pianos and less than a million player pianos. *Copyrights: Hearings on H.R. 6250 and H.R. 9137 Before the House Comm. on Patents*, 68th Cong. (1924) (statement of E.C. Mills). As one commentator noted about the wildly popular "Victrola" phonograph machine introduced in 1906, "[o]nce, a piano

invariably means radio or recorded music, the income from which easily dwarfs that of sheet music sales.[82] Congress, in short, was terribly wrong in its assessment of the role that recorded music would come to play in American life—and accordingly in its assessment of the relative significance of recorded music and sheet music for copyright law.

B. *Motion Pictures*

Invented toward the end of the 19th century,[83] motion pictures were confirmed as copyrightable subject matter by an appellate court in 1903.[84]

---

had graced the parlor of the middle-class home and gave it an air of refinement and culture. Now a fine Victrola and a collection of the exclusive Victor Red Seal records made the same statement." ANDRE MILLARD, AMERICA ON RECORD: A HISTORY OF RECORDED SOUND 131 (1995). Later, it was radio that nearly drove the phonograph recording business out of business. Sharply improved sound quality boosted sales of radio receivers in the "radio Christmas" season of 1924; in that same year, sales of phonograph record players from the Victor company dropped 60% , and those of Edison's company dropped more than 50%. *Id.* at 138. *See also* GELATT, *supra* note 72, at 265 (stating "by January 1933, the record business in America was practically extinct"). Jukeboxes were largely responsible for rescuing the recorded music industry: in 1936, over half of all records were produced for the jukebox market. MILLARD, *supra* at 169. In the ironic flip-flops that have characterized the commercialization of sound technology, radio broadcasting went into decline when television began to usurp the market for live musical and variety performances in the late 1940s and early 1950s. Phonograph records in part accounted for radio's reemergence as an important medium for music. MICHAEL FINK, INSIDE THE MUSIC BUSINESS 14 (1989) (stating "[r]adio, which in the early 1920s had nearly destroyed the record business, now owed its own recovery to its new role as something of a promotional tool for the recording industry"); SEGRAVE, *supra* note 70, at 50.

82. *See* LEONARD FEIST, AN INTRODUCTION TO POPULAR MUSIC PUBLISHING IN AMERICA 47 (1980).

> While the American population had swelled [since the 1920s] and its musical skills and awareness had grown, sheet music has never regained an economic significance in direct ratio to these changes. Where once a single popular song frequently sold over one million printed copies, purchase of half that number in a country with a trebled population was regarded as a phenomenon in the 1970s.

Id. Interestingly, even the medium of sheet music is adaptable to the digital age. As of this writing (Fall 1998), one company, called "Sunhawk," which came to the attention of this writer by accident, has developed a sort of "interactive sheet music" in digital format that can be bought over the Internet. *See Solero and Sunhawk Technology* <http://www.sunhawk.com/hawk/techfct.html>.

83. In 1872, zoologist Eadweard Muybridge designed what he called a "zoopraxiscope," a rotating disk with still images on it. Viewers would look through a small hole at the rotating disk and see a form of animation. Muybridge designed the device to

The new-use issue—whether motion pictures made use of and hence infringed some preexisting copyrighted work—appears not to have arisen in the early days of the industry. Most likely, the absence of major new-use infringement questions can be attributed to the fact that movies, at first, did not record or make use of some already copyrightable works in the way that the phonograph made use of already copyrightable music. In addition, not until the mid-1920s was sound added to motion pictures; necessarily, the use of music or other sounds on films as a possible new-use copyright infringement would not arise before that time.[85]

Indeed, for the first ten or so years of development, most motion pictures were recordings of live events and scenes,[86] which are not copyrightable. The early years of motion picture performance in one American city, Rochester, New York, for example, featured films of wrestling matches, dancing performances, horse racing, railroad trains entering a station, "a tub race, the coronation of the present czar, a watermelon match, a Parisian street scene, march of the French school children," and other "views": travel scenes from Moscow, Budapest, Venice, Dresden, and the United States.[87] Much of the appeal of movies was that they brought distant and exotic scenes to one's hometown.[88] Not until

---

resolve a major controversy of his day: whether all four feet of a horse are ever off the ground at the same time when the horse is galloping. M. JACKSON-WRIGLEY & ERIC LEYLAND, THE CINEMA 7–8 (1939). By 1885, William Friese-Greene had demonstrated a motion picture projected onto a screen. *Id.* at 6. Thomas Edison's assistant, William Dickson, was pioneering many of the advances later credited to Edison himself in the late 1880s. JOHN FELL, A HISTORY OF FILMS 10–11 (1979) (source on file with author).

84. Edison v. Lubin, 122 F. 240 (3d Cir. 1903).

85. *See* MILLARD, *supra* note 81, at 152–55.

86. For that matter, many early phonograph recordings were of nonmusical events, such as lectures, comedy monologues, religious evangelism, and the like. *See* GELATT, *supra* note 72, at 88–89; MILLARD, *supra* note 81, at 81. In part, turn of the century recording was driven by the fact that some sounds reproduced much better than others: banjo sounds, for example, were much easier to reproduce than violin sounds, and male voices could more easily be reproduced than female voices. MILLARD, *supra* note 81, at 81. Unlike motion picture technology, however, sound recordings required considerable equipment and typically were done in a recording studio.

87. GEORGE C. PRATT, *"No Magic, No Mystery, No Sleight of Hand": The First Ten Years of Motion Pictures in Rochester, in* "IMAGE" ON THE ART AND EVOLUTION OF THE FILM: PHOTOGRAPHS AND ARTICLES FROM THE MAGAZINE OF THE INTERNATIONAL MUSEUM OF PHOTOGRAPHY 39, 39–42 (Marshall Deutelbaum, ed., 1979) (quoting a contemporaneous newspaper account).

88. *See* KRISTIN THOMPSON & DAVID BORDWELL, FILM HISTORY: AN INTRODUCTION 12 (1994) (stating "most [film] subjects were nonfiction, or 'actualities.' These might be 'scenics,' or short travelogues, offering views of distant lands") (source on file with author). Films like this were only a minute or two long. Films were widely offered for rental

some years' worth of these vignettes had passed and the public's attention had begun to wane did motion pictures as a vehicle for dramatic storytelling come to the fore. After years of frequent showings of the travel oriented "views," for example, the city of Rochester went nearly two years, between 1901 and 1903, with no motion picture showings at all.[89] At that point, films "were still in danger of permanent extinction . . . . Their rescue came single handedly from the introduction and advance of the 'story' film . . . comprising a series of scenes related to a central character or group of characters."[90]

The first "stories" told were, perhaps not surprisingly, adaptations of stage dramas. Two notable films of this period are often cited as turning points in motion pictures' history, Edison Films' *The Great Train Robbery* in 1903, and D.W. Griffith's *The Birth of a Nation* in 1915. The former film was based on a road show drama of the same name,[91] while Griffith's was based on a 1905 play, *The Clansman*.[92]

When motion pictures became a vehicle for the adaptation of stage plays, the first new-use issue involving motion pictures arose. Toward the end of the century, publisher Harper & Brothers had bought the copyright to a recent popular novel by General Lew Wallace, *Ben Hur*, for the purpose of "dramatizing" the novel as that term was then used: making a stage play. Around the same time the Kalem Company decided to make a motion picture of the Wallace novel, hiring a writer to develop what today we would call a screenplay. It then made the film from the screenplay and licensed theaters to show it. Harper & Brothers brought suit.[93]

At that time, dramatic works themselves had been explicit copyrightable subject matter for about thirty-five years—since 1856—long before motion pictures had been invented.[94] When the right to "dramatize"

---

in film catalogs, such as those of the American Mutoscope and Biograph company in 1902, which classified its films as "'Comedy, Vaudeville, Trick, Sports and Pastimes, Notable Personages, Railroads, Scenic, Fire and Police, Military, Parades, Marine, Children, Educational, Expositions, Machinery, Miscellaneous.'" DAVID ROBINSON, FROM PEEP SHOW TO PALACE: THE BIRTH OF AMERICAN FILM 71 (1996) (quoting the American Mutoscope and Biograph catalogue), a litany strongly suggestive of nonfiction content. Exceptions were notable: Parisian Georges Méliès "transformed the cinema into a narrative medium . . . creating [around 1900] his own fantasy universe *at a time when most filmmakers were still content simply to photograph the world as it appeared before them.*" *Id.* at 74–75 (emphasis added).

89. PRATT, *supra* note 87, at 52.

90. *Id.* at 52.

91. ROBINSON, *supra* note 88, at 81.

92. PRATT, *supra* note 87, at 46.

93. Kalem Co. v. Harper Bros., 222 U.S. 55, 60 (1911) [hereinafter *Kalem II*].

94. Daly v. Palmer, 6 F. Cas. 1132, 1133 (C.C.S.D.N.Y. 1868) (No. 3552).

an existing nondramatic work was added in 1891,[95] it encompassed only stage plays: although motion picture research was well underway by 1891, the first public showing of a motion picture was not until 1895.[96]

The district court found for the plaintiff, Harper & Brothers.[97] The Second Circuit heard the first appeal and concluded that Kalem had indeed infringed Harper's right to dramatize the novel.[98] The court determined that showing a film was the same as putting on a play.[99] Kalem apparently argued that a play contained spoken dialog and that its movie was, like other movies of the day, a silent film.[100] This sort of factual distinction seems wholly irrelevant today, and struck the court as not much more even then: live dramatic productions include pantomime, noted the court, so that the absence of sound in a movie simply made the movie like a pantomime.[101]

Kalem also argued that it could not be an infringer because it had taken only the novel's ideas, not its "writing."[102] Today we might look on this as

---

> The act of August 18, 1856 (11 Stat. 138), provides, that any copyright thereafter granted under the laws of the United States, "to the author or proprietor of any dramatic composition, designed or suited for public representation, shall be deemed and taken to confer upon the said author or proprietor, his heirs and assigns, along with the sole right to print and publish the said composition, the sole right also to act, perform, or represent the same, or cause it to be acted, performed, or represented, on any stage or public place, during the whole period for which the copyright is obtained."

Id.

95. Today we know the right at issue as the broader one of either controlling the making of "derivative works" or the making of a "public performance" of the work under section 106 of the United States Code.

96. ALBERT R. FULTON, MOTION PICTURES: THE DEVELOPMENT OF AN ART FROM SILENT FILMS TO THE AGE OF TELEVISION (Norman ed., 1960).

97. Harper & Bros v. Kalem Co., 169 F. 61, 62 (2d Cir. 1909) [hereinafter *Kalem I*]. "A final decree granting a perpetual injunction was entered in the court below, from which this appeal is taken." *Id.*

98. *Id.* at 63. "When the film is put on an exhibiting machine, which reproduces the action of the actors and animals, we think it does become a dramatization, and infringes the exclusive right of the owner of the copyrighted book to dramatize it . . . ." *Id.*

99. *Id.*

100. *See Kalem I*, 169 F. at 64.

101. *Id.*

102. *Id.* In the Supreme Court, Kalem also argued that motion pictures are just part of a machine and hence could not infringe copyrights. *Kalem II*, 222 U.S. at 58. "The exhibition of the pictures, arranged upon a film which is, during all the time of its use, a part of a machine, is not an infringement of the book copyright." *Id.* The "just-part-of-a-machine" argument followed arguments made earlier that piano rolls did not infringe copyright. *See* Kennedy v. McTammany, 33 F. 584, 584 (C.C.D. Mass. 1888) (stating "I cannot convince myself that these perforated strips of paper are copies of sheet music, within the meaning of

the familiar argument that copyright protects only "expressions" of ideas, not the actual ideas themselves. But the court viewed the argument more as going to a combination of subject matter and infringement: can a movie made from a novel itself be a "writing" and hence infringe the rights in the novel?[103] The court misunderstood the nature of infringement, which does not depend on the infringing work being itself copyrightable,[104] but no matter: the court concluded that the Constitutional term "writing" had over the years been broadly applied to paintings, statutes, etc., and so was not offended by being extended to cover "film dramatizations."[105]

The Supreme Court agreed with the Second Circuit in an opinion by Justice Holmes issued in 1911.[106] Unlike the Second Circuit, the Supreme Court understood that the issue was not the copyrightability of the film. More precisely, where the appeals court had seemed to think that infringement by the film depended on the film itself sustaining a copyright (being considered a "writing"), the Supreme Court noted that the film's own copyrightability had nothing to do with escaping the charge of infringement.[107] But like the Second Circuit, even the Supreme Court focused on the matter of the movie's silence as being the touchstone of the question whether it could be a dramatization.[108] Again, the familiar analogy of pantomime carried the day, with the Supreme Court finding only a slight and legally insignificant difference between a "live" pantomime and a filmed one:

> We are of opinion that Ben Hur was dramatized by what was done .... Action can tell a story, display all the most vivid relations between men, and depict every kind of human emotion, without the aid of a word. It would be impossible to deny the title of drama to pantomime as played by masters of the art. *Daly v.*

---

the copyright law. They are not made to be addressed to the eye as sheet music, but they form part of a machine"); *see also* White-Smith Music Publ'g Co. v. Apollo Co., 209 U.S. 1, 7 (1908) (stating "[t]hings intended for mechanical function—for use in themselves—will not infringe copyright ....") (argument of Charles S. Burton and John J. O'Connell, counsel for defendant player-piano manufacturer Apollo Company). It also foreshadowed similar arguments raised nearly a hundred years later over computer programs in read-only memory, in *Williams Electronics, Inc. v. Artic Int'l, Inc.*, 685 F.2d 870, 874 (3d Cir. 1982) (stating "[d]efendant argues that there can be no copyright protection for the ROMs because they are utilitarian objects or machine parts"). However, these arguments had little effect in *Kalem II*.

103. *See Kalem I*, 169 F. at 65.

104. *Id.* at 63.

105. *Id.* at 64–65.

106. *Kalem II*, 222 U.S. at 63.

107. *Id.* at 62.

108. *Id.*

> *Palmer*, 6 Blatchf. 256, 264. But if a pantomime of Ben Hur would be a dramatizing of Ben Hur, it would be none the less so that it was exhibited to the audience by reflection from a glass and not by direct vision of the figures—as sometimes has been done in order to produce ghostly or inexplicable effects. The essence of the matter in the case last supposed is not the mechanism employed but that we see the event or story lived.[109]

The Court reached past superficial arguments to see "the essence of the matter" without being distracted by a focus on the "mechanism employed."[110] Perhaps this was a mild retreat from the *White-Smith* case's insistence only three years earlier that copyright applied only to the mechanism, and *not* to the essence of the matter.[111] In any event, the motion picture industry fell under the obligation to pay royalties for stories used and nevertheless rapidly grew to become the major economic force it is today.

C. *Cable Television*[112]

Rural homes in the 1950s, especially those in valleys or on the far side of mountains, were often unable to receive television signals clearly. With hindsight, it seems a logical improvement for someone to erect a large receiving antenna on the top of a mountain and "pipe" the received signal along a wire cable to those rural homes. The first term coined for what we call "cable television" today was "CATV," which stood for "Community

---

109. *Id.* at 61. The actual basis of the motion picture studio's liability for "dramatization" of the novel in theaters—under the control of independent contractors—was the doctrine of contributory infringement.

> The defendant not only expected but invoked by advertisement the use of its films for dramatic reproduction of the story. That was the most conspicuous purpose for which they could be used, and the one for which especially they were made. If the defendant did not *contribute to the infringement* it is impossible to do so except by taking part in the final act. It is liable on principles recognized in every part of the law.

Id. at 62–63 (emphasis added) (citations omitted).

110. *Kalem II*, 222 U.S. at 61.

111. *See supra* text accompanying note 26.

112. Much of the discussion of cable television is drawn from HARDY I, *supra* note 8, at 252–56 and from I. Trotter Hardy, *Computer RAM "Copies": Hit or Myth? Historical Perspectives on Caching as a Microcosm of Current Copyright Concerns*, 22 U. DAYTON L. REV. 423, 442–46 (1997) [hereinafter Hardy II].

Antenna Television."[113] Quite simple in concept, the idea of bringing television signals over a wire instead of through the air was novel. But it was successful, and the cable industry began to grow.

Not surprisingly, the copyright owners of the television programs being picked up by cable receiving antennas and transmitted to additional homes began to demand royalty payments from the cable companies. These demands were refused; lawsuits for copyright infringement followed shortly thereafter. Two similar cases involving these facts reached the United States Supreme Court a few years apart, *Fortnightly Corp. v. United Artists Television, Inc.*[114] and *Teleprompter Corp. v. Columbia Broadcasting System, Inc.*[115]

The issue in both cases was whether a cable station that, without authorization, received and further transmitted a copyrighted program should be held to be a copyright infringer.[116] Plaintiff's theory was that such a transmission constituted a "performance" of the copyrighted works.[117] As the performances were to the public and for profit (cable companies were not, to put it in Justice Holmes's famous words, "eleemosynary" institutions)[118] and were accomplished without permission or royalties, plaintiffs argued that the cable stations infringed their copyright rights.[119]

The defendant cable companies argued, quite straightforwardly, that merely by picking up a signal and passing it on, they did not "perform" anything.[120] The Supreme Court found for the defendant cable companies, determining that cable systems did not "perform" the shows they transmitted.[121] This conclusion was

---

113. *See* Fortnightly Corp. v. United Artists Television, Inc., 392 U.S. 390, 391 (1968). *See also* MARY ALICE MAYER PHILLIPS, CATV: A HISTORY OF COMMUNITY ANTENNA TELEVISION 4 (1972).

114. 392 U.S. 390 (1968).

115. 415 U.S. 394 (1974).

116. *Fortnightly* dealt with broadcast signals picked up from the local area and transmitted over cable. Fortnightly Corp. v. United Artists Television, Inc., 392 U.S. 390 (1968). *Teleprompter* dealt with broadcast signals picked up from distant markets. Teleprompter Corp. v. Columbia Broad. Sys., Inc., 415 U.S. 394 (1974). For purposes of the discussion in this article, both raise the same issues.

117. *Fortnightly*, 392 U.S. at 395; *Teleprompter*, 415 U.S. at 402.

118. Herbert v. Shanley Co., 242 U.S. 591, 594 (1917). One early cable system was created by John Walson, part owner of an appliance store, in 1948 to boost sales of television sets in the local, rural area. PHILLIPS, *supra* note 113, at 8–9. Initially given away, this cable service proved so popular that the very next year, 1949, Walson began charging a $100 installation fee and two dollars per month. *Id.*

119. *Fortnightly*, 392 U.S. at 390; *Teleprompter*, 415 U.S. at 404.

120. "The petitioner maintains that its CATV systems did not 'perform' the copyrighted works at all." *Fortnightly*, 392 U.S. at 395.

121. *Id.* at 402.

founded largely on the reasoning that cable companies were merely passive carriers[122] that did not rise to the level of "performing" in the ordinary sense of that term—or as the Court put it, "Broadcasters perform. Viewers do not perform."[123] The Court viewed cable as merely an extension of broadcast television, of little economic or other significance in itself.[124] "Essentially, a CATV system no more than enhances the viewer's capacity to receive the broadcaster's signals . . . ."[125] Cable systems

> "have nothing to do with sponsors, program content or arrangement. They sell community antenna service to a segment of the public for which [broadcasters'] programs were intended but which is not able, because of location or topographical condition, to receive them without rebroadcast or other relay service by community antennae . . . ."[126]

In other words, the Court saw cable television functioning mainly to promote some other already paid for medium—in this case, broadcast television—in much the same way that phonograph recordings were first seen as merely promoting sheet music.[127]

---

122. Note that the cable companies were not "passive carriers" as that term is often used in connection with telephone companies or Internet Service Providers. In the latter cases, the carrier is in a contractual relation with the sender of the information in question. With the cable companies, there was no contractual relation with the sender—the broadcasting companies—at all. In addition, cable companies have the ability to choose what signals to receive and retransmit, and to what audiences they will perform the retransmission.

123. *Fortnightly*, 392 U.S. at 398 (citation omitted). The Court announced that it would not simply look to the ordinary meaning of the word "perform," noting instead that

> [a]t the outset it is clear that the petitioner's systems did not "perform" the respondent's copyrighted works in any conventional sense of that term, or in any manner envisaged by the Congress that enacted the law in 1909. But our inquiry cannot be limited to ordinary meaning and legislative history . . . .

Id. at 395 (citations omitted). But in fact, the majority opinion largely *did* limit itself to ordinary meaning, especially in concluding that: "Broadcasters perform. Viewers do not perform. Thus, while both broadcaster and viewer play crucial roles in the total television process, a line is drawn between them. One is treated as active performer; the other, as passive beneficiary." *Id.* at 398–99 (citations omitted).

124. *Id.* at 399.

125. *Id. See also id.* at 400 (where the court stated "[b]roadcasters procure programs and propagate them to the public; CATV systems receive programs that have been released to the public and carry them by private channels to additional viewers").

126. *Fortnightly*, 392 U.S. at 400 n.28 (quoting Intermountain Broad. & Television Corp. v. Idaho Microwave, Inc., 196 F. Supp 315, 325 (D. Idaho 1961)).

127. See *supra* text accompanying notes 70–72.

Just as Congress was shortsighted in its assessment of recorded music a generation earlier, so the Supreme Court was dramatically shortsighted in its assessment of the significance of cable television. Far from remaining merely an adjunct to broadcast television, by the time Congress was revising the Copyright Act in the mid-1970s, the cable industry was a major economic force: nearly 3500 cable operators served 7700 communities, reaching 10.8 million homes and earning revenues of $770 million.[128] Cable was well beyond the point of simply extending existing broadcast signals to a wider and rural audience. It had become an alternative network, competing with broadcast networks[129]—and for that matter, growing much more rapidly in urban, affluent areas than among the rural poor.[130]

In a replay of what had happened with recorded sound a generation earlier when Congress debated the protection of musical compositions against the backdrop of a negative Supreme Court ruling, near endless Congressional debates[131] over cable television's copyright obligations arose against the backdrop of a negative Supreme Court ruling. In the end, as with the phonograph, a compromise was reached: Cable companies would pay a royalty, but the royalty would be fixed by Congress, and copyright owners would have no choice but to accept that royalty.[132]

D. *Current New-Use Issues*

The Internet has begun a new round of new-use issues. One such issue is whether audio and video sent over the Internet infringe any copyright rights. Digitizing audio or video signals—whether live or recorded—is quite simple with today's computers. Once digitized and resident on a computer's hard disk, these digital files can be set up to be played on demand. A number of new uses have appeared that depend on this digitizing capability. One innovative company developed a technique to play digitized music files over a telephone line as a customized aural greeting, in the process fulfilling one of Alexander Graham Bell's predictions about the

128. H.R. Rep. No. 94-1476 at 88 (1976).

129. PAUL GOLDSTEIN, COPYRIGHT PRINCIPLES, LAW AND PRACTICE, § 5.8.2 at p. 642 (1996).

130. *See* Phillips, *supra* note 113, at 171–72 (stating: "Industry leaders have recently expressed concern for a *neglected* sector of the American public—the rural dweller") (emphasis added; statement published in 1972).

131. *See* Litman, *supra* note 7, at 332 (stating "[i]t took eleven years and the combined efforts of the Copyright Office, the bar associations, the House and Senate Subcommittees, the FCC, and the White House Office of Telecommunications Policy to force interested parties to reach an agreement on the revision bill's treatment of cable television").

132. *See* Jessica D. Litman, *Copyright, Compromise, and Legislative History*, 72 CORNELL L. REV. 857 (1987). *See also* 17 U.S.C. § 111 (1994).

telephone's use for music some hundred years after he first made it.[133] A trade association representing music recording companies, the Recording Industry Association of America ("RIAA"), filed suit against this telephone music provider in early 1996 and soon thereafter a settlement was reached in which the defendant company agreed to stop making this use of copyrighted music.[134] As a settlement, of course, this proceeding did not establish that the new-use in question was infringing, though that seems likely to have been the outcome had the matter continued to trial.

Many Internet sites make recorded music available on demand over the Internet. Apparently these sites, at least initially, did not obtain licenses for their distributions. The RIAA sent a cease-and-desist letter to one such site, then called *AudioNet.com*, in early 1996 for exactly that activity.[135] The site—since renamed *broadcast.com*—has apparently removed the allegedly infringing materials and claims to have licensed the materials it continues to provide.[136] This same site provides links to live radio and television broadcasts, as well as various concerts and other audio and video events. This author is not aware of any conclusive legal determination that

---

133. *See* LEWIS COE, THE TELEPHONE AND ITS SEVERAL INVENTORS: A HISTORY 78 (1995).

134. *See Recording Industry Association of America, Nine Record Companies Reach Settlement In Infringement Action* <http://www.riaa.com/antipir/ releases/nine.htm> (stating

> Send-A-Song operates a commercial service for customers to order particular recordings to be played over the telephone, accompanied by a personal message, in the form of an "aural greeting card." Prior to the settlement, Send-A-Song made copies of the plaintiffs' sound recordings without the plaintiffs' consent, stored them in Send-A-Song's computers, and then transmitted these copies over the telephone to the recipients of Send-A-Song's services).

135. *See Recording Industry Association of America, RIAA Demands Internet Service Stop Violating Record Companies' Rights* <http://www.riaa.com/antipir/releases/rights.htm>.

136. *See broadcast.com, Terms and Conditions* <http://www.broadcast.com/about/ terms.html> (stating "[a]ll material on this site, including but not limited to images, illustrations, audio clips, and video clips, is protected by copyrights which are owned and controlled by broadcast.*com* or by other parties *that have licensed their material* to broadcast.*com*") (emphasis added); *Recording Industry Association of America, RIAA Releases Midyear Anti-Piracy Stats: CD Seizures, Dominated by Bootlegs, Increase Astronomically and Overtake Cassette Seizures* <http://www.riaa.com/antipir/releases/ midstats.htm> (stating:

> the RIAA demanded an Internet service stop violating record companies' rights when it sent a cease and desist letter to AudioNet. The company was providing an interactive service that offered 400 digital performances of full-length albums from a variety of musical genres, without the authority of many of the various sound recording copyright owners. AudioNet dropped all the infringing works within days).

such Internet live "broadcasts" infringe copyrights, so technically this new-use issue remains an open question. Nonetheless, the brief dispute with the RIAA and even the name change to *broadcast.com* certainly suggest that the site regards itself as a kind of broadcasting station, presumably subject to the same copyright rules as other more traditional broadcasters like radio and television.

V. NEW USES: ANALYSIS

When new technologies raise the new-use issue, the debate unfolds in a surprisingly predictable way. Whatever the forum, whether in congressional hearings or in court, representatives of authors and composers and those who, like publishers and distributors, are allied with those interests appear on one side. These parties tend to stress that copyright has long accommodated new technologies, that Congress intended to protect works of authorship in general, and that authors make little enough money as it is such that they need all the incentives that a new technology can give them; and consequently, that Congress ought to ensure that the new technology falls under a full regime of copyright liability applicable to existing technologies.

Opposing these arguments will be representatives of user groups: the owners of the new technology like radio that enables the new-use of others' copyrighted works, along with perhaps libraries, schools, research organizations, or the like. These parties concentrate their arguments either on a narrow reading of the statute as not applicable to the technology, or on the broader and more appealing argument that the new technology deserves a chance to grow without the encumbrance of exposure to copyright liability, or that the new-use of copyrighted works merely advertises the old use and as an affirmative benefit to copyright owners should not be held to infringe the existing works.

The arguments on both sides encompass two important policy considerations: the benefits of giving new technologies "room to grow" by not encumbering them with full copyright liability; and the benefits of ensuring that as a technology grows to become economically significant, those who create works of authorship for it will have an adequate incentive to continue their creative efforts. Sometimes the "no encumbrance" side of this argument has won out, as happened in the Supreme Court's decisions that cable television did not have to pay royalties to the creators of broadcast television programs.[137] At other times the reverse has been true, as happened

137. *See* Fortnightly Corp. v. United Artists Television, Inc., 392 U.S. 390 (1968); Teleprompter Corp. v. Columbia Broad. Sys., Inc., 415 U.S. 394 (1974).

when courts decided that radio broadcasters did have to pay royalties for the copyrighted material they broadcast.[138]

The argument that a new-use merely "advertises" an old use and hence should not be held to infringe is a particularly familiar one and leads naturally into the heart of this article's analysis of the new-use issue. Representatives of the phonograph recording industries in the 1900s strongly argued to Congress that records merely served as advertising for the sheet music market;[139] the producers of the motion picture *Ben Hur* argued before the Supreme Court that their movie would benefit sales of the book;[140] radio station owners in the 1920s argued to Congress that radio served mainly to advertise the sales of sheet music;[141] library photocopying of journal articles in the 1950s and 1960s was described by some as primarily a beneficial advertisement for the journals;[142] the Supreme Court found that cable television in the late 1960s merely promoted broadcast television;[143] representatives of an Internet news site argued that "framing" others' web sites benefited the sites framed;[144] the owner of an Internet site celebrating widely available digitized music over the Internet argued that the availability of such music benefited the bands whose music was thus made available.[145]

---

138. *See e.g.*, M. Witmark & Sons v. L. Bamberger & Co., 291 F. 776, 780 (D.N.J. 1923).

139. *See supra* text accompanying note 71.

140. *Kalem II*, 222 U.S. at 57 (1911). "Not only is there no evidence here that the copyright proprietors were injured even in the slightest degree; but, on the contrary, the defendant asserted by letter that its films would benefit the complainants, and this they did not deny, but stood upon their naked assertion of legal right." *Id.*

141. *See To Amend the Copyright Act: Hearings on S. 2600 Before the Subcomm. of the Comm. on Patents*, 68th Cong. 31–32 (1924) (statement of Charles H. Tuttle of the National Association of Broadcasters).

142. John C. Koepke, *Assessment of Documentation Practices in Reprography*, IN REPROGRAPHY AND COPYRIGHT LAW 50, 53 (Lowell H. Hattery & George P. Bush eds., 1964) (stating:

> The small journal will tell you that photoduplication actually increases its circulation rather than decreases it.... We have talked to many librarians who have told us that, after seven or eight requests for an article that may have appeared in a rather obscure journal, they have found it desirable to begin to subscribe to the journal....).

143. *See supra* text accompanying notes 123–127.

144. David S. Hilzenrath, *Online Publishers Wage a Battle Over Frame and Fortune*, THE WASH. POST, Feb. 11, 1997, at D4. "'A lot of news organizations are very pleased by what [TotalNews is] doing,' because TotalNews generates more visitors to their sites, said Lisa Farringer, a Washington attorney representing TotalNews." *Id.* (emphasis omitted).

145. *See* Michael Robertson, *Artists Use MP3 To Reach More Fans, Sell More CDs* <http://www.mp3.com/news/088.html> (stating:

On their face, these advertising arguments make no sense. Even when the arguments are true—and it has often been true that a new-use of copyrighted works does promote the sales of an existing format[146]—nothing in copyright policy supports the *obliging* of authors to advertise their creativity, and certainly not obliging them to advertise on terms and in places that they may not desire.[147] If authors have a right to object to others' advertising their works, in circumstances where withholding their objections would benefit them, then the authors will simply withhold their objections in order to gain the benefits of the advertising.[148] After all, novelists have the

---

> One strategy for artists to consider is to seed the Internet with one or more songs. This enables music listeners to get a taste of an artist's style or a sample from a CD. If they like what they hear they will spread the music and a percentage will buy the CD).

The term "MP3" refers to a type of data compression technology that is especially suited to compressing digital music files.

146. The music business has been particularly attuned to the desirability of advertising music through new uses, from vaudeville and phonograph records, which initially advertised sheet music sales, to radio, which advertised first sheet music sales then phonograph record sales and now CDs. *See generally* SEGRAVE, *supra* note 70; *see also id.* at 13, 37, 51 (vaudeville advertising sheet music, radio advertising sheet music, and radio advertising records). The number of new bands that voluntarily permit their music to be digitized and available on the World Wide Web today suggests that these bands find the new-use of Internet broadcasting to be valuable advertising. One popular music download site, <http://www.mp3.com>, claimed that "MP3.com is the #1 music download site on the Internet, with 3,000,000 visitors per month. In the past year, MP3.com has facilitated more than 5,000,000 legal, original song downloads—approximately 75,000 songs daily." Michael Robertson, *Platinum Entertainment Offers Free MP3 Downloads Via MP3.Com* <http://www.mp3.com/news/123.html>.

147. *Accord* M. Witmark & Sons v. L. Bamberger & Co., 291 F. 776, 779–80 (D.N.J. 1923).

> There is another point which, although striking us as immaterial, deserves some comment. The defendant argues that the plaintiff should not complain of the broadcasting of its song because of the great advertising service thereby accorded the copyrighted number. Our own opinion of the possibilities of advertising by radio leads us to the belief that the broadcasting of a newly copyrighted musical composition would greatly enhance the sales of the printed sheet. But the copyright owners and the music publishers themselves are perhaps the best judges of the method of popularizing musical selections. There may be various methods of bringing them to the attention of music lovers. It may be that one type of song is treated differently than a song of another type. But, be that as it may, the method, we think, is the privilege of the owner. He has the exclusive right to publish and vend, as well as to perform.

Id.

right to object to someone else's publishing their novels, yet most novelists are all too eager to waive that right in return for that very publication. That is how copyright law works.

Behind these nonsensical facial arguments about advertising, we can discover a much more principled assertion that focuses on authors' incentives to create. In copyright terms, the advertising argument can be understood as saying that because a particular new-use benefits copyright authors, those authors do not need any further incentive to create for the new-use medium. If they need no further incentive, then imposing infringement liability for the new-uses merely penalizes the public by requiring them to pay for something that would have been created and available for free anyway.[149]

---

148. In the June 1906 hearings on what became the 1909 Copyright Act, the testimony of witness Paul Cromelin of the Columbia Phonograph Company, went for pages and pages, with numerous quoted letters from others to him, all designed to convince Congress that phonograph record sales did indeed benefit music composers through the sale of sheet music. At one point, Mr. Cromelin was interrupted by Representative John Chaney, who asked how the granting of a right to composers to control recordings would make any difference to that state of affairs:

> MR. CHANEY. Let me ask you this question: There is not very much doubt but what your theory of this is all right—that all these people [i.e., composers] want to get their music before the public, and they are seeking every means of advertising it. Now, in this bill, should it pass [and give composers the right to demand royalties from recording], is there anything to prevent that continuing, and, if so, what is it that would interfere with it?

See BRYLAWSKI, *supra* note 22, Part H at 333.

At which point Cromelin appeared mildly flustered and was saved when another witness, attorney Albert H. Walker, quickly steered the discussion to other concerns, namely that music publishers, acting on behalf of composers, would all sign exclusive contracts with a single manufacturer of piano rolls, the Æolian Company, and hence create an unstoppable monopoly:

> MR. WALKER. [A]s soon as the Æolian contract goes into effect the [music] publishers will no longer be at liberty to send these pieces to Mr. Cromelin, and will be under an ironclad contract running for thirty-five years to sell them to the Æolian Company only.

See id. at 334.

The arguments that music publishers would tie up composers in a web of exclusive contracts, and that such exclusive arrangements constituted a harmful monopoly, seem a bit hypocritical: recording companies like Cromelin's routinely signed exclusive contracts with *performers*, contracts that at times included royalty payments based on the sales of the records. *See id.* at 215–17 (testimony from various parties concerning recording companies' exclusive contracts with certain performers).

149. *See, e.g.*, GOLDSTEIN, *supra* note 129, § 1.14 at p. 1:40 (noting the argument that "To give greater property rights than are needed to obtain the desired quantity and quality of

Even understood in this more principled way, the arguments about advertising and authors' incentives miss the mark. The question is not whether an incentive is necessary when works of authorship like music already exist and a technology like the phonograph, radio, cable television, or the Internet is new. At its earliest stages—say, on the date of its first invention—a new-use technology will obviously not have an effect on authors' incentives. It would be silly to suggest that the day Edison first achieved the playback of a recorded sound or the Internet first transmitted an audio file of music, music composers everywhere suddenly had a need for an additional royalty incentive in order to continue composing.

Obviously the day of invention—even if it could clearly be identified—is too soon to look at the question of a new technology's effects on copyright incentives. We should instead ask: will this new-use technology grow in economic importance, at some point in the future, to the point that not imposing royalty obligations on it would seriously diminish authors' incentives to create? If that point never comes, then we should never impose royalty obligations on the new-use. If it does come, then we should.

Determining the "right" degree of incentives, let alone when they become necessary, is an issue fraught with difficulty. Rather than undertake that task, we can make a simplifying assumption. Let us assume for purposes of analysis that at the time a new-use technology arises, the existing copyright incentives are already at the "right"—the necessary and appropriate—level for all other technologies and uses. That is, instead of trying to calculate a measure of incentives and asking when authorial incentives in the aggregate, from all possible uses of copyrighted works, have reached or deviated from the "right" level, we can instead ask the easier question of when, if ever, will current incentives *decline* because of a new-use technology? By assuming that current incentives are at the "right" level to start with, if we can determine a point at which they decline from that level, then we have determined the point at which incentives need to be added to bring authorial creativity back up to the "right" level.

In short, we can focus on displacement: will a new-use technology eventually displace existing uses of copyrighted works—the uses that do generate royalty income and hence provide a present incentive? If the new-use industry ends up displacing present forms of copyright exploitation, then

---

works would impose costs on users without any countervailing benefits to society") *Id.* (footnotes omitted); Jessica Litman, *Revising Copyright Law for the Information Age*, 75 OR. L. REV. 19, 31–32 n.43 (1996) (stating "it is conventional to argue that copyright holders should receive only such incentives as are necessary to impel them to create and disseminate new works") (citation omitted); Wendy J. Gordon, *Fair Use as Market Failure: A Structural and Economic Analysis of the* Betamax *Case and its Predecessors*, 82 COLUM. L. REV. 1600, 1610 (1982) (stating "[c]opyright . . . create[s] ownership rights in intellectual property, with the primary goal of generating monetary incentives for the production of creative works").

a new incentive in the form of royalties from the new industry's use will be needed. If it does not ever displace present-day forms of exploitation, then a new incentive will not be needed.

The problem, of course, is that without foresight, neither Congress nor the courts can know which growth path a new-use industry is likely to follow. Will the new-use remain forever an aside to some existing market, potentially[150] only a minor source of income to copyright owners because the primary sources are not displaced; or will it outgrow and dominate that existing market, displacing it to become a major source of income for copyright owners; or something in between?

The short and accurate answer is "no one knows." But this situation is a classic case of the need for a decision maker — court or Congress — to make decisions under uncertainty; techniques exist to help us in that effort. The decision maker will be faced with what statisticians call "Type I and Type II" errors.[151] The labels themselves mean nothing and provide no useful insights into the problem, but they do constitute a kind of shorthand that makes further discussion a bit more convenient. The terms are used here solely for that reason. A Type I error means that a decision was made to do something that need not or should not have been done. A Type II error means that a decision to do something was not made, but should have been.

In the context of technologies that allow new uses of copyrighted works, that cryptic summary means this. A Type I error would be committed if a decision-maker decided to impose royalty obligations on a new-use industry when royalty payments were unnecessary because the industry was destined to remain only marginally important to copyright owners. A Type II error would be committed if the decision-maker concluded that the new-use industry should not be required to pay royalties, and yet the industry was destined to become a major market for copyright owners.

One way to address the problem of uncertainty in this copyright context is to ask which of these two errors is the more likely and the more serious; other things being equal, if one error is both more likely and more serious than other errors, then that error should be avoided. That is, if one error is likely to bring about a greater harm to the public than the other, and the decision maker has no independent reason to pick one outcome over the other, then the error most likely to cause the greatest harm should be avoided. The question of infringement for new uses of existing copyrighted works therefore reduces itself to an inquiry as to which harm is likely to be greater, a Type I or a Type II error.

---

150. The new-use is only "potentially" a source of income because whether it is or is not an actual source depends on how the copyright issues are decided.

151. *See, e.g.*, MICHAEL O. FINKELSTEIN & BRUCE LEVIN, STATISTICS FOR LAWYERS 124–26 (1990).

A. *Type I Errors*

A Type I error means that a decision is made that the new-use is an infringement, and consequently that the copyright owner has a right to demand royalties, even though it will eventually prove to be the case that the new-use industry does not become a significant market for copyright owners. What is the harm from that outcome?

Two related harms seem possible. First is that a requirement to make royalty payments may be enough to stifle the new-use industry, leaving it to founder when it might have survived, or perhaps leaving it weakened, amounting to less than it might have amounted. We might call this a Type Ia error—again, only for convenience; there is no special magic in labels. This possibility of this type of error has been indirectly noted in academic literature. Professor Jessica Litman has written about the many new technologies that have not been required to pay royalties, but instead, have been allowed to grow up in the "shelter of a copyright exemption."[152] This view, that being sheltered from royalty obligations fosters and promotes the growth of desirable new industries, implies the contrary: that if these new-use industries *had* been obligated to pay royalties, they would have been stifled or suppressed[153]—and that would be what this article terms a Type Ia, or "suppression" error.

Perhaps worse, a second type of harm from Type I errors would arise if copyright owners were content with their own system of exploiting copyrighted works and simply did not want any competition from new uses. They might therefore deny a license to the new industry even if the industry were willing and could afford to pay a suitable royalty. We can call this a Type Ib, or "status quo" error, implying that the existing copyright owners and copyright industries are happy with the status quo and simply do not care to authorize a change by licensing any new uses.[154]

---

152. Litman, *supra* note 149, at 29 n.33; *see generally id.* at 27 (stating "copyright shelters and exemptions have, historically, encouraged rapid investment and growth in new media of expression").

153. *Accord* Twentieth Century Music Corp. v. Aiken, 422 U.S. 151, 166 (1975) (Blackmun, J., concurring) (stating "I had hoped, secondarily, that the reasoning of *Fortnightly* and *Teleprompter* would be limited to CATV. At least in that context the two decisions had the arguably desirable effect of *protecting an infant industry from a premature death*") (emphasis added).

154. Litman, *supra* note 149, at 25 (stating "[m]ost [current copyright stakeholders] would prefer that the new copyright rules for new copyright-affecting technologies be designed to enable current stakeholders to retain their dominance in the marketplace") (footnotes omitted).

B. *Type II Errors*

A Type II error means that a decision is made that the new-use is not an infringement, even though the industry is destined to become potentially a major source of income to copyright owners. What is the harm here?

Most obviously, the harm is that the lack of royalties from the new industry will mean a significant disincentive for authors as the old royalty paying industry gradually shrinks in importance. In that event, the public will lose the benefit of whatever a greater incentive might have brought.

Let us take the phonograph record industry as an example. In the early days of the industry, the incentives for the creation of musical compositions came almost entirely from the sale of sheet music, which dominated the market for music in the home.[155] Yet eventually the phonograph recording industry grew enormously more important in sales and dollar volume than the sheet music industry.[156] Had the recording industry been exempt from royalty payments, for example, it is most unlikely that composers' income from the sale of sheet music would have continued to this day to induce the creation of the socially desirable amount of music.

C. *Which Harm is Greater?*

So which harm is the greater, a "Type I" or a "Type II" error? The first harm from a Type Ia error is that a new-use industry might be suppressed or weakened by the obligation to pay royalties. That is only a harm, though, if the public would have derived greater total benefits from the new industry's presence and strength than its absence—that is, if the new-use industry had survived *and* all other things had been equal.

Manifestly, however, all other things would not be equal. In particular, authors unable to derive revenue from the new-use of their works are worse off than they would be if they were able to derive revenue. In a rough sense, what the new-use industry gains by not having to pay royalties is offset by what authors lose by not receiving royalties.[157] Conversely, under the opposite copyright liability regime (one of full liability), the new royalty revenues that authors can command from the new-use are offset by the corresponding increased royalty costs for the new industry.

In short, we want to maximize the benefits—less the costs—of *both* old and new uses of copyrighted works. A new-use industry strengthened means

155. *See supra* text accompanying note 70.

156. *See* FEIST, *supra* note 82 and accompanying quotation. See also the phonograph company earnings figures listed *supra* note 72.

157. The trade-off will not necessarily be one for one: not all authors entitled to demand royalties would demand them, or demand as much as they might.

an old use industry weakened. And vice versa. Unless one is committed to the proposition that new things are *ipso facto* superior to old things,[158] one cannot say that the stifling of a new-use industry is necessarily bad. So the question of the Type I error becomes not just "was the new-use industry stifled or weakened," but more precisely "was the new-use industry stifled or weakened *inappropriately*, i.e., to the public's overall detriment?"

How might the "stifling of an industry to the public's detriment" happen? Start with this assumption: Apart from the royalties question, the new-use industry would have to bring benefits greater than its costs to survive in any event. If it did not earn a profit, it would fail to survive in the marketplace. Absent some sort of larger market failure,[159] an individual business's or industry's failure would be a socially useful result because it would free up resources to be used in more socially desirable ways. If a new-use industry brought so little value to the public that it was destined to fail even without paying royalties, then the requirement of paying royalties might hasten its demise—and that would be a good thing.

On the other hand, if the new-use industry were so socially beneficial that it was destined to earn substantial profits, then an obligation to pay royalties within some reasonable range would not be enough to stifle it. At least we know that an obligation to pay royalties does not *necessarily* prevent an industry from growing—both radio and television, and for that matter, motion pictures,[160] have grown up under such royalty obligations.

We come to an important conclusion. Whether a new-use industry is obliged to pay royalties or not makes the most difference when that new

158. *Cf.* Litman, *supra* note 149, at 27, where Professor Litman appears to hold the view that new is *ipso facto* better than old. (stating "[suppose] we imagined the viewpoint of a hypothetical benevolent despot with *the goal of promoting exciting new technology*"). *Id.* (emphasis added).

159. "Larger market failure" implies some sort of externality. Pollution is the classic negative externality: something that affects others but with effects that are not captured in a marketplace transaction and hence not reflected in the price of polluting company's product. A firm with uncorrected negative externalities imposes costs on others that the firm does not have to bear; that means that the firm might succeed when it "ought" to fail. A firm might also generate "positive externalities," or benefits provided to others that the firm cannot capture through appropriate pricing of its products. For example, a firm that designed especially good looking Internet sites might find their sites used as "teaching aids" or models for emulation by aspiring Internet page designers. To the extent that the aspiring designers do not themselves pay for the "instruction" they receive from studying the firm's site designs, the firm has conferred external benefits on those designers.

160. *See Kalem II*, 222 U.S. at 62 (1911) (stating that a motion picture made from a novel infringes the novel owner's right to control dramatizations of the novel, even though the right of "dramatization" in the statute was enacted at a time before the development of motion pictures when stage plays were all that was expressly contemplated).

industry is barely profitable. And—again, absent market failures—an industry that is barely profitable is one that makes a comparably small contribution to society. Finally, that conclusion leads us to a useful rule of thumb: If a decision maker makes a Type Ia error, finding infringement liability where the industry is of only slight significance and consequently for which the obligation to pay royalties is likely to be a significant factor in causing the industry to fail, the magnitude of the error is likely to be quite small.

Now we must address the second type of harm, a Type Ib error: Congress or courts impose infringement liability and a corresponding obligation to pay royalties in a situation in which authors will refuse to license the new-use in order to preserve their existing business. For industries destined to fail for want of providing any significant public value, we are no worse off if copyright owners refuse a license. By hypothesis, a copyright owner's refusal to permit licensing merely hastens the demise of an nonbeneficial industry, a socially desirable outcome. But for those new-use industries that might have provided significant value to society, a copyright owner's refusal to license would presumably put the new-use industry out of business, and that would be harmful to the public.

Is this outcome likely in practice? Do authors (copyright owners) actually refuse to license uses of their works when it would be profitable for them to do so? Of course, anything can happen. People can be motivated by "irrational" forces: anger, spite, etc. But in the main, one would expect that if authors can make money by licensing, they will.[161] It is in their self-interest to do so. In other words, the likelihood that authors given both a right and a market that permits them to demand royalties in some profitable amount, would instead refuse royalties in any amount, seems small—far less than the likelihood that they would happily receive them. At the very least, if one has to make rules that govern most situations, most of the time, one is more likely to be right if one predicts that when money can be made, the people in a position to make it will try to make it.

---

161. *Cf.* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 316 (5th ed. 1998) (stating in relation to patents that "it is always more profitable to license production to a more efficient producer than it is to produce oneself"); ARMEN A. ALCHIAN & WILLIAM R. ALLEN, EXCHANGE AND PRODUCTION: COMPETITION, COORDINATION, & CONTROL 292 (3d ed. 1983) (describing in relation to patents the fallacy of "a commonplace of modern folklore that gasoline producers have a new fuel or carburetor that would enormously reduce the demand for gasoline, but to protect their wealth they have withheld the device"); ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 138 (1988) (referring to patents: "[T]he use of a patent to suppress an invention is exceedingly unlikely. The far more common case is that the licensing of a patent for a fee is much more valuable to the patentee than is the act of not revealing an invention").

Summing up, we can see that the harm from a Type Ib error is significant, but the likelihood that such an error will be made—in which a new-use industry would have prospered, to the public's overall benefit, but the relevant authors refused, on economically irrational grounds, to grant a license for that use—is low.[162]

D. *Type II Errors*

A Type II error means that the new-use industry is found not to infringe but is destined to grow in importance to the point that the industry's failure to pay royalties will constitute a significant disincentive to authors. What is the harm here?

The obvious harm is that with inadequate incentives, authors create (or publishers publish, or distributors distribute, etc.) less than they might have and the public is worse off as a result. Is that a likely harm? Surprisingly, we have no examples of an important industry that was held to have no royalty obligations and for which the lack of obligation persisted throughout the industry's history. The examples that would likely have fit that pattern all ended up eventually with some form of royalty obligation, frequently in the form of a compulsory license. The phonograph and cable television certainly fit this model, as did the jukebox until 1993.[163]

One might question, then, whether there is any harm at all when a court declines to impose infringement liability and hence a royalty obligation on a new-use industry. If the industry is destined to remain of little public benefit, then the loss of its royalties to authors will not be significant. Yet, if the industry does become important, then Congress will act to impose compulsory license royalties. That has at least been something of the historical pattern.

The problem with this reasoning is that it assumes two things: first, that the royalty obligation (again, typically in the form of a compulsory license) will be imposed at about the same time as the industry becomes significant enough to justify the requirement and not earlier or later; and second, that compulsory licenses—if that is the mechanism—are a desirable way to accommodate the royalty obligation. The evidence to date suggests that the

162. One counterargument is that we do not care about "authors" literally. It is the old use *industry* that matters, the industry that is not an "author" itself but a licensee of authors. The counterargument fails, however: New authors arise all the time and have the option to transfer their rights to old *or* new-use industries. To the extent that the old use industry is itself the "author" of the works its sells, then the argument in the text holds directly.

163. *See* 17 U.S.C. § 115 (Supp. 1995) (phonorecords); 17 U.S.C. § 111(c), (d) (1994) (cable television); 17 U.S.C. § 116(b) (1988), *repealed by* Act of Dec. 17, 1993, Pub. L. No. 103-198, § 3(a), (b)(2), 107 Stat. 2309.

first assumption is questionable and that the second is correct only as a matter of politics, but certainly incorrect as a matter of economics.

The first assumption is that a decision to impose infringement liability on a new-use industry will not just happen eventually, but will happen at roughly the "right" time. The "right" time is the time that the need for an incentive to authors arises. If the obligation is imposed later than that, then the public will be the poorer for the delay; moreover, a belated imposition of royalties will almost certainly not be retroactive,[164] so that the loss to the public is one that can never be repaid. When exactly that time first arises is obviously a difficult question to answer. Certainly authors and the new-use industry would not agree on the matter: Authors are likely to believe that the "right" time for royalty payments is from the beginning, whenever the new-use first arose; the new-use industry is likely to believe that the right time is "never."

The very difficulty of determining objectively when the right time arises, coupled with a strong self-interest on both sides that effectively prevents them from having an objective view at all, implies that there is little or no incentive in either the legislative or judicial arenas for decision makers to discover what the "right" time is for the imposition of a royalty obligation. That is, no one in a position to take action—the parties, the courts, or Congress—stands to gain by trying to determine the right time for royalty imposition. Consequently, one must conclude that when infringement liability and a royalty obligation is belatedly imposed on a new-use industry, the assumption that this imposition will come at the "right time" is probably wrong. At the very least, we can say that there is no built-in incentive for the assumption to be true and hence, no reason to expect the timing to be "right."

The point about economics—that compulsory licenses are wasteful of resources—is easier to demonstrate. A compulsory license is a form of price fixing: Congress or an agency sets the price for a broad class of bargains[165]—those that deal with the buying and selling of certain copyright

164. A retroactive imposition of liability would mean this: First, a new-use industry is found (by a court or Congress) not to infringe some existing works; second, the new-use industry grows in importance to the point that the lack of royalty payments becomes a significant disincentive to authors; third, a decision is made (by court or Congress) that the new-use industry *should* pay royalties; and finally, the decision maker extends this new royalty obligation to past acts that have already been determined not to infringe. This last step seems very likely to be a denial of due process and hence unconstitutional.

165. For example, for pre-1998 transactions, the license to record a musical composition that has already been recorded is set in the statute at "either two and three-fourths cents, or one-half of one cent per minute of playing time or fraction thereof, whichever amount is larger." 17 U.S.C. § 115(c)(2) (1994). After 1998, the decision maker shifts from Congress to the Copyright Office, which has acquired the authority to establish license prices

licenses; the parties have little or no room to change the price term.[166] As such, a compulsory license has whatever drawbacks price controls have. Absent significant market failures,[167] a compulsory license makes for a wasteful allocation of social resources.[168]

Compulsory licenses might be justified on two other grounds, however. First, that such a license can reflect a Congressional policy determination simply to favor one industry or activity over another. For example, Congress might decide to favor cable television with compulsory license payments that were lower than fair market value precisely to foster the growth of cable at the expense of other activities. Whether this is a desirable way to create subsidies instead of alternatives like tax deductions or outright subsidy payments from general tax revenues is partly a matter of politics and political philosophy.

In addition, there is a possibility that a compulsory license will lower transaction costs. This is at times offered as a justification for such licenses,[169] but this point is misleading at best. Other things being equal,

---

under 17 U.S.C. §§ 801–803 (1994). In the case of cable royalties, the price is based on a station's annual revenue and determined from a complex series of conditions. *See* 17 U.S.C. § 111(d) (1994).

166. Under many copyright compulsory license provisions, the statutorily specified price serves as a ceiling; the parties may reach agreement for a lower price. *See, e.g.*, 17 U.S.C. § 115(c)(3)(B) (Supp. II 1997) (stating "copyright owners of nondramatic musical works and any persons entitled to obtain a compulsory license [for cover records] . . . may negotiate and agree upon the terms and rates of royalty payments"); 17 U.S.C. § 118(b) (1994) (stating that owners of copyright in certain musical and other works and "any public broadcasting entities, respectively, may negotiate and agree upon the terms and rates of royalty payments"). From early on, lesser-known music recordings "covered" by better-known artists have in fact received less than the statutory royalty. *See* SEGRAVE, *supra* note 70, at 18, 20.

167. *See supra* text accompanying note 159.

168. *See, e.g.*, Stanley M. Besen & Robert W. Crandall, *The Deregulation of Cable Television*, 44 LAW & CONTEMP. PROBS. 77, 77–79 (1981); ALCHIAN & ALLEN, *supra* note 161, at 62. Note that by hypothesis I am describing a new-use industry that has grown to the point where royalties from an "old use" industry have fallen off significantly; consequently, I am describing a situation for which a royalty obligation from the new-use industry is consistent with overall reliance on copyright as an incentive for the public's benefit. One can always assert that Congress is free to deny copyright to any activity and that it can certainly extend a limited copyright in the form of compulsory licenses to any activity as well. I do not gainsay that point; I am not talking about Congressional *power* but rather about a situation in which anyone who agreed with the fundamental principles of copyright—an incentive for creation that redounds to the public's benefit—would agree that a royalty is called for.

169. Transaction costs were offered as the reason for a statutorily specified compulsory license for cable television in the 1976 Copyright Act: "[I]t would be impractical and unduly burdensome to require every cable system to negotiate with every copyright owner whose work was retransmitted by a cable system." H.R. REP. NO. 94-1476, at 89 (1976).

price fixing *always* lowers transaction costs because it avoids the need for bargaining. If that were a suitable justification in general, then Congress ought to establish prices for every transaction in every market, copyright or otherwise. That Congress has never systematically attempted to fix the prices of all goods and services in the United States marketplace suggests that the transaction cost rationale alone must not in fact be a helpful explanation for the existence of compulsory licenses.[170]

In any event, there is no evidence in our recent compulsory license provisions such as for jukeboxes,[171] cable television,[172] phonograph recording,[173] public broadcasting,[174] satellite transmissions,[175] and others that social welfare is improved by that mechanism.[176] Whereas there *is* reason to think that the fair use provision—itself a kind of compulsory license that operates in situations with additional indications of public benefit—accomplishes overall socially desirable objectives.[177]

Economics aside, it appears that the large number of compulsory licenses in copyright law is based on the fact that politically, the compulsory license makes a great deal of sense. When a Type II error is made early on, and an industry prospers without liability that should, at some point, be obliged to pay royalties, it is politically difficult—perhaps impossible—for Congress to switch the industry "cold turkey" from no liability to full liability. Nor would that switch be fair to the industry which, after all, has relied for its investments on a past decision that its actions did *not* constitute

---

170. *See also* Hardy II, *supra* note 112, at 446 (stating "[a] reduction in transaction costs through legislation is beneficial only if all sides benefit from the reduction. If one side benefits but only to the corresponding detriment of the other side, then Congress has merely shifted resources from one side to the other by a form of price-fixing").

171. 17 U.S.C. § 116(a) (1988), *repealed by* Copyright Royalty Reform Act of 1993, Pub. L. No. 103-198 § 3, 107 Stat. 2309 (1993).

172. 17 U.S.C. § 111(d) (1994).

173. *Id.* at § 115.

174. *Id.* at § 118(b)(3).

175. *Id.* at § 119.

176. Compulsory licensing may at times have even more pernicious and unexpected consequences than a simple failure to promote the general welfare. The compulsory licensing of recorded music, for example, which takes the form of allowing the making of "cover records" without permission, has been said to have encouraged both racism and payola. *See* SEGRAVE, *supra* note 70, at 18–19 (stating the compulsory licensing of cover records allowed: "racism to be more prevalent, especially noticeable in the 1950s when racist radio stations refused to play, for example, Little Richard, substituting instead a white cover by Pat Boone. [The presence of multiple versions of the same song in] turn has put more pressure on companies to dispense payola").

177. *See* Gordon, *supra* note 149, at 1602.

infringement.[178] A compulsory license, then, is often the only compromise that can be reached at that stage in the growth of the new-use industry.[179]

Finally, whenever a decision about infringement liability reaches Congress, one expects a fair amount of lobbying and arguing about the outcome. The 1909 Copyright Act hearings, for example, were full of witnesses and lengthy testimony about the issue of phonograph recordings and piano rolls.[180] The issue of cable television's copyright liability consumed a substantial amount of debate during the 1976 Copyright Act revision process—as, for that matter, did nearly every issue![181] In a sense, whenever an important issue like cable television or recorded sound surfaces in Congress during a revision effort, substantial "transaction costs" are entailed in lobbying and testifying.

The cost of a Type II error, in sum, consists of three parts. First is the cost of the public's loss of access to creative expression during the period in which the new-use industry should have been paying royalties.[182] Second, there is the cost of a compulsory license, which is essentially the waste of

178. For example, see the 1908 arguments of counsel for the Apollo Company (piano roll manufacturer), Charles S. Burton and John J. O'Connell, that past court decisions holding piano rolls not to infringe musical compositions constituted "prior decisions [that] have established a rule of property *and of business*, and should be sustained under the doctrine of *stare decisis*, unless greater injury would result from sustaining than from reversing them." White-Smith Music Publ'g Co. v. Apollo Co., 209 U.S. 1, 7 (1908) (emphasis added); *Revision of Copyright Laws: Hearings Before the Joint Comm. on Patents*, 59th Cong. (1906), *reprinted in* BRYLAWSKI, *supra* note 22, Part J at 289 (statement of Frank L. Dyer, of the Edison Manufacturing Company and National Phonograph Company) (stating

> I submit, gentlemen, that a radical change in the law would seriously disturb vested interests which have enormously developed under the present law. The National Phonograph [company] has a pay roll of over $45,000 per week, over 4,000 employees, and makes over 100,000 records and 1,500 machines daily .... The business has developed under the security of the present law ....).

179. For useful exposition of the events behind the adoption of the compulsory license provision for cable television in the 1979 Copyright Act, see Litman, *supra* note 7, at 326–32. *See also* Darlene A. Cote, Note, *Chipping Away at the Copyright Owner's Rights: Congress' Continued Reliance on the Compulsory License*, 2 J. INTELL. PROP. L. 219 (1994).

180. *See generally* Copyright Act of 1909, Pub. L. No. 60-349, 35 Stat. 1075 (codified as amended at 17 U.S.C. §§ 101–914 (1994)).

181. *See* Litman, *supra* note 132, at 857.

182. I apologize for possibly beating a dead horse, but once again I remind the reader that I am talking here about an industry that "should have been paying royalties" because, *by hypothesis*, the industry has grown to the point that its failure to pay royalties constitutes a significant loss of incentives to authors and therefore, a loss to the public.

resources inherent in any price fixing arrangement.[183] And finally, there is the cost of the decision making process when authors line up against a new-use industry during the process of copyright revision. These include: lobbying costs, publicity campaigns, time consumed in Congressional hearings by participants, time given up by members of Congress that might have been applied to other issues, and whatever other expenses accompany a major legislative battle between opposed industry groups.[184]

E. *Type I and II Errors: Summary*

We can chart the various errors and their harms. As is so often true with copyright issues, assessments of the magnitude of harm and its frequency from various courses of action are largely subjective; this article makes no claim otherwise. With the subjective nature of the following assessments taken into account, on balance, we have something like this chart:

Error type	Likely frequency	Likely harm
Type Ia	?	insubstantial
Type Ib	low	substantial
Type II	high	substantial

Unless the expected frequency of Type Ia errors is extremely high, the greatest expected harm from wrong decisions about the infringement liability of new-use industries is that of a Type II error. That is, the error we should be concerned to avoid is that of failing to impose infringement liability on the new-use industry. In turn, this means that—all other things being equal, and there being no other basis for a decision—*the decision maker faced with deciding whether a new-use industry should be obliged to pay royalties will more likely be right when deciding "yes" than "no."*

The history of various new technologies sketched out in this article tends to confirm this general rule of thumb. The technologies discussed here

183. There is no *requirement* that the imposition of a belated royalty obligation take the form of a compulsory license with its inefficiencies. It is just that as a practical matter, that seems to be the usual course for Congress to take because it reflects a political compromise. Note also that one may choose to put a high value on government decision making such as price controls for its own sake. From that perspective, the "cost" of a compulsory license in poorly allocated resources may perhaps be offset by whatever "gain" inheres in the fact that a resource allocation decision was made by Congress rather than privately.

184. *See generally* Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. CHI. LEGAL F. 217, 252–58 (1996).

that grew to enormous significance in American life have included the phonograph and subsequent mechanisms for recording sounds, motion pictures, radio, television, cable television, and the Internet. Motion pictures, radio, and television were new-use technologies that were subject to the usual copyright royalty obligations from the start. All have prospered nonetheless. Recorded sound and cable television were not subject to such obligations and have evolved under complex and economically wasteful compulsory license provisions that have long since outlasted any conceivable justification other than the inertia of the status quo. Though anything is possible, one would be hard-pressed to conclude that either of these latter technologies would have suffered a premature death under copyright's usual royalty regime.

Whether one agrees or disagrees with this analysis, at the very least the analysis shows what the relevant inquiry is. In particular, the relevant inquiry is *not* merely looking at the new-use industry and its current financial health alone, without considering the effects on the old use industries, and without taking into account the various possibilities for the new-use industry's future growth. Proper decision making about copyright's application to new-use technologies requires instead an inquiry into the future growth possibilities of the new-use industry and the potential for its negative effect on existing copyright using industries.

VI. CONCLUSION

Copyright law seems never to be caught up with technology, with the result that Congress is under constant pressure to amend the Copyright Act to bring the law up to date with new developments. At first blush, this need for continual amendment is puzzling: Congress expressly tried to make the last major revision of copyright laws, adopted in 1976, flexible enough to handle future technologies without need for frequent changes. A closer look reveals, however, that Congress only solved one of at least four issues that almost invariably arise with new technologies.

Looking back at technological developments over the last century that include photography, piano rolls, phonograph recording, motion pictures, radio, television, cable television, and the Internet, we can see copyright issues emerging in four recognizable patterns: 1) the question of subject matter coverage for new media of fixation; 2) the question of subject matter coverage for new types of works; 3) the question of decentralized infringement; and finally 4) the question of new uses of existing copyrighted works.

We also see a checkered history of courts' and Congress's accommodation to these four issues, with the most success accruing to the first issue, that of new media of fixation. By and large, the current Copyright

Act's focus on intangible "works" as copyright's subject matter reasonably well handles new developments in media of expression such as laser disks or the like.

The other issues remain far more problematic. One of the most intriguing is the last, that of a new technology that creates a new way of using existing copyright works. Frequently, courts and Congress have viewed this new-use issue in the wrong light. By focusing on the industries and technologies prominent at the time the new-use issue first arises, copyright decision makers have tended to assess the royalty obligations of the new-use by examining the new technology's effects on existing uses. Thus in hearings on the 1909 Copyright Act, Congress clung doggedly to the argument that phonograph records would only enhance the "real" market, the market for sheet music.[185] Radio broadcasters in the 1920s argued that radio only enhanced that same market. The Supreme Court in the 1970s was strongly swayed by the view that cable television was merely an enhancement to the "real" market, the market for broadcast television.

In none of these cases did the decision maker focus on the more important question: Will the new-use industry eventually grow to displace today's technologies for exploiting copyrighted material? For if that displacement occurs, then authorial incentives will decline unless offset by a new royalty stream from the new-use technology. Given that no one can predict the future growth of today's technology, copyright decision makers should rely instead on an analysis that looks at this question: How bad could it be if the decision maker guesses wrongly about the growth of a new-use technology? By using the statistical concept of "Type I" and "Type II" errors, this article concludes that, other things being equal, copyright decision makers ought to resolve the issue of copyright royalty obligations arising from uncertainty about the future of a new-use technology by deciding in favor of royalty obligations.

185. *See generally* Copyright Act of 1909, Pub. L. No. 60-349, 35 Stat. 1075 (codified as amended at 17 U.S.C. §§ 101–914 (1994)).

Marc Rohr
Faculty Moderator & Professor of Law – Nova Southeastern University

Professor Marc Rohr has been teaching at the Shepard Broad Law Center of Nova Southeastern University since 1976 (with stints away as a visiting professor at Santa Clara University and the University of San Diego). Professor Rohr received his B.A. from Columbia University in 1968 and his J.D. from Harvard University (where he served as an editor for the law review) in 1971.

Prior to joining the NSU law faculty, Professor Rohr was an associate at a law firm in San Francisco, where he was engaged in commercial litigation. Prior to that experience, he was a staff attorney in both a Legal Services office on the Papago reservation in Arizona and with the Lawyers' Committee for Civil Rights Under Law in Philadelphia.

Professor Rohr has taught primarily in the areas of Copyright & Trademark Law, Constitutional Law, and Civil Procedure. He has written articles dealing primarily with First Amendment matters and procedural questions. His interest in intellectual property, and his concerns about the regulation of freedom of speech, have led him to the world of the Internet.

Can Congress Regulate "Indecent" Speech on the Internet?

Marc Rohr*

TABLE OF CONTENTS

I. INTRODUCTION

In the wake of the invalidation of the heart of the Communications Decency Act ("CDA") by the United States Supreme Court, in the case of *Reno v. American Civil Liberties Union*,[1] is there any way in which Congress can constitutionally limit non-obscene speech on the Internet on the ground that such speech is "indecent," pornographic, or "harmful to minors"?[2]

The CDA provisions which were struck down as violative of the First Amendment essentially made it illegal to use the Internet to knowingly

 The author wishes to thank his Goodwin research assistant, Judy Stroud, for her assistance in the production of this article.

1. 117 S.Ct. 2329 (1997).

2. Even if Congress can constitutionally do so, it may well be that only Congress can do so, because any similar regulation enacted by a state might violate the Commerce Clause, as was held by a federal district court in *American Libraries Ass'n. v. Pataki*, 969 F. Supp. 160, 169 (S.D.N.Y. 1997).

transmit an "indecent" communication to a minor, or to display a "patently offensive" sexual communication "in a manner available to" a minor.[3]

The question that remains is whether Congress can do anything to cure the defects that led to the invalidation of the CDA. In exploring that question, the first part of this article will briefly review the relevant pre-*Reno* precedents at the Supreme Court level. It will then proceed to an analysis of the Supreme Court ruling in *Reno*, as well as a brief consideration of the two lower court decisions[4] that held the CDA invalid prior to the Supreme Court ruling. Finally, this article will consider, in light of those rulings, the constitutionality of the recently enacted Child Online Protection Act.[5]

II. THE RELEVANT PRE-*RENO* PRECEDENTS

Beginning in the early 1970s, the Supreme Court developed the general rules governing the validity of regulations of speech under the First Amendment. In the absence of a special rule applicable to the kind of regulation at issue, the Court typically asks whether a regulation of speech is content based or content neutral, and, if it is content based, the Court scrutinizes the regulation strictly, requiring the government to employ means narrowly tailored to accomplish a government interest of compelling magnitude.[6] The regulation must be necessary to the achievement of the important goal,[7] and it must represent the least restrictive means of doing

3. *See infra* text accompanying note 69.

4. ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997); Shea v. Reno, 930 F. Supp. 916 (S.D.N.Y. 1996), *aff'd*, 117 S. Ct. 2501 (1997).

5. Pub. L. No. 105-277, 112 Stat. 2681 (to be codified at 47 U.S.C. § 223 (1998)). Freedom of speech issues involving the Internet have also arisen in other contexts, which are beyond the scope of this article. Those contexts include: state regulations, *see* ACLU v. Johnson, 4 F. Supp. 2d 1029 (D.N.M. 1998); Urofsky v. Allen, 995 F. Supp. 634 (E.D. Va. 1998); American Libraries Ass'n v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997); ACLU v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997); university policies, *see* Loving v. Boren, 133 F.3d 771 (10th Cir. 1998); county library policies, *see* Mainstream Loudoun v. Board of Trustees, 24 F. Supp. 2d 552 (E.D. Va. 1998); city web site limitations, *see* Putnam Pit, Inc. v. City of Cookeville, 23 F. Supp. 2d 822 (M.D. Tenn. 1998); other aspects of the Communications Decency Act, *see* Apollomedia Corp. v. Reno, 19 F. Supp. 2d 1081 (N.D. Cal. 1998); federal obscenity laws, *see* United States v. Thomas, 74 F.3d 701 (6th Cir. 1996); and the Federal Child Pornography Prevention Act, *see* Free Speech Coalition v. Reno, No. C 97-0281VSC, 1997 WL 487758 (N.D. Cal. 1997). See also S.B. 97, 106th Cong. (1998) and H.R. Res. 368, 106th Cong. (1999), which would require blocking and filtering of Internet access via computers in public schools and libraries.

6. Burson v. Freeman, 504 U.S. 191 (1992); Simon & Schuster, Inc. v. New York State Crime Victims Bd., 502 U.S. 105 (1991).

7. R.A.V. v. City of St. Paul, 505 U.S. 377 (1992).

so.[8] While the point is not clearly established, there is also some basis in the case law for contending that to survive this level of judicial scrutiny, a regulation must be effective in achieving its goal.[9] Because the CDA was undeniably a content based regulation of speech, "strict scrutiny" was in fact used by the Court in *Reno.*[10]

But some special rules, and some other important general principles, had been established prior to the emergence of those general rules pertaining to content based regulations of speech. In 1957, the Court held that "obscenity," properly defined, was entitled to no constitutional protection,[11] a position to which it has adhered ever since.[12] At about the same time, in a case called *Butler v. Michigan,*[13] the Court ruled that a state could not completely prohibit the distribution of literature deemed harmful only to minors, because it would have the effect of reducing the adult population to reading only that which was fit for children to read.[14] That proposition, stated at a time prior to the Court's development of the great bulk of the rules that govern free speech cases today, was put forth as an independent principle, and was apparently *the* basis for the result in *Butler.* In 1968, in contrast, in a case called *Ginsberg v. New York,*[15] the Court upheld a state statute that prohibited the sale of certain materials—defined as obscene *as to minors—only* to minors;[16] thus, the principle of *Butler* was not violated.[17]

A general principle that appears to be well established, first articulated in the 1971 decision in *Cohen v. California*[18] and reaffirmed by later rulings,[19] is that government may not suppress speech simply because

8. Sable Communications v. FCC, 492 U.S. 115 (1989).

9. See *Turner Broad. Sys., Inc. v. FCC,* 512 U.S. 622, 664 (1994), which borrows oft-quoted language to that effect from a commercial speech case, *Edenfield v. Fane,* 507 U.S. 761, 770–71 (1993). Since commercial speech is said to receive less protection than non-commercial speech, it follows logically that strict scrutiny must be understood as requiring at least as persuasive a justification for limiting non-commercial speech as is required in the case of a regulation of commercial speech. See also *Shaw v. Hunt,* 517 U.S. 899, 915–16 (1996), to the same effect, but applying strict scrutiny in the context of an Equal Protection Clause challenge.

10. *See infra* text accompanying note 54.

11. Roth v. United States, 354 U.S. 476 (1957).

12. *See* Miller v. California, 413 U.S. 15 (1973); Pope v. Illinois, 481 U.S. 497 (1987).

13. 352 U.S. 380 (1957).

14. *Id.* at 383.

15. 390 U.S. 629 (1968).

16. *Id.* at 639.

17. *Id.* at 643.

18. 403 U.S. 15 (1971).

19. Texas v. Johnson, 491 U.S. 397 (1989); Hustler Magazine v. Falwell, 485 U.S. 46 (1988); Erznoznik v. City of Jacksonville, 422 U.S. 205 (1975).

unwilling viewers or listeners may be offended thereby.[20] The Court has never explicitly stated that the government interest in shielding unwilling listeners from offensive speech fails to rise to the level of magnitude required of a content based regulation of speech. Instead, the Court has said, in effect, that we are inescapably subject to speech that offends us, outside the privacy of our homes, and that we are obliged to "[avert] our eyes" in such situations, at least when doing so is a feasible response to the offensive stimulus.[21] The Court has also recognized the difficulty of drawing workable lines when one begins to contemplate regulating speech according to its offensiveness or "outrageousness."[22]

But *FCC v. Pacifica Foundation*,[23] decided in 1978, was a special case, and the government's victory therein predictably encouraged the government to engage in further attempts to regulate in the name of protecting children from "indecent" speech.[24] *Pacifica* involved the famous George Carlin monologue, which a radio station broadcast at midday, concerning the "seven 'dirty words'"[25] that one could not say on radio or television. The station was consequently sanctioned by the FCC, acting pursuant to a federal statute which allowed the FCC to prohibit "obscene" or "indecent" speech on radio or television.[26] The Supreme Court, explicitly focusing only on the FCC's application of the law to this radio station in this instance, upheld the FCC's action, placing great weight on the facts that (a) radio broadcasts come into the home; and (b) children are in the audience.[27] The majority strongly implied that the time of day of the broadcast made a difference.[28] Although the Court appeared to recognize the FCC's action as based on the content of speech, references to strict judicial scrutiny were nowhere to be seen. In upholding the FCC's action, moreover, the Court devoted no time or energy to the constitutionality of the governing statute, which, again, prohibited "indecent" speech over the public airwaves. "Indecency," it is important to note, has never been a legal term of art, like obscenity, embodying an established meaning.

It has become a familiar, if somewhat fuzzy, tenet of First Amendment law that broadcasting receives less than the usual amount of First Amendment protection,[29] a maxim that provided some support for the

20. *Cohen*, 403 U.S. at 21.
21. *Id.*
22. *Id.* at 25; *Hustler*, 485 U.S. at 55.
23. 438 U.S. 726 (1978).
24. *Id.* at 738.
25. *Id.* at 770.
26. *Id.* at. 731 (citing 18 U.S.C. § 1464 (1976)).
27. *Id.* at 763–64 (Brennan, J., dissenting).
28. *Pacifica*, 438 U.S. at 750.
29. *See, e.g.*, Red Lion Broad. Co., v. FCC, 395 U.S. 367 (1969).

holding in *Pacifica*. Partly for that reason, *Pacifica* has proven to be fairly easy to distinguish from later cases involving different media of communication. When government has sought to protect minors from ostensibly harmful communications via mail[30] or telephone,[31] for example, *Pacifica* has been distinguished—mail, because its impact on small children was seen as so much smaller,[32] and "dial-a-porn" telephone communications, because they do not come into the home in an unsought and unexpected manner.[33]

The 1989 "dial-a-porn" decision, *Sable Communications v. FCC*,[34] is significant for another reason as well—namely the Court's use of strict scrutiny, which by 1989 had become a fairly dependable judicial response to a content based regulation of speech. Again, a well-established component of strict scrutiny is the insistence that the government employ the least restrictive means of regulating the targeted speech. In *Sable*, the Court recognized a compelling interest on the part of the government in protecting children from emotionally harmful communications,[35] and appeared willing to believe that the pornographic telephone conversations in question might be harmful. But, because there was evidence in the record of alternative methods of shielding children from these pornographic messages, the Court was not persuaded that a total ban represented the least restrictive means of doing so.[36] The principle of the *Butler* case, meanwhile, was again set forth.[37]

With respect to cable television, it appeared for nearly a decade that the Supreme Court perceived that medium as differing significantly from broadcast television,[38] but in a more recent opinion a plurality of the Court emphasized the similarities of those two media.[39] In that case, which involved federal regulation of "indecency" on cable television, a plurality of the court declined to employ strict scrutiny, despite the clearly content based nature of the regulation, because of uncertainty as to the appropriate

30. Bolger v. Youngs Drug Prod. Corp., 463 U.S. 60 (1983).

31. Sable Communications v. FCC, 492 U.S. 115 (1989).

32. *Bolger*, 463 U.S. at 74.

33. *Sable*, 492 U.S. at 128.

34. 492 U.S. 115 (1989).

35. *Id.* at 122. *See also* Denver Area Educ. Telecomm. Consortium, Inc. v. FCC, 518 U.S. 727, 755 (1996) (plurality opinion); *id.* at 806 (Kennedy, J., concurring in part).

36. *Sable*, 492 U:S. at 128–29.

37. *Id.* at 126–27.

38. Wikinson v. Jones, 480 U.S. 926 (1987), *aff'g* Jones v. Wilkinson, 800 F.2d 989 (10th Cir. 1986), *aff'g* Community Televison v. Wilkinson, 611 F. Supp. 1099 (D. Utah 1985).

39. *Denver Area Educ. Telecomm. Consortium*, 518 U.S. 727.

standards to apply to a medium of communication seen as new and unique.[40] The dissenters on this point, constituting a majority of the Justices, would have employed strict scrutiny.[41] A demanding level of judicial review was utilized nonetheless, but the possibility that the Court would depart from its general analytical framework, by virtue of the special nature of the medium of communication at issue, had arisen.

III. THE STATUTE

The two statutory provisions at issue, to be codified as sections 223(a) and (d) of Title 47,[42] came to be known as the "indecent transmission" provision and the "patently offensive display" provision.[43]

The "indecent transmission" provision, section 223(a), made it a federal crime, *inter alia,* to do the following acts, "knowingly," "in interstate or foreign communications," "by means of a telecommunications device": to create and initiate the transmission of any communication "which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age."[44]

The "patently offensive" display provision, section 223(d), made it a federal crime, *inter alia,* to do either of the following, "knowingly," "in interstate or foreign communications," by use of an interactive computer service:

> to send to a specific person or persons under 18 years of age, or . . . to display in a manner available to a person under 18 years of age, "any . . . communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs . . . ."[45]

Significantly, two affirmative defenses were provided by the statute, in section 223(e)(5), precluding conviction of a defendant who

> "(A) has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent

40. *Id.* at 741–42.

41. *Id.* at 783 (Kennedy, J., concurring and dissenting in part). *See also id.* at 832 (Thomas, J., dissenting in part).

42. Child Online Protection Act, Pub. L. No. 105-277, 112 Stat. 2681 (to be codified at 47 U.S.C. § 223(a), (d) (1998)).

43. *Reno*, 117 S. Ct. 2329, 2338 (1997).

44. *Id.* at 2338 (citing 47 U.S.C.A. § 223(a) (Supp. 1997)).

45. *See id.* at 2338–39 (citing 47 U.S.C.A. § 223(d) (Supp. 1997)).

> access by minors to a [prohibited] communication . . . which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology; [sic] or
>
> "(B) has restricted access to such communication by requiring use of a verified credit card . . . or adult personal identification number."[46]

IV. THE JUDICIAL REACTION TO THE CDA

A. *The Supreme Court Decision in* Reno

1. The Majority Opinion

Justice Stevens wrote the opinion for a majority of seven Justices, affirming the decision of a three-judge District Court,[47] invalidating these provisions, except to the extent that section 223(a) bars "obscene" communications.[48]

In the first three sections of his opinion, Stevens summarized the district court's extensive findings of fact pertaining to sexually explicit material on the Internet and available mechanisms for restricting access thereto,[49] described the statute and the history of its enactment,[50] and briefly described the reasoning of the lower court.[51]

a. *Key Findings of Fact*

Some of the District Court's important findings of fact, restated in Part I of Justice Stevens' opinion, deserve restatement at this point.

Concerning sexually explicit material on the Internet, Stevens, quoting in part from the findings below, wrote:

> Though such material is widely available, users seldom encounter such content accidentally. . . . Almost all sexually explicit images are preceded by warnings as to the content. For that reason, "odds

46. *Id.* at 2339 n.26.
47. *ACLU*, 929 F. Supp. 824, 849 (E.D. Pa. 1996).
48. *Reno*, 117 S. Ct. at 2350.
49. *Id.* at 2334–37.
50. *Id.* at 2337–39.
51. *Id.* at 2339–41.

> are slim" that a user would enter a sexually explicit site by accident. Unlike communications received by radio or television, "the receipt of information on the Internet requires a series of affirmative steps more deliberate and directed than merely turning a dial. A child requires some sophistication and some ability to read to retrieve material and thereby to use the Internet unattended."[52]

Concerning age verification, again quoting in part from the findings below, he wrote this:

> The District Court categorically determined that there "is no effective way to determine the identity or the age of a user who is accessing material through e-mail, mail exploders, newsgroups or chat rooms." The Government offered no evidence that there was a reliable way to screen recipients and participants in such fora for age.
>
> . . .
>
> Technology exists by which an operator of a Web site may condition access on the verification of requested information such as a credit card number or an adult password. Credit card verification is only feasible, however, either in connection with a commercial transaction. . . . For that reason, . . . credit card verification was "effectively unavailable to a substantial number of Internet content providers." . . . Moreover, the imposition of such a requirement "would completely bar adults who do not have a credit card and lack the resources to obtain one from accessing any blocked material."
>
> . . . [T]he District Court found that an adult password requirement would impose significant burdens on noncommercial sites, both because they would discourage users from accessing their sites and because the cost of creating and maintaining such screening systems would be "beyond their reach."
>
> . . .
>
> "Even if credit card verification or adult password verification were implemented, the Government presented no testimony as to

52. *Id.* at 2336 (quoting *ACLU*, 929 F. Supp. 824, 844–45 (E.D. Pa. 1996)).

> how such systems could ensure that the user of the password or credit card is in fact over 18. The burdens imposed by credit card verification and adult password verification systems make them effectively unavailable to a substantial number of Internet content providers."[53]

b. *Legal Analysis*

Justice Stevens began his analysis of the constitutionality of the CDA in Part IV of his opinion. However, instead of beginning by identifying the statute as content based, and therefore subject to strict scrutiny, he began by addressing the government's argument "that the CDA is plainly constitutional under three of our prior decisions,"[54] *Ginsberg v. New York*,[55] *FCC v. Pacifica Foundation*,[56] and a clearly inapplicable case, *City of Renton v. Playtime Theatres, Inc.*[57]

Stevens distinguished *Ginsberg* on several grounds, including: 1) *Ginsberg* involved a law that barred sales to minors, but not to adults;[58] 2) "the New York statute applied only to commercial transactions[;]"[59] and 3) the forbidden material in *Ginsberg*, unlike the material prohibited under the CDA, was defined in part by the absence of "serious literary, artistic, political, or scientific value."[60]

Pacifica was distinguishable on a variety of grounds as well, including the observation—foreshadowed by Stevens' summary of the district court's findings of fact—that, in contrast to the radio broadcast in *Pacifica*, "the risk of encountering indecent material [on the Internet] by accident is remote because a series of affirmative steps is required to access specific material."[61]

In Part V of his opinion, Stevens considered, in essence, whether the constitutional analysis in the case should be affected by the nature of the

---

53. *Reno*, 117 S. Ct. at 2336–37 (quoting *ACLU*, 929 F. Supp. 824, 844–47 (E.D. Pa. 1996)).

54. *Id.* at 2341.

55. 390 U.S. 629 (1968).

56. 438 U.S. 726 (1978).

57. 475 U.S. 41 (1986). The Court in *Playtime Theatres, Inc.* divined a theory which allowed it to treat what appeared to be a content based regulation of speech as if it were content neutral. *Id.* at 47–49. By contrast, said Stevens, quite accurately, "the CDA is a content-based blanket restriction on speech." *Reno*, 117 S. Ct. at 2342.

58. *Id.* at 2341.

59. *Id.* (citing Ginsberg v. New York, 390 U.S. 629, 647 (1968)).

60. *Id.*

61. *Id.* at 2342.

communications medium involved.[62] The primary point of comparison, of course, was broadcasting, long deemed to be subject to greater regulation because of the "scarcity of available frequencies" and the "invasive nature" of radio and television.[63] "Those factors are not present in cyberspace,"[64] wrote Stevens, who went on to conclude there was "no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium."[65]

In Part VI of his opinion, Stevens toyed with the arguable vagueness of the statutory provisions at issue, but stopped short of relying on that vagueness as a basis, under the Due Process Clause of the Fifth Amendment, for invalidating the statute.[66] He began by noting the "ambiguities" in the challenged provisions—namely, the word "indecent" and the phrase "patently offensive."[67] In the discussion that followed, he actually seemed to have regarded these words as "vague," yet, again, did not rest his decision on that basis.[68] Notably, he devoted little time to the word "indecent," focusing instead on the phrase "patently offensive," and rejecting the government's contention that that phrase could not be unconstitutionally vague because it constitutes one part of the Court's own three-part definition of unprotected "obscenity."[69]

But if the vagueness of these terms was not reason, in and of itself, to strike down the CDA, what was the significance of these observations? Early in this discussion, referring to the "uncertainty" that the CDA would create, Stevens stated that "[t]his uncertainty undermines the likelihood that the CDA has been carefully tailored to the congressional goal of protecting minors from potentially harmful materials."[70] For this proposition he cited no precedent, and, indeed, this author can think of no prior decision that made this kind of connection between the problem of vagueness and the requirement, under strict scrutiny, that a law be narrowly tailored to accomplish the legislative goal. At the end of this section of his opinion, Stevens said:

---

62. *Reno*, 117 S. Ct. at 2343.

63. *Id.*

64. *Id.*

65. *Id.* at 2344.

66. *Id.* "Regardless of whether the CDA is so vague that it violates the Fifth Amendment," he wrote, "the many ambiguities concerning the scope of its coverage render it problematic for purposes of the First Amendment." *Reno*, 117 S. Ct. at 2344.

67. *Id.*

68. *Id.* at 2344–48.

69. *Id.* at 2345 (discussing Miller v. California, 413 U.S. 15 (1973)).

70. *Id.* at 2344.

> Given the vague contours of the coverage of the statute, it unquestionably silences some speakers whose messages would be entitled to constitutional protection. That danger provides further reason for insisting that the statute not be overly broad. The CDA's burden on protected speech cannot be justified if it could be avoided by a more carefully drafted statute.[71]

But one would have expected the Court to have endorsed the latter proposition in any event, and to have "insist[ed] that the statute not be overly broad" regardless of any problems of vagueness.[72] Arguably, then, this discussion of vagueness contributed nothing to the Court's resolution of the case. But it suggests that the terminology at issue, if used in future legislation, might be deemed intolerably vague, even if Congress somehow found a way to overcome the defects that did lead the Court to invalidate the CDA.

Part VII of Justice Stevens' opinion contained the heart of his strict scrutiny analysis, and it is to this part of his opinion that one must look to determine, as best one can, precisely what was wrong, constitutionally, with the CDA.

"[W]e have repeatedly recognized," he wrote, "the governmental interest in protecting children from harmful materials."[73] That apparently meant that the government's goal was of sufficient importance to satisfy strict scrutiny; Stevens didn't say that explicitly, but the Court had previously so stated.[74]

The problem, then, in general terms, was that the statute was not sufficiently narrowly tailored to survive strict scrutiny. But why not? Here are the key passages from this part of Stevens' opinion:

> In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another. That burden on adult speech is unacceptable if less restrictive

---

71. *Id.* at 2346.

72. *Reno*, 117 S. Ct. at 2346.

73. *Id.*

74. Sable Communications v. FCC, 492 U.S. 115, 126 (1989). *See also* text accompanying notes 8, 35. Precisely what harm would likely befall children as a result of exposure to non-obscene sexually explicit materials has never been identified by the Supreme Court. But see the discussion of this point in the Report of the House Committee on Commerce on the Child Online Protection Act, H.R. REP. NO. 105-775 (1998), 1998 WL 691067 at 27–28.

> alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.[75]

The government interest in protecting children, he continued, "does not justify an unnecessarily broad suppression of speech addressed to adults. As we have explained, the Government may not '[reduce] the adult population . . . to . . . only what is fit for children.'"[76]

The last sentence quoted represents, of course, the principle of the *Butler* case. But the preceding sentences appear, in and of themselves, to treat the *Butler* principle as something other than absolute; the burden on adult speech, it is said, is unacceptable *if* less restrictive alternatives would do the job as well. Because, under strict scrutiny, *any* burden on speech is unacceptable if less restrictive alternatives would do the job as well, the reference to the *Butler* principle arguably becomes superfluous.

At this point Stevens detoured slightly from his statement of governing principles, taking time to explain why communication between adults was burdened by the CDA:

> Given the size of the potential audience for most messages, in the absence of a viable age verification process, the sender must be charged with knowing that one or more minors will likely view it. Knowledge that, for instance, one or more members of a 100—person chat group will be minor—and therefore that it would be a crime to send the group an indecent message—would surely burden communication among adults.[77]

As noted previously, the district court had found that existing technology did not include any effective method for a sender to prevent minors from obtaining access to its Internet communications without also denying access to adults, and that the use of age verification devices would prove quite burdensome for many speakers.[78] Thus, the CDA would significantly burden adult communication on the Internet.[79]

Stevens continued, in characteristically unstructured fashion:

---

75. *Reno*, 117 S. Ct. at 2346.

76. *Id.* (quoting Sable Communications v. FCC, 492 U.S. 115, 128 (1989)).

77. *Id.* at 2347.

78. *Id.* at 2336–37.

79. At that point, Stevens added this: "By contrast, the District Court found that . . . currently available *user-based* software suggests that a reasonably effective method by which parents can prevent their children accessing sexually explicit . . . material . . . will soon be widely available." *Id.* at 2347 (quoting *ACLU*, 929 F. Supp. 824, 842 (E.D. Pa. 1996)). The legal relevance of that observation is far from clear.

> The breadth of the CDA's coverage is wholly unprecedented. . . . [T]he scope of the CDA is not limited to commercial speech or commercial entities. . . .The general, undefined terms "indecent" and "patently offensive" cover large amounts of nonpornographic material with serious educational or other value. Moreover, the "community standards" criterion . . . means that any communication available to a nationwide audience will be judged by the standards of the community most likely to be offended by the message.[80]

The regulated subject matter, he went on to say, might "extend to discussions about prison rape or safe sexual practices, artistic images that include nude subjects, and arguably the card catalogue of the Carnegie Library."[81]

Stevens then invoked the government's argument that, in effect, the First Amendment surely does not protect the communication of all "indecent" or "patently offensive" messages to minors, regardless of whether the message contains "value."[82] The Court "need neither accept nor reject" that argument, said Stevens.[83] "It is at least clear," he continued, "that the strength of the Government's interest in protecting minors is not equally strong throughout the coverage of this broad statute."[84] He hypothesized further at this point: "[A] parent who sent his 17-year-old college freshman information on birth control via e-mail could be incarcerated even though neither he, his child, nor anyone in their home community, found the material 'indecent' or 'patently offensive', if the college town's community thought otherwise."[85]

Was the problem, then, that Congress had gone too far by shielding minors even from sex-related communication that contained serious artistic or educational value? Was the law overinclusive, to that extent, because such material does not give rise to the harms that Congress has a compelling interest in preventing? If that is what Justice Stevens was thinking, he did not say it.

Was there a particular constitutional infirmity stemming from the fact that "indecency" might be determined through the prism of the "community standards" of a distant, or nationwide, "community?" Stevens didn't say

80. *Reno*, 117 S. Ct. at 2347.
81. *Id.* at 2348.
82. *Id.*
83. *Id.*
84. *Id.*
85. *Reno*, 117 S. Ct. at 2348.

that, either, nor has case law in the obscenity context suggested that such an approach raises constitutional problems.[86]

Instead of expressly basing the Court's ruling on any or all of those concerns, Stevens concluded this key section of his opinion with the following paragraph:

> The breadth of this content based restriction of speech imposes an especially heavy burden on the Government to explain why a less restrictive provision would not be as effective as the CDA. It has not done so. The arguments in this Court have referred to possible alternatives such as requiring that indecent material be "tagged" in a way that facilitates parental control of material coming into their homes, making exceptions for messages with artistic or educational value, providing some tolerance for parental choice, and regulating some portions of the Internet—such as commercial web sites—differently than others, such as chat rooms.[87]

Was Stevens saying here that less restrictive alternatives existed? Or merely that "*possible* alternatives" existed, which is to say that the existence of such alternatives was possible, but not certain? If the latter, was the constitutional infirmity a procedural problem of sorts—namely, that the government had simply not satisfied its burden of *proving* that no less restrictive alternatives existed? If so, was that a fair conclusion? Did any such less restrictive alternatives exist? Did Stevens identify any, in the language just quoted? Bearing in mind that a less restrictive alternative must be employed when it will accomplish the government's goal at least as well as the challenged regulation, can that be said of the "tagging" alternative to which Stevens referred?[88] Of the other "possible alternatives" he cited, how could it be said that: (a) "making exceptions for messages with artistic or educational value;"[89] or (b) regulating only "commercial" web sites,[90] would fully achieve the government's goal?

The final sentence of this apparently dispositive paragraph was this: "Particularly in the light of the absence of any detailed findings by the Congress, or even hearings addressing the special problems of the CDA, we are persuaded that the CDA is not narrowly tailored if that requirement has any meaning at all."[91] A failure by Congress to utilize less restrictive

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

87. *Reno*, 117 S. Ct. at 2348.

88. *See* Butler v. Michigan, 352 U.S. 380 (1957); *infra* comments in note 129 and accompanying text.

89. *Reno*, 117 S. Ct. at 2348.

90. *Id.*

91. *Id.*

available alternatives would lead to the conclusion that the statute was not sufficiently narrowly tailored, which in turn would render the statute unconstitutional. But why the sudden and unexpected reference to the absence of Congressional findings or hearings?[92] Is Congress obliged to make findings, or to hold hearings, when it legislates in a manner that affects freedom of expression, or was the apparently hasty and spontaneous nature of the enactment of this statute simply an aggravating factor in the minds of the Justices?[93]

In Part IX of his opinion, Justice Stevens responded to, and rejected, the government's argument that the statute was constitutional by virtue of the affirmative defenses provided therein:

> First, relying on the "good faith, reasonable, effective and appropriate actions" provision, the Government suggests that "tagging" provides a defense that saves the constitutionality of the Act. The suggestion assumes that transmitters may encode their indecent communications in a way that would indicate their contents, thus permitting recipients to block their reception with appropriate software. It is the requirement that the good faith action must be "effective" that makes this defense illusory. The Government recognizes that its proposed screening software does not currently exist. Even if it did, there is no way to know whether a potential recipient will actually block the encoded material. Without the impossible knowledge that every guardian in America is screening for the "tag," the transmitter could not reasonably rely on its action to be "effective."[94]

As to the other affirmative defense, applicable when a transmitter restricts access by requiring the use of a verified credit card or adult identification, Stevens returned to the finding of the district court that "it is not economically feasible for most noncommercial speakers to employ such verification" techniques; "[a]ccordingly, this defense would not significantly narrow the statute's burden on noncommercial speech."[95] Additionally, the government "failed to adduce any evidence that these verification techniques

92. Earlier in his opinion, Justice Stevens briefly described the process by which the CDA had been enacted, observing that "[n]o hearings were held on the provisions that became law." *Id.* at 2338 n.24.

93. See *United States v. Lopez*, 514 U.S. 549, 549 (1995), in which Chief Justice Rehnquist, writing for the majority, commented on the absence of congressional findings, in the course of striking down a federal statute on the ground that the subject of the regulation did not have a substantial effect on interstate commerce. *Id.*

94. *Reno*, 117 S. Ct. at 2349.

95. *Id.*

actually preclude minors from posing as adults."[96] Thus, an "unacceptably heavy burden" on adult speech remained, and "the defenses do not constitute the sort of "narrowly tailoring" that will save an otherwise patently invalid unconstitutional provision."[97] But did not Justice Stevens' pronouncements concerning the inefficacy of these defenses tend to discredit his earlier suggestion that Congress had not employed the least restrictive means of achieving its goals?

2. The Concurring Opinion

The only other opinion written by any of the Justices in this case was that written by Justice O'Connor, joined by Chief Justice Rehnquist, partly dissenting and partly concurring in the judgment.[98] O'Connor began by stating that she viewed the CDA "as little more than an attempt by Congress to create 'adult zones' on the Internet."[99] She then proceeded to set down the following governing principles (which apparently exist, for her, outside of any structured strict-scrutiny analysis):

> The Court has previously sustained such zoning laws, but only if they respect the First Amendment rights of adults and minors. That is to say, a zoning law is valid if (i) it does not unduly restrict adult access to the material; and (ii) minors have no First Amendment right to read or view the banned material.[100]

For this proposition she relied on the holdings in *Butler v. Michigan*,[101] *Sable Communications v. FCC*,[102] and *Bolger v. Youngs Drug Products Corp*,[103] and distinguished *Ginsberg v. New York*,[104] which upheld a statute that in no way curtailed adult access to sexually explicit material.[105]

---

96. *Id.*
97. *Id.* at 2350.
98. *Id.* at 2351 (O'Connor, J., concurring in part, dissenting in part). O'Connor's partial dissent was based on her view that the "indecen[t] transmission" provision and the "specific person" provision were constitutional, to the extent that they applied to Internet communications "where the party initiating the communication knows that all of the recipients are minors." *Reno*, 117 S. Ct. at 2356 (O'Connor, J., concurring in part, dissenting in part).
99. *Id.* at 2351.
100. *Id.* at 2352–53.
101. 352 U.S. 380 (1957).
102. 492 U.S. 115 (1989).
103. 463 U.S. 60 (1983).
104. 390 U.S. 629 (1968).
105. *Id.* at 673–75.

O'Connor then ruminated a bit on the nature of "zoning" in cyberspace—via "gateway technology," (*e.g.*, screening software)—and ultimately concluded: "Gateway technology is not ubiquitous in cyberspace, and because without it 'there is no means of age verification,' cyberspace still remains largely unzoned—and unzoneable."[106] "Although the prospects for the eventual zoning of the Internet appear promising," she continued, "we must evaluate the constitutionality of the CDA as it applies to the Internet as it exists today."[107] Given present conditions, she concluded, the "display" provision was unconstitutional, because its prohibition would "[impinge] on the First Amendment right of adults to make and obtain this speech and, for all intents and purposes, '[reduce] the adult population [on the Internet] to reading only what is fit for children.'[108] . . . As a result, the 'display' provision cannot withstand scrutiny."[109] For her, then, it appears that the *Butler* principle controlled, independently of any other mode of First Amendment analysis.

Returning to her two-part inquiry, stated above, O'Connor then considered "[w]hether the CDA substantially interferes with the First Amendment rights of minors."[110] Her response was that it did not, but that was because of the established rule that, for a statute to be stricken as facially overbroad under the First Amendment, it had to be *substantially* overbroad.[111] She did not deem the CDA to be substantially overbroad, but did seem to think that it did violate the First Amendment rights of minors in some of its applications.[112] In this analysis she was guided by the case of *Ginsberg v. New York*,[113] which "established that minors may constitutionally be denied access to material that is obscene as to minors."[114] She explained:

> Because the CDA denies minors the right to obtain material that is "patently offensive"—even if it has some redeeming value for minors and even if it does not appeal to their prurient interests—Congress' rejection of the Ginsberg "harmful to minors" standard

106. *Reno*, 117 S. Ct. at 2354 (O'Connor, J., concurring in part, dissenting in part) (quoting *ACLU*, 929 F. Supp. 824, 846 (E.D. Pa. 1996)).

107. *Id.* (O'Connor, J., concurring in part, dissenting in part).

108. *Id.*

109. *Id.* (quoting Butler v. Michigan, 352 U.S. 380, 383 (1957)).

110. *Id.* (quoting Broadrick v. Oklahoma, 413 U.S. 601, 615 (1973)).

111. *Reno*, 117 S. Ct. at 2356 (O'Connor, J., concurring in part, dissenting in part).

112. *Id.*

113. 390 U.S. 629 (1968).

114. *Reno*, 117 S. Ct. at 2356 (O'Connor, J., concurring in part, dissenting in part).

> means that the CDA could ban some speech that is 'indecent' (i.e., "patently offensive") but that is not obscene as to minors."[115]

But, again, the CDA was not, in her view, *substantially* overbroad in this regard: "In my view, the universe of speech constitutionally protected as to minors but banned by the CDA—i.e., the universe of material that is 'patently offensive,' but which nonetheless has some redeeming value for minors or does not appeal to their prurient interest—is a very small one."[116]

While this discussion did not affect the way in which these two Justices would have disposed of this case, it did reveal their belief that even minors have a First Amendment right to offensive, sexually explicit material when that material "has some redeeming value for minors."[117] If other Justices were to join them in taking this position (as seems likely, considering that O'Connor was joined in this opinion by Chief Justice Rehnquist), it would serve as an additional limitation on the ability of Congress to regulate speech deemed harmful to minors.

B. *The Lower Court Decisions*

1. ACLU v. Reno

While it is the Supreme Court decision that counts, the opinions written by each of the judges of the special three-judge court that initially decided the case of *ACLU v. Reno*,[118] may nonetheless shed additional light on the possible judicial response to any future variations of the CDA that may emerge from Congress. Those opinions foreshadowed Justice Stevens' reasoning to a considerable extent, but contained some additional analytical reactions to the CDA that were not addressed, and certainly not discredited, by the Supreme Court decision. Thus, even if Congress could cure every defect identified by Justice Stevens, a new statutory regulation of Internet speech might yet run afoul of a principle put forth in one of these three

115. *Id.*

116. *Id.* Justice O'Connor clarified the role of "value" in this context, as follows: minors do not enjoy a right to all material having "value," rather, "under *Ginsberg*, minors only have a First Amendment right to obtain patently offensive material that has 'redeeming social importance *for minors.*'" *Id.* (quoting Ginsberg v. New York, 390 U.S. 629, 633 (1968)).

117. *Id.*

118. 929 F. Supp. 824 (E.D. Pa. 1996). Following an introduction, findings of fact, and a brief statement of conclusions of law, each of the three judges wrote an opinion representing only his own views. *Id.* at 824.

opinions. Those additional bases for striking down the CDA should thus be explored.

Chief Judge Sloviter took a bit of time questioning whether the government had a compelling interest "in regulating the vast range of online material covered or potentially covered by the CDA"[119]—in other words, whether the government truly had a compelling interest with respect to the full range of the CDA's potential applications.[120] This approach appears to confuse the question of whether the government's goal is one of compelling importance with the separate question of whether the statute is narrowly tailored to accomplish that goal. Still, a distinguished federal judge made this argument, although he disclaimed reliance upon it in striking down the statute.[121]

In addition, Judge Sloviter made observations that, in effect, give substance to an argument, though not explicitly offered as such, that the CDA was not *necessary* to achieve the government's purposes:

> Minors would not be left without any protection from exposure to patently unsuitable material on the Internet should the challenged provisions of the CDA be preliminarily enjoined. Vigorous enforcement of current obscenity and child pornography laws should suffice to address the problem the government identified in court and which concerned Congress. When the CDA was under consideration by Congress, the Justice Department itself communicated its view that it was not necessary because it was prosecuting online obscenity, child pornography and child solicitation under existing laws, and would continue to do so.[122]

---

119. *Id.* at 853 (Sloviter, C.J.).

120. Chief Judge Sloviter concluded, for example, that "where non-pornographic, albeit sexually explicit, material also falls within the sweep of the statute, the interest will not be as compelling." *Id.* at 852 (Sloviter, C.J.).

121. This point found fleeting expression in Justice Stevens' opinion as well, when he remarked that "the strength of the Government's interest in protecting minors is not equally strong throughout the coverage of this broad statute." *Reno*, 117 S. Ct. at 2348.

122. *ACLU*, 929 F. Supp. at 856–57 (Sloviter, C.J.). The existence and applicability of federal obscenity and child pornography laws were noted by Justice Stevens only in a footnote, accompanied by the observation that "when Congress was considering the CDA, the Government expressed its view that the law was unnecessary because existing laws already authorized its ongoing efforts to prosecute obscenity, child pornography, and child solicitation." *Reno*, 117 S. Ct. at 2347 n. 44. *See* 18 U.S.C.A. §§ 1464–65, 2251, 2422(b) (West Supp. 1998).

Judge Buckwalter, writing separately, concluded that the words "indecent" and "patently offensive" were unconstitutionally vague.[123] With respect to the word "indecent," he did not regard the United States Supreme Court's decision in *Pacifica* as having precluded such an argument.[124] He was troubled, as well, by the ambiguity attendant upon the statutory reference to "community standards."[125]

Judge Dalzell, the third member of the court, concluded his lengthy opinion with this observation, bearing upon the inevitable ineffectuality of the congressional act: "Moreover, the CDA will almost certainly fail to accomplish the Government's interest in shielding children from pornography on the Internet. Nearly half of Internet communications originate outside the United States, and some percentage of that figure represents pornography."[126]

2. Shea v. Reno

In *Shea v. Reno*,[127] the other 1996 decision of a three-judge court striking down the CDA, the court, whose holding was based on reasoning that anticipated that of Justice Stevens to a great extent, made a comment similar to that made by Judge Dalzell regarding the likely ineffectiveness of the statute:

> It is . . . unnecessary, given our holding . . ., to decide whether the potential ineffectiveness of the CDA in eradicating the problem of minors' having access to sexually explicit material on the Internet renders the statute constitutionally defective. Because the CDA only regulates content providers within the United States, while perhaps as much as thirty percent of the sexually explicit material on the Internet originates abroad . . ., the CDA will not reach a significant percentage of the sexually explicit material currently available. . . . [T]he apparent ineffectiveness of the CDA underscores our holding today that the Government has failed to

123. *ACLU*, 929 F. Supp. at 858. Judge Sloviter indicated that he agreed with Judge Buckwalter on this point. *Id.* at 856 (Sloviter, C.J.).

124. *Id.* at 862. *See Reno*, 117 S. Ct. 2329, 2342. Judge Dalzell, in his supporting opinion, disagreed with Judge Buckwalter on this point. *ACLU*, 929 F. Supp. at 868–69 (Dalzell, J.).

125. *Id.* at 863 (Buckwalter, J.).

126. *Id.* at 882 (Dalzell, J.). This, too, was a point acknowledged by Justice Stevens only in a footnote, as follows: "Because so much sexually explicit content originates overseas, [appellees] argue, the CDA cannot be 'effective.' . . . We find it unnecessary to address those issues to dispose of this case." *Reno*, 117 S. Ct. at 2347–48 n.45.

127. 930 F. Supp. 916 (S.D.N.Y. 1996).

> demonstrate that the CDA does not "unnecessarily interfer[e] with First Amendment freedoms."[128]

This court made a link, it seems, between the ineffectiveness of the statute and the requirement that a content based regulation be "necessary" to the accomplishment of a compelling state interest. If an argument of this kind is taken seriously, it may well follow that *no* regulation of Internet speech can withstand First Amendment scrutiny.

V. WHAT DOES THE CDA LITIGATION SUGGEST, WITH REGARD TO THE VALIDITY OF FUTURE LEGISLATION?

The United States Supreme Court decision in *Reno* makes clear that the Courts' formal response to content based regulation of speech on the Internet will be strict judicial scrutiny. Again, that means that the government's goal must be a very important one—apparently not a problem when government seeks to protect children from emotional and psychological harm—and that any such regulation must be necessary to the achievement of that goal, and narrowly tailored to do so, regulating no more, and no less, than is required to accomplish the purpose. In addition, the law must represent the least speech-restrictive means of achieving the government's goal.

Can any regulation of speech on the Internet pass that test?

While the Stevens opinion in *Reno* purported to find the CDA inadequately tailored to the achievement of its goal, and, more specifically, to have failed to satisfy the "least restrictive means" requirement of strict scrutiny, his opinion is quite unclear as to why those conclusions were reached. Indeed, as noted earlier, there appear to be *no* less restrictive ways in which Congress might *just as effectively* achieve the goal of shielding minors from sexually explicit online communications. The Court's unpersuasive use of strict scrutiny makes it harder to evaluate the validity of prospective future legislative initiatives of this kind—but the fact that the United States Supreme Court said what it did will tend to lead lower courts, in future cases, to effectively presume that a regulation of this kind fails strict scrutiny, and perhaps to engage in similarly conclusory analyses.

Arguments flowing from the requirements of strict scrutiny that *might* provide more satisfying bases for striking down such a regulation, however, include the following: 1) such a regulation is unnecessary, because existing federal statutes already prohibit those communications, online or elsewhere, that pose the greatest risks to the emotional and psychological well-being of minors; 2) such a regulation is inescapably and fatally underinclusive (and thus not narrowly tailored to achieve its goal), because sexually explicit

128. *Id.* at 941.

communications emanating from foreign sources effectively cannot and will not be banned by American legislation; and 3) for the same reason, such a regulation cannot be effective in achieving its goal.

But the real meaning of the *Reno* decision may have nothing to do with the well-established "strict scrutiny" analysis. Instead, the decision may simply (although not unambiguously) make clear, forty years after the United States Supreme Court originally set forth this principle in *Butler v. Michigan*,[129] that government really may not, consistently with the First Amendment, shield minors from speech deemed harmful to them, but which is protected speech with respect to adults, by means of a regulatory scheme—even one limited to a specific medium of communication—that effectively deprives adults of access to that speech via that medium. If that is what *Reno* stands for, then no CDA-type regulation, taking the form of a blanket prohibition of speech deemed harmful to minors, will stand.

If that is indeed the key to *Reno*, then none of the more detailed grievances lurking in Stevens' opinion—including, most notably, the fact that the speech banned by the CDA was not defined by the absence of "value" [130](serious or otherwise)—should have any legal significance. Non-obscene material lacking "value" would, after all, still be protected speech with respect to adults. Likewise, the arguable vagueness of statutory terms such as "indecency" probably drops out of the analysis, in effect, because the *Butler* principle invalidates even a blanket prohibition that could survive a vagueness challenge.

But what is to be made of Stevens' observation that the CDA was not limited, in its application, to "commercial" websites?[131] Is there any good reason to believe that a CDA-like statute limited to commercial websites would be constitutional? That would narrow the reach of the regulation, and commensurately reduce—but not eliminate—the burden placed upon protected speech.

The *Butler* principle would not, however, prevent Congress from imposing upon online communicators an affirmative obligation to take specified steps designed to minimize the likelihood that minors would come into contact with sexually explicit communications. And that is what Congress has done, in the wake of the failure of the CDA.

---

129. 352 U.S. 380 (1957). The Court reiterated the *Butler* principle in other decisions, most notably in *Sable Communications of California, Inc. v. FCC*, 492 U.S. 115, 126–27 (1989), and in *Bolger v. Youngs Drug Prod. Corp.*, 463 U.S. 60, 73 (1983), during the 1980s, but none of those decisions depended on that principle.

130. *Reno*, 117 S. Ct. at 2341, 2344 n.37, 2349.

131. *Id.* at 2347.

VI. THE CHILD ONLINE PROTECTION ACT

Congress enacted the Child Online Protection Act[132] ("COPA") on October 21, 1998. In assessing the constitutionality of the Act, it is useful to first consider two prior versions of the bill that ultimately became law.

When initially introduced in the House of Representatives on April 30, 1998, the Child Online Protection Act contained the following core provision: "Whoever in interstate or foreign commerce is engaged in the business of selling or transferring, by means of the World Wide Web, material that is harmful to minors shall restrict access to such material by persons under 17 years of age."[133]

Criminal penalties were provided in the event of violations. The bill went on to provide that one would not be liable if one restricted access to said material "by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number[,] or in accordance with such other procedures as the [FCC] may prescribe)."[134] The phrase "harmful to minors" was defined in a manner quite comparable to the definition, in the New York statute upheld by the Supreme Court in *Ginsberg v. New York*,[135] of material which was deemed obscene as to minors, and which could not legally be sold to minors.[136]

Would this bill, if enacted, have survived strict constitutional scrutiny?

Unless the Supreme Court repudiates the definition that even Justice Brennan found to be acceptable thirty years ago in *Ginsberg*, there appears to be no problem with respect to the scope of the targeted communications. Moreover, the concerns (of uncertain magnitude) expressed in *Reno* with regard to: (a) the CDA's inclusion of material with "value,"[137] and (b) the CDA's applicability to non-commercial sources of communications,[138] are here eliminated. Furthermore, the wording of this bill imposed an affirmative obligation on those sources—to "restrict access"—rather than a prohibition of the targeted communications.[139] Culpability would thus not have been imposed on communicators who are helpless to avoid making online communications accessible to minors, other than by censoring their communications to adults—the apparent primary vice of the CDA. Rather, one would be culpable only for failing to utilize existing screening devices. If one did utilize such devices, guilt would not be imposed simply because

132. Pub. L. No. 105-277, 112 Stat. 2681 (to be codified at 47 U.S.C. § 223 (1998)).
133. H.R. 3783, 105th Cong. § 3 (1998).
134. *Id.*
135. 390 U.S. 629 (1968).
136. *Id.*
137. *Reno*, 117 S. Ct. at 2341, 2344 n.37, 2349.
138. *Id.* at 2347.
139. *Id.* at 2339.

some minors gained access to the targeted communications. Thus, Reno's concern with the illusoriness of the CDA's affirmative defenses would apparently play no role in an evaluation of this bill. While this bill might still have been found to be unconstitutional, these points of distinction from the CDA would have bolstered its chances of surviving a First Amendment challenge.

However, by the time this bill emerged from the House Committee on Commerce in early October, its core provision had been significantly modified to read as follows:

> (a) Requirement to Restrict Access.-
>
> (1) Prohibited conduct.—Whoever, in interstate or foreign commerce, by means of the World Wide Web, knowingly makes any communication for commercial purposes that includes any material that is harmful to minors, without restricting access to such materials by minors pursuant to subsection (c), shall be fined . . ., imprisoned . . ., or both.[140]

Subsection (c) provided an affirmative defense, comparable to that in the original bill, that would preclude liability on the part of a defendant who took appropriate steps to restrict access by minors to "harmful" material.[141] The core provision of the bill had thus been transformed from a requirement that access be restricted to a ban on certain communications, *unless* access were restricted. The language of this provision evolved further during the month of October. The key language of the statute, as it was enacted, is as follows:

> SEC. 231. RESTRICTION OF ACCESS BY MINORS TO MATERIALS COMMERCIALLY DISTRIBUTED BY MEANS OF WORLD WIDE WEB THAT ARE HARMFUL TO MINORS.
>
> "(a) REQUIREMENT TO RESTRICT ACCESS.—
>
> "(1) PROHIBITED CONDUCT.—Whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors shall

140. H. R. REP. No. 105-775, 105th Cong. (1998), 1998 WL 691067 at *4–5.
141. *Id.*

be fined not more than $50,000, imprisoned not more than 6 months, or both.[142]

"(c) AFFIRMATIVE DEFENSE.—

"(1) DEFENSE.—It is an affirmative defense to prosecution under this section that the defendant, in good faith, has restricted access by minors to material that is harmful to minors—

(A) by requiring use of a credit card, debit account, adult access code, or adult personal identification number;

(B) by accepting a digital certificate that verifies age; or

(C) by any other reasonable measures that are feasible under available technology.[143]

(e) DEFINITIONS.—For purposes of this subsection, the following definitions shall apply:

"(6) MATERIAL THAT IS HARMFUL TO MINORS.—The term "material that is harmful to minors" means any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that—

"(A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;

"(B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and

"(C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

"(7) MINOR.—The term 'minor' means any person under 17 years of age.[144]

---

142. COPA, Pub. L. No. 105-277, 112 Stat. 2681 (to be codified at 47 U.S.C. § 231(a)(1) (1998)).

143. *Id.* (to be codified at 47 U.S.C. § 231(c)(1)).

The statute also created a Commission on Online Child Protection, "for the purpose of conducting a study . . . regarding methods to help reduce access by minors to material that is harmful to minors on the Internet."[145]

As enacted, then, the COPA is no longer susceptible to being read as merely requiring that Internet content providers take certain prescribed steps to restrict access by minors to "harmful" material. Rather, like the CDA, it prohibits certain speech on the Internet, but provides that the use of prescribed methods of restricting access shall constitute an affirmative defense to liability. Thus, the resemblance between the COPA and the CDA is greater than we had been led to anticipate.

Still, there are significant differences between the CDA and the COPA. As has already been noted, those differences include: 1) a redefinition of the targeted communications that is probably constitutionally acceptable; and 2) a limitation of the scope of the targeted communications to those communicated: a) "by means of the World Wide Web;"[146] and b) "for commercial purposes."[147] Moreover, a "minor" is now defined as a person under seventeen years of age,[148] a year younger than a minor protected by the CDA.[149] In addition, and very significantly, there is no requirement in the COPA, as there was in the CDA, that a method of restricting access by minors must, in order to serve as an affirmative defense, be "effective." Recall that, in *Reno*, Justice Stevens stated that "[i]t is the requirement that the good faith action must be 'effective' that makes this defense illusory."[150] Presumably, the elimination of that flaw greatly enhances the prospect that the COPA will survive a First Amendment challenge. Note also that, for whatever it may be worth, Congress did a better job "procedurally," this time around, than it had in laying a satisfactory predicate for the ill-fated CDA. Both houses of Congress, during 1998, held hearings pertaining to the subject of this legislation, and, in its Report, the House Committee on

144. *Id.* (to be codified at 47 U.S.C. § 232(e)(6)–(7) (1998)). Also defined in section (e), most notably, are the phrases "by means of the World Wide Web" and "commercial purposes." *Id.*

145. Pub. L. No. 105-277, 112 Stat. 2681 (to be codified at __ U.S.C. __ (1998)).

146. This limitation is given emphasis in the House Report, which observed that the statute "does not apply to content distributed through other aspects of the Internet such as one-to-one messaging (e-mail), one-to-many messaging (list-serv), distributed message databases (USENET newsgroups); real time communications (Internet relay chat); real time remote utilization (telnet) or remote information retrieval other than the World Wide Web (ftp and gopher)." H. R. REP. NO. 105-775 (1998), 1998 WL 691067 at *30.

147. *Id.*

148. *Id.* at *31.

149. *See supra* text accompanying note 3.

150. *Reno*, 117 S. Ct. 2329, 2349 (1997).

Commerce set forth pertinent findings of fact with respect to both the need for regulation and the absence of sufficient regulatory alternatives.[151]

The COPA, then, is a more limited interference with freedom of speech than was the CDA. But is it nonetheless likely to fall to a First Amendment challenge? The answer may hinge on the extent to which even a prohibition that is limited to those web sites operated "for commercial purposes" is seen as placing too great a burden on freedom of speech.[152] The Supreme Court in *Reno* made much of the burdens placed by the CDA on those communicators who could not easily utilize available age verification devices.[153] In that part of his opinion in which he reviewed the district court's findings of fact, Justice Stevens observed that credit card verification was only feasible in connection with commercial transactions; by contrast, using that approach "would impose costs on non-commercial Web sites that would require many of them to shut down."[154] "Moreover," he went on to say, "the imposition of such a requirement 'would completely bar adults who do not have a credit card and lack the resources to obtain one from accessing any blocked material.'"[155] Later, in the core part of his analysis of the CDA, Stevens noted that the district court had "found that it would be prohibitively expensive for noncommercial—as well as some commercial—speakers who have Web sites to verify that their users are adults. . . . These limitations must inevitably curtail a significant amount of adult communication on the Internet."[156]

Narrowing the reach of the statute to "commercial" providers thus goes far toward reducing the extent to which online adult communications are burdened, or suppressed, by a requirement that age verification devices be employed. But Stevens' statement that "it would be prohibitively expensive for . . . [even] some commercial . . . speakers who have Web sites to verify

151. H. R. REP. NO. 105-775 (1998), 1998 WL 691067 at *3–4. Note also that, in the Congressional Findings that appear at the outset of the COPA itself, it is asserted that "(4) a prohibition on the distribution of material harmful to minors, combined with legitimate defenses, is currently the most effective and least restrictive means by which to satisfy the compelling government interest . . . ." *Id.* at *4.

152. "The decision in *ACLU* suggests that the constitutionality of an Internet-based 'harmful-to-minors' statute likely would depend, principally, on how difficult and expensive it would be for persons to comply with the statute without sacrificing their ability to convey protected expression to adults and to minors." L. Anthony Sutin, *Department of Justice Letter on CDA II* <http://www.aclu.org/court/acluvrenoII_doj_letter.html>. (L. Anthony Sutin, as Acting Assistant Attorney General, authored this letter dated October 5, 1998, to Congressman Thomas Bliley, the Chairman of the Committee on Commerce, wherein he outlined the Department's views on the COPA.).

153. *Reno*, 117 S. Ct. at 2337.

154. *Id.*

155. *Id.* (citing *ACLU*, 929 F. Supp. 824, 846 (E.D. Pa. 1996)).

156. *Id.* at 2347 (citing *ACLU*, 929 F. Supp. 824, 845–48 (E.D. Pa. 1996)).

that their users are adults,"[157] if still factually accurate, suggests that even this drastic narrowing of the field of regulatory targets may not suffice to save the statute. The clear argument to be made by a challenger is that a requirement that "prohibitively expensive" devices be employed amounts to a prohibition of protected communications between adults, with respect to those speakers for whom the devices are "prohibitively expensive." That would seem to bring the *Butler* principle back into play.

A legal challenge to the COPA has, in fact, already been launched. The ACLU, along with several other organizations, has filed a lawsuit seeking to have the COPA declared unconstitutional and to enjoin its enforcement.[158] In its complaint, the ACLU attempts to demonstrate the breadth of the coverage of the COPA, notwithstanding its limitation to web sites operated "for commercial purposes:"

> The Act purports to restrict only content provided on the Web "for commercial purposes," but in fact it explicitly bans a wide range of protected expression that is provided *for free* on the Internet by individuals and organizations. . . . [T]he Act targets all other communications made publicly accessible on the Web "for commercial purposes," defined very broadly as being "engaged in the business of making such communications." . . . The Act's definition of a person "engaged in the business" explicitly states that "it is not necessary that the person make a profit" nor that the making of the communications be the person's "principal business.". . . Just like many traditional print newspapers, bookstores, and magazine publishers, many Web publishers make a profit (or attempt to make a profit) through advertising. . . . Thus, the Act impacts a wide range of providers of free content, from fine art to popular magazines to news and issue-oriented expression.[159]

The ACLU goes on, in its complaint, to contend that, for many of these targeted online content providers, the methods of restricting access that give rise to an affirmative defense under the COPA are, in fact, "technologically and economically infeasible."[160]

---

157. *Id.* at 2347.

158. *ACLU in Court: ACLU v. Reno Complaint* <http://www.aclu.org/court/acluvrenoII_complaint.html>. [hereinafter *ACLU Complaint*]. In November 1998, a federal district judge issued a temporary restraining order, enjoining enforcement of the statute. ACLU v. Reno, No. CIV.A.98-5591, 1998 WL 813423 at *1 (E.D. Pa. Nov. 23, 1998). This was followed by the entry of a preliminary injunction on February 1, 1999. ACLU v. Reno, No. CIV.A.98-5591, 1999 WL 44852 at *27 (E.D. Pa. Feb. 1, 1999).

159. *See ACLU Complaint, supra* note 158, ¶ 65.

160. *See ACLU Complaint, supra* note 158, ¶¶ 67–69.

The resolution of the constitutional question may, then, ultimately depend on further empirical developments of a technological and economic nature: *are* these means of restricting access to web sites technologically or economically infeasible, "prohibitively expensive," or otherwise intolerably burdensome? If they are feasible, and not prohibitively expensive, then the COPA may be constitutional.

In issuing a preliminary injunction against the enforcement of the COPA (and denying the government's motion to dismiss the complaint), Judge Reed made extensive findings of fact concerning the costs of compliance with the new statute,[161] leading him to conclude that "the plaintiffs have established a substantial likelihood that they will be able to show that COPA imposes a burden on speech that is protected for adults."[162]

Even if a significant amount of adult speech is burdened by the COPA, does the *Butler* principle admit of any flexibility? Might the concededly strong government interest, and the limited nature of the regulation, at some point outweigh the fact that some online communications that are constitutionally protected as to adults will not be permitted to be made? Of course, if a court finds that the government could have achieved its goals through less restrictive means, then the COPA will be struck down, just as was the CDA. In his memorandum of February 1, 1999, Judge Reed suggested that the case might be decided on that basis:

> On the record to date, it is not apparent to this Court that the defendant can meet its burden to prove that COPA is the least restrictive means available to achieve the goal of restricting the access of minors to this material. . . . The record before the Court reveals that blocking or filtering technology may be at least as successful as COPA would be in restricting minors' access to harmful material online without imposing the burden on constitutionally protected speech that COPA imposes on adult users or Web site operators. Such a factual conclusion is at least some evidence that COPA does not employ the least restrictive means.[163]

The arguable defect in this reasoning is that, as Justice Stevens observed in the process of invalidating the CDA, there is no assurance that parents will actually employ such blocking or filtering devices.[164]

---

161. See *ACLU v. Reno*, 31 F. Supp. 2d 473, 488-92 (E.D. Pa. 1999) for findings of fact 41–64.

162. *ACLU*, 31 F. Supp. 2d at 495.

163. *Id.* at 497.

164. *See supra* text accompanying note 94.

More persuasively, however, Judge Reed went on to call attention to "other aspects of COPA which Congress could have made less restrictive[:]"

> Notably, the sweeping category of forms of content that are prohibited—"any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind"—could have been less restrictive of speech on the Web and more narrowly tailored to Congress' goal of shielding minors from pornographic teasers if the prohibited forms of content had included, for instance, only pictures, images, or graphic image files, which are typically employed by adult entertainment Web sites as "teasers."[165]

Finally, if all other bases for a First Amendment challenge fail, would a court invalidate this law simply because it cannot effectively rid the Internet of all such "harmful" communications, particularly those that emanate from abroad? Judge Reed made reference to this concern as well:

> [T]his Court's finding that minors may be able to gain access to harmful to minors materials on foreign Web sites, non-commercial sites, and online via protocols other than http demonstrates the problems this statute has with efficaciously meeting its goal. Moreover, there is some indication in the record that minors may be able to legitimately possess a credit or debit card and access harmful to minors materials despite the screening mechanisms provided in the affirmative defenses. . . . These factors reduce the benefit that will be realized by the implementation of COPA in preventing minors from accessing such materials online.[166]

These seem to be the considerations that are likely to govern the determination of whether the COPA is consistent with the First Amendment. Thanks to the ACLU and its fellow plaintiffs, it appears that a final judicial resolution of these issues will, in fact, be made in the near future.

165. *ACLU*, 31 F. Supp. 2d at 497.
166. *Id.* at 496-97.

The Brave New World of Banking on the Internet: The Revolution of our Banking Practices

TABLE OF CONTENTS

I. INTRODUCTION

The electronic medium of communication known as the Internet is rapidly becoming the home of a new virtual economy. Using the Internet, a consumer has the ability to purchase products and receive goods in the privacy of the home. This new ability to buy and sell goods online is quickly becoming a major component of electronic commerce. It is within electronic commerce that financial institutions have shifted to Internet-based electronic banking.[1] Internet-based electronic banks and Internet banking open the doors for financial institutions to attract new customers and lower the institutions' overall costs.[2]

1. Bret G. Wilson, *Banking on the Net: How to Get Your Financial Services Client There with Minimal Trouble*, 43 PRAC. LAW. INST. CORP. L. HANDBOOK SERIES 25, 26 (Mar. 1997).
2. *Id.*

Initially, financial institutions only had Internet or Web pages with general information about banks.[3] Banks expanded their Internet Web sites to provide consumers with the ability to conduct their banking transactions via the World Wide Web and the Internet as both banks and consumers increased their Internet usage.[4] Banking on the Internet has created several choices of electronic alternatives to conventional forms of money, and banking services by financial and nonfinancial institutions.[5] Electronic banking includes electronic fund transfers and electronic payment systems. It also includes banking services provided by financial institutions as well as nonfinancial institutions. The nonfinancial institutions are often referred to as nonbanks.[6] There are a number of nontraditional entrants in the banking industry, including AT&T and Microsoft, that are competing with traditional banks.[7] Currently, there are three different types of electronic banking.[8] The first is "online banking," where an individual connects to a traditional bank's private network to perform conventional banking transactions.[9] The second is "web-based banking," where an individual connects to a traditional bank over the public Internet to perform conventional banking transactions.[10] The third type of electronic banking is through an actual "Internet bank."[11] The Internet-based bank focuses on providing bank-like services without the conventional structure, or even building of a traditional bank.[12] Internet-based banks offering services solely on the Internet are also competing with the traditional banks. Because of such diversity in electronic banking, its role within electronic commerce has changed tremendously within a short amount of time. In particular, there is an increasing presence of electronic money on the Internet, which is slowly impacting the entire financial industry.

"Electronic cash . . . refers to any electronic notation for money."[13] Since electronic cash is the currency of the Internet, it promises to have a wide impact on bank supervision and monetary policy. Electronic money is

---

3. Kimbrelly Kegler, *Electronic Banking: Security, Privacy, and CRA Compliance*, 2 N.C. BANKING INST. 427 (1998).

4. *Id.*

5. Marty Fisher-Haydis & Kara R. Yancey, *Developments in Banking Law: 1996*, 16 ANN. REV. BANKING L. 76, 92 (1997).

6. *Id.* at 99.

7. Dan L. Nicewander, *Electronic Banking—Smart Cards, Cyberspace and the Internet*, 50 Consumer Fin. L. Q. Rep. 22 (1996).

8. Kegler, *supra* note 3, at 426.

9. *Id.*

10. *Id.*

11. *Id.*

12. *Id.*

13. Fisher-Haydis & Yancey, *supra* note 5, at 76.

being marketed as a mechanism to facilitate commerce. This market can be very lucrative, especially in light of the growth of the Internet. At the end of 1997 there were thirty million worldwide users of the Internet and thirty-five million households in the United States with personal computers.[14] In December 1998, NUA, an Internet statistics company, reported that there were 151 million worldwide Internet users, or three percent of the world population, with over seventy-three million Internet users in the United States.[15] It is speculated that electronic money will replace approximately 400 billion dollars of the United States' currency circulating worldwide.[16] Indeed, it is predicted that the amount of cash in circulation will continue to fall from 400 billion dollars to 200 billion dollars by the year 2005.[17] Without a national monetary policy that manages "electronic money," such money will potentially make the money supply infinite because electronic money could possibly be infinite. Our current monetary policies and regulatory agencies are not structured to deal with "electronic money," its liquidity, and origination.

Internet banking presents new legal and regulatory issues regarding banks and nonbank entities and their ability to gather, transfer, and store money. The federal and international agencies that regulate banks are faced with the problem of trying to apply existing regulations to banking on the Internet or create new regulations. The banking functions being performed on the Internet pose both legal and regulatory challenges.[18] Regulating the movement of money and transactions is much more complex than regulating a bank's web page. New regulatory issues also arise from using nonbank entities to store money on the Internet. Additionally, the two key issues of privacy of confidential information and security of financial transactions must be addressed.[19] This article will focus on banking on the Internet, and specifically the role of nonbank entities, privacy and security issues in electronic banking, and regulatory issues regarding banking on the Internet.

---

14. Catherine Lee Wilson, *Banking on the Net: Extending Bank Regulation to Electronic Money and Beyond*, 30 CREIGHTON L. REV. 671, 673 (1997).

15. *NUA Internet Statistics* (visited Dec. 28, 1998) <http://www.nua.ie/surveys/how_many_online/index.html>.

16. D. Lee Falls, *Dateline 2005: Does Banking on the Internet Need to be Regulated?* 14 BANKING POL'Y REP. No. 24 1, 10 (1995).

17. *Id.*

18. Melanie L. Fein, *The New Business of Banking: What Banks Can Do Now*, 912 PRAC. LAW. INST. CORP. L. PRAC. COURSE HANDBOOK SERIES 91, 95–96 (1995).

19. *Id.* at 95.

II. INTERNET-BASED BANKS

One of the most significant features of the Internet is the ability to eliminate geographic barriers. It is this unique nature of the Internet that allows a financial institution, as well as a nonfinancial institution, to exist solely on the Internet. There are no brick walls, tellers, and no branch offices. Services are offered twenty-four hours a day. Such advantages of Internet-based banks are growing, but there are disadvantages for both the consumer and the financial institution. For instance, one disadvantage for the financial institution is that it is subject to uncoordinated and inconsistent regulations by states because the financial institution offers banking services over the Internet to customers in various states and across the world. Furthermore, the Internet-based bank must comply with the Community Reinvestment Act ("CRA")[20] because the CRA mandates that any Federal Deposit Insurance Corporation ("FDIC") insured bank must address and service the community needs in which the bank operates.[21] Being able to determine exactly what constitutes the "community" on the Internet is a challenge that all Internet-based banks face.[22]

While there are more than 840 banks that have Internet sites, the Office of Thrift Supervision has granted thrift charters to only two Internet-based banks, Security First Network Bank[23] and Atlanta Internet Bank.[24] The Office of the Comptroller of the Currency ("OCC") has also approved the charter for CompuBank, N.A.[25] The Security First Network Bank and the Atlanta Internet Bank offer all of their services over the Internet. It appears that such banking services will be able to compete with the larger banks, such as Citibank and NationsBank, because more customers may be reached and "fewer bricks mean higher returns."[26] With reduced costs, the Internet-based bank can offer better interest rates on money market accounts, certificate of deposits, and even checking accounts.[27] Indeed, the customer base of Internet banks have grown tremendously. For example, Atlanta Internet Bank began with about twenty customers in late 1996, and now has

---

20. Consumer Reinvestment Act of 1977, 12 U.S.C. § 2901 (1994).

21. 12 U.S.C. §§ 2901–07 (1994); 12 C.F.R. § 25.11(b)(1) (1998).

22. The Security First Bank Network, an Internet bank based in Atlanta, concentrates its CRA efforts in the Atlanta community. *See* Kegler, *supra* note 3, at 438.

23. *Security First Network Bank* (visited Dec. 1, 1998) <http://sfnb.com>.

24. *Atlanta Internet Bank Home Page* (visited Dec. 24, 1998) <http://www.atlantabank.com> [hereinafter *Atlanta*] (as of Feb. 20, 1999, this site no longer available).

25. *See* New York Times (Cyber Times), *Fewer Bricks Mean Higher Returns at New Internet Banks* (visited Feb. 25, 1998) <http://www.pcn.com> [hereinafter *Fewer Bricks*] (as of Jan. 30, 1999 this site had changed).

26. *Id.*

27. *Id.*

approximately 6,500 customers with deposits totaling near $95 million.[28] Within eighteen months, Atlanta Internet Bank has acquired assets of $175 million.[29] Now eighty percent of Atlanta Internet Bank's customers are outside of Georgia and from twenty-one countries around the world.[30] Security First Network Bank is also growing, and has about $45 million dollars in deposits.[31] Moreover, these Internet banks enjoy the same Federal Deposit Insurance Corporation ("FDIC") protection for their depositors as traditional banks' customers receive.

While these types of banks, as well as any nonbanks, can offer many conveniences and advantages, the consumer should be aware of problems that lurk on the Internet. The FDIC cautions the consumer about companies "pretending to be banks offering unusually high interest rates," because such institutions may not be FDIC insured.[32] The FDIC recommends that the consumer find out about a particular financial institution before giving out personal information and conducting transactions.[33] The FDIC also suggests that a consumer should be skeptical about any Internet site or any advertisement that makes an offer that is too good to be true.[34] The consumer should be cautious about banking with international financial institutions, because such institutions may not be complying with all of the federal and state regulatory requirements, which may result in the institution being here today and gone tomorrow.[35] The FDIC offers an Internet site where a consumer can either find out if a financial institution is FDIC insured or report any suspicious activity.[36] The future of these types of banks is uncertain, but the technology allowing all banking services to be available at the stroke of a finger and in the privacy of the home is here to stay.

---

28. *Id.*

29. *CNN-Cyberbanks: Anytime, Anywhere* (visited Apr. 18, 1998) <http://cnn.com/TECH/computing/9804/18/online.banking/index.html>.

30. *See generally Atlanta, supra* note 24.

31. *Id.*

32. *Internet Banking and Shopping: Cyber-Buyer Beware* (visited Dec. 25, 1998) <http://www.fdic.gov/consumer/consnews/fal97/netbank.html>.

33. *Id.*

34. *Id.*

35. One such situation arose in Idaho. There, European Union Bank, a bank chartered in Antigua, promoted itself to the residents of Idaho. The State Department of Finance issued a cease and desist order on the grounds that the bank was soliciting deposits on the Internet to Idaho residents without being chartered to operate a bank or any other form of financial institution in Idaho. *State Business of Banking Laws and the Internet, 21st Century Banking Alert No. 97-9-10* (visited Jan. 29, 1998) <http://www.ffhsj.com/bancmail/ 21starch/ 970910.html>.

36. *Suspicious Internet Banking* (visited Dec. 25, 1998) <http://www.fdic.gov/consumer/suspicious/sspcious.html>.

III. INTERNET BANKING AND ITS MONEY SUPPLY

Electronic banking is not significantly different from traditional banking concepts and activities. It simply represents an alternative delivery system for traditional banking products.[37] Electronic banking is very broad in scope and includes electronic funds transfers, electronic payment systems, global financial and banking systems, and personal computer ("PC") access to bank services.[38] Until recently, traditional banks and banking services primarily used private networks to manage transactions for consumers, corporations, financial institutions, and other entities.[39] The Internet offers an additional, but public, network for these services and systems. Recently, there has been a shift to Internet-based electronic banking. Internet banking is currently a small part of the world of electronic banking. However, since Internet banking deals directly with the consumer market, it offers the greatest potential for growth. The transition to Internet-based banking has opened the door to many new technologies, financial opportunities, and forms of commerce. For instance, electronic money is the result of such new technology that has emerged as a potential new currency to be used by banks, consumers, and merchants on the Internet.[40] Some believe that this is the beginning of the end of money as we currently know it. James Gleich states:

> Cash is quaint, technologically speaking—unless you're impressed by intaglio-steel-plate-printed paper with embedded polyester strips (meant to inconvenience counterfeiters). Cash is expensive—tens of billions of dollars drain from the economy each year merely to pay for the printing, trucking, safekeeping, vending, collecting, counting, armored-guarding and general care and feeding of our currency. Cash is obsolete.[41]

But not everyone shares that view. The U.S. Department of the Treasury states:

---

37. *An Introduction to Electronic Money Issues*, prepared for the United States Department of the Treasury Conference, Toward Electronic Money and Banking: The Role of Government, September 19–20, 1996, Washington, D.C. [hereinafter *Electronic Money Issues*] (on file with author).

38. *Id.*

39. *Id.*

40. *Id.*

41. James Gleick, *The End of Cash* (visited Jan. 14, 1999) <http://www.around.com/money.html>.

> Conversion of Treasury payments, now running at about 800 million a year, to an all electronic format will bring changes permitting, for example, a consolidation of disbursing operations that currently produce checks. [A]mong the less technologically advanced countries, cash is the principal means of payment, the dollar seems to be one of the currencies of choice, and the infrastructure that will support widespread use of electronic money seems many years away.[42]

A. *What is Electronic Money?*

The term electronic money refers to the recording or storing of information about the funds or "value" available to a consumer.[43] This information is stored on a device in the possession of the consumer, such as a personal computer, or "smart card."[44] The device is then updated with information over either a private network or a public network, like the Internet.[45] For example, a phone card with a preset value of five dollars is a "smart card." While "smart card" technology is a type of electronic money, electronic money also includes "electronic cash." The advantages of electronic money are that it can: 1) offer new revenue streams for banks and other issuers or nonbanks in the form of fees; 2) "float" interest on balances stored and held by the issuer; and 3) cost savings from reduced cash handling costs.[46] Often, the term "electronic cash" is used interchangeably with the term "electronic money." Electronic money provides a means for consumers to purchase goods and for retailers to sell goods efficiently when using a credit card is not feasible or desirable.[47]

Several private companies have created "electronic money software products." Three such software products that facilitate the creation and management of electronic money are NetCash, ecash, and CyberCoin. These emerging products focus on balancing the privacy aspect of credit cards with

---

42. *Electronic Money Issues*, *supra* note 37.

43. *Id.*

44. *Id.*

45. *Id.*

46. *Implications for Central Banks of the Development of Electronic Money* (visited Jan. 14, 1999) <http://www.bis.org/publ/bisp01.htm>.

47. *Id.*

the anonymity of cash.[48] Currently, there is no one system that is universally accepted to make, issue, or manage electronic money.[49]

NetCash is a form of electronic money that is distributed by an online private bank, NetBank.[50] The customer sends United States ("U.S.") dollars to NetBank in exchange for a NetCash coupon.[51] The customer receives the coupon as an encrypted e-mail. It has three parts: "the 'NetCash U.S. $' keyword, the dollar amount, and the serial number of the bill."[52] When the customer wants to purchase a product, the customer sends a coupon to NetBank. Then, NetBank sends "digital coins" to the merchant as payment for the product.[53] The merchant also has an account with NetBank, and may then convert the "digital coins" back to dollars.[54]

DigiCash, founded in 1990, is a leading pioneer in electronic payment systems using public key cryptography.[55] DigiCash uses "ecash," a trademarked product specifically developed for the Internet, as a form of electronic cash.[56] Customers and merchants use the bank's public key to decode messages and conduct transactions.[57]

DigiCash uses ecash "coins" which have a specified value.[58] An electronic "purse"[59] is established for the customers and merchants. The coins are then moved between customer, bank, and merchant to complete transactions.[60] To receive the value, the payee confirms the validity of the coins by depositing them online into an ecash account. This transaction will not reveal the name or address of the payer because each ecash coin is secured by a high-level encryption method. Like bank notes, ecash can be

---

48. *North American Media Engines-Resource Centre-Articles-Net Money* (visited Mar. 15, 1998) <http://www.name.net/netmoneys.html> [hereinafter *North American Media*].

49. *Id.*

50. *Id.*

51. *Id.*

52. *Id.*

53. *North American Media*, *supra* note 48.

54. *Id.*

55. *Id.*

56. *DigiCash-Profile* (visited Jan. 14, 1999) <http://www.digicash.com/digicash/digicash/profile/index.html>.

57. *Id.*

58. *ecash - An Introduction to ecash* (visited Apr. 9, 1998) <http://www.digicash.com/ecash/intro/index.html>.

59. *Glossary of ecash* (visited Feb. 16, 1999) <http://www.digicash.com/ecash/docs/purse_manual/gloss.html>.

60. *DigiCash – How ecash Works Inside* (visited Apr. 8, 1998) <http://www.digicash.com/ecash/docs/works/> [hereinafter *How ecash Works Inside*].

withdrawn from and deposited into deposit accounts.[61] The "coins" include strings of digits, with each string corresponding to a different digital "coin."[62] Each coin has a denomination, or value, so that a purse of digital coins is managed automatically by the customer's ecash software.[63] The customer's ecash software chooses coins with the desired value from the purse on the PC and then sends them over the network. When the merchant's software receives the "coins," the software automatically sends the "coins" to the bank. To ensure that each coin is used only once, the bank records the serial number of each coin in its database. If no such serial number has been previously recorded, the bank stores it and informs the merchant that the coin is valid and that the deposit is accepted.[64]

DigiCash's use of ecash has now gone one step further in providing privacy and anonymity. DigiCash uses "blind signatures," which prevent the bank from recognizing a particular account.[65] Instead of the bank creating a blank coin, the customer's computer creates the coin at random.[66] The coin is put in a "digital envelope" and sent to the bank.[67] The bank then withdraws one dollar from the customer's account and creates one dollar in digital form, similar to an embossed stamp on an envelope, before returning it to the customer's computer.[68] The "blind signature" mechanism allows the validating signature to be applied through the envelope.[69] When the customer's computer removes the envelope, it has obtained a coin of its own choice, validated by the bank's stamp.[70] However, because the bank is unable to recognize the coin, "the bank cannot tell who made the payment."[71] Therefore, the customer is anonymous and privacy is maintained.

Another company that has developed electronic money is CyberCash, Inc. ("CyberCash"). CyberCash has developed a "CyberCoin" that can be

---

61. *Id.*
62. *Id.*
63. *Id.*
64. *Id.*
65. The bank creates unique blank digital coins and validates them with its special digital stamp. *How ecash Works Inside*, *supra* note 60. This would normally allow the bank to recognize the particular coins when accepted in a payment and thus tells the bank exactly which particular customer made a payment. *Id.*
66. *Id.*
67. *Id.*
68. *Id.*
69. *How ecash Works Inside*, *supra* note 60.
70. *Id.*
71. *Id.*

used for purchases ranging from twenty-five cents to ten dollars.[72] The "CyberCoin" provides a means of paying for smaller items, when using a credit card would be inefficient.[73] In other words, "CyberCoin" is the equivalent of pocket change.[74] CyberCash seems to be placing some much needed emphasis on making the electronic cash transaction cost effective.

A principal disadvantage of electronic money in most of the current products is that the mechanisms used to store values and perform transactions use an electronic medium; therefore keeping track of all the past transactions, certificates, and coins and preventing double spending, would require massive databases.[75] Furthermore, software technology would have to be used to prevent an electronic purse and all of its contents from being used over and over again.

Such money can also result in many issues for banks. As previously noted, the makers of this money may not be banks, but rather private companies that are acting as banks in some manner. Federal regulators of banks are faced with the challenge of possibly regulating such companies as traditional banks. Secondly, through encryption methods, the banks are receiving money and depositing "money," without being able to trace such money. This leads to the issue of whether such strings of characters are indeed "money," as society knows it to be.

B. *Is it Money?*

One question facing regulators is whether a string of characters constitutes "money." Traditionally, the federal government has had the power "to coin Money, [and] regulate the Value thereof."[76] "[T]he Federal Government has not [always] been the sole issuer of currency."[77] Private and state banks also issued money until 1913, when the Federal Reserve System was established as the central banking system.[78]

---

72. *CyberCash - Free Wallet* (visited May 16, 1998) <http://www.cybercash.com/cybercash/consumers/wallet.html>.

73. *CyberCoin: Micropayments Revolutionize Web Commerce* (visited Jan. 14, 1999) <http://www.cybercash.com/cybercash/services/cybercoin.html>.

74. *Id.*

75. B. Clifford Neuman & Gennady Medvinsky, *NetCheque, NetCash, and the Characteristics of Internet Payment Services* (visited Jan. 14, 1999) <http://www.press.umich.edu/jep/works/NeumNetPay.html>.

76. U.S. CONST. art. I, § 8, cl. 5.

77. Wilson, *supra* note 14, at 691.

78. *Id.*

Now, a new tender is being developed which involves private companies generating "money."[79] "Whether on a card or the hard drive of a personal computer, the current forms of electronic money involve the storage of 'value' which is exchanged for goods or services."[80] Examination of the underlying features and properties of electronic money is essential to determining whether electronic money is money or something else that needs to be defined and possibly regulated, or even eliminated.[81] It can be argued that "electronic money," as a stored value, is a form of private money that would be accepted as legal tender. "However, the new electronic money systems lack [some] essential" traits of money.[82] First, when executing a transaction using an "electronic value," instead of cash or private money, the transaction is not completed in a single step.[83] Unlike cash or private money transactions, "electronic value" transactions require merchants to submit the value to the issuing bank before they receive cash, with the electronic money moving through various complex systems before the transaction is completed.[84] Second, electronic money does not qualify as a substitute for private money, "because all current electronic money developments allow the holder of the stored value to redeem it for the national currency," whereas private money may not be redeemed as such.[85]

The question of whether electronic money is money also raises the issue of customer confidence regarding the circulation of "electronic money." Currently, a customer has confidence that a credit given by a bank is redeemable for cash. Such confidence is largely due to the regulatory scheme of the FDIC that protects against bank failure. There is a risk, that if a nonbank becomes insolvent consumers would not be protected, and thus would be susceptible to a complete loss of funds stored in the nonbank.[86]

Electronic money is invisible and lacks any physical characteristics. If electronic money is to gain the confidence of the customer, it must fall under regulatory schemes. Nonbank entities will issue "electronic value" in exchange for U.S. currency. Under our current scheme, the entity would have to qualify as a "bank" before federal banking regulators could examine and control the activities of the issuer. Assuming the entities issuing smart cards and other electronic forms of "electronic value" are not banks and are not currently covered by our federal banking regulations, the issue then

---

79. *Id.*
80. *Id.* at 690.
81. *Id.* at 691.
82. Wilson, *supra* note 14, at 692.
83. *Id.*
84. *Id.*
85. *Id.*
86. UNITED STATES DEP'T OF TREASURY, TOWARD ELECTRONIC MONEY AND BANKING: THE ROLE OF GOVERNMENT (1996).

becomes whether the bank regulatory agencies should govern such entities or if some other governmental agency should regulate them.

IV. THE ROLE OF REGULATORY AGENCIES

In the midst of advancements in using the Internet for banking services, federal and international banking regulators continue to evaluate their roles in managing and monitoring electronic commerce, money, and more specifically, electronic banking. As new technology emerges everyday, more and more regulatory agencies try to find ways to guide the institutions they govern. There are also interagency bodies, such as the Federal Financial Institutions Examination Council ("FFIEC") that are empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions.[87] The FFIEC plays an important role in disseminating wide-spread guidance among the federal agencies. There are also international groups, such as the Bank for International Settlement, ("BIS"), who try to promote standards and principles regarding banking. In the United States, the Federal Reserve System, the Office of the Comptroller of the Currency ("OCC"), and the FDIC have continued to address the development of electronic banking and money systems and the appropriate U.S. government involvement. These three agencies have different roles, but they all regulate financial institutions. The FDIC is an independent agency that focuses on insuring banks. The OCC focuses on chartering national banks, and is part of the Department of the Treasury. The Federal Reserve System is an independent agency that focuses on monetary stability. Although these agencies have separate and distinct purposes, they often work together to promote a secure national banking system. For example, the FDIC has regulations to ensure a bank is safe and sound in order to be insured, while the OCC has regulations to ensure our national banking system is secure and stable.

On the global front the Group of Ten Nations ("G-10") and the BIS, are taking an active role in the regulation, and management of electronic

87. "The Federal Financial Institutions Examination Council (Council) was established on March 10, 1979, pursuant to the title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630." The FFIEC is empowered to prescribe uniform principles, standards and report forms for the Board of Governors of the Federal Reserve System, ("FRB"), the Federal Insurance Corporation, ("FDIC"), the National Credit Union Administration ("NCUA"), the Office of the Comptroller of the Currency ("OCC"), and the Office of Thrift Supervision ("OTS"). *See FFIEC Mission Statement* (visited Dec. 21, 1998) <http://www. ffiec.gov/mission.html>.

banking.[88] Working together, these organizations must lead individuals, corporations, and banking entities through these changing times.

A. *The Bank for International Settlements and the Basle Committee*

The Internet is helping to drive the integration of financial markets worldwide. This integration depends highly on the world's banks, its regulators, and the system's overall financial stability. The world's oldest international financial organization that addresses globalization of financial markets is the BIS.[89] It primarily promotes the cooperation of central banks and fosters international financial stability.[90] The BIS is owned and controlled by central banks and other international financial institutions.[91] The Board of Directors is comprised of the Governors of the central banks of Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom, and the Chairman of the Board of Governors of the United States Federal Reserve System.[92] As of March 1998, forty-five central banks have voting rights at the general meetings of the BIS.[93]

In promoting the stability of the international monetary and financial systems, the BIS has been involved in the efforts of such groups as the G-

---

88. *See generally Group of Ten, Electronic Money* (Visited Dec. 26, 1998) <http://www.bis.org/publ/gten01.html>.

89. *The Bank for International Settlements* (visited Dec. 26, 1998) <http://www.bis.org/about/prof-gh.htm> [hereinafter *Bank for International Settlements*].

90. *Id.*

91. *Id.*

92. *Id.*

93. Forty-five central banks included:

> all the G-10 central banks, namely those of Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom and the United States of America - and the central banks of Australia, Austria, Brazil, Bulgaria, China, the Czech Republic, Denmark, Estonia, Finland, Greece, Hong Kong, Hungary, Iceland, India, Ireland, Korea, Latvia, Lithuania, Mexico, Norway, Poland, Portugal, Romania, Russia, Saudi Arabia, Singapore, Slovakia, South Africa, Spain and Turkey, together with the Central Bank of Bosnia and Herzegovina, the Croatian National Bank, the National Bank of the Republic of Macedonia, and the Bank of Slovenia, which have been issued shares of the Bank pending a comprehensive settlement of all outstanding questions in connection with the legal status of the suspended Yugoslav issue of the Bank's capital.

Id.

10.[94] The G-10 is comprised of eleven industrial countries: Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom, and the United States.[95] These countries consult and cooperate on economic, monetary, and financial matters.[96] In 1975, the G-10 set up a committee to improve collaboration between bank supervisors known as the Basle Committee on Banking Supervision ("Basle Committee").[97] The Basle Committee provides a forum of discussion on the handling of specific banking supervision issues, coordinates the sharing of supervisory responsibilities, and seeks to enhance standards of supervision.[98] The BIS has participated in G-10 meetings since the Basle Committee was formed, because the Governors of the G-10 central banks meet regularly at the same time as the Basle monthly meetings.[99]

In March 1998, the Basle Committee took an initial step in reviewing supervisory issues related to technological advances. The Basle Committee distributed an assessment of the risks, and recommended approaches to risk management in electronic banking and electronic money activities to supervisors worldwide.[100] The risk management document suggests that "operational risk, reputational risk, and legal risk [are] the most important risk categories for electronic banking and electronic money."[101]

The risk management document identified operational risk as a risk category that must be addressed in dealing with electronic banking and electronic money. "Operational risk arises from the potential for loss due to significant deficiencies in system reliability or integrity."[102] Operational risk

---

94. The General Arrangements to Borrow ("GAB") of 1962, under which 10 member countries of the International Monetary Fund ("IMF"), including Switzerland, agreed to make resources available to the IMF outside their quotas, led to the countries participating in the GAB being known as the Group of Ten ("G-10"). *Bank for International Settlements, supra* note 89. Since 1963, the G-10 has been a principal forum for discussion of international monetary questions. *Id.*

95. *Id.*

96. *Id.*

97. *See* Report from Basle Comm. on Banking Supervision, *The Year 2000: A Challenge for Financial Institutions and Bank Supervisors* (Sept. 1997) <http://www.bis.org/publ/bcb531.pdf> (as of Feb. 20, 1999 this site no longer available).

98. *Id.*

99. *Id.*

100. Basle Committee on Banking Supervision, *Risk Management for Electronic Banking and Electronic Money Activities* (visited Dec. 24, 1998) <http://www.bis.org/publ/bcbs35.htm> [hereinafter *Risk Management for Electronic Banking*].

101. *Id.*

102. *Id.*

includes security risks that have the potential of both external and internal attacks and misuse of a bank's computing system.[103] Controlling access to a bank's system has become increasingly difficult with the expansion of computer capabilities and the accessibility of a public network, such as the Internet. Not only is there a potential for tremendous monetary loss, but there is also the potential for tremendous liability in fraudulently created activities. Operational risk also includes risks associated with a bank's system design, implementation, and maintenance.[104] The rapid change in information technology poses the risk that a system adequate today will not be adequate tomorrow.[105] Even computer software given to customers for online banking can quickly become obsolete and require updates.[106] Further, involvement of customers increases the potential of customer misuse of products and services.[107] The amount of services and products that are available to the customer is expanding everyday. Customers must be educated about necessary security precautions that should be taken, or else the risk of a security breach is heightened. Operational risk also includes customer misuse of banking products and services.[108] An uneducated customer can unintentionally open the door for security breaches by conducting financial transactions in a non-secure electronic environment. Criminals may then gain access to the financial transaction. Such access may lead to financial losses both to the customer and to the bank.[109]

Another risk category is reputational risk, that is, "the risk of significant negative public opinion that results in . . . critical loss of funding [for the bank] or [a loss of] customers."[110] Reputational risk can arise from systems or products not working properly, or from a significant security breach.[111] It also can arise from mistakes, malfeasance, and fraud by third parties. Reputational risk can be significant for a single bank and can also be significant for the banking system as a whole. Such risk can lead to extreme public distrust of *any* bank's ability to conduct business on the Internet. This

---

103. *Id.*
104. *Id.*
105. *Risk Management for Electronic Banking*, *supra* note 100.
106. *Id.*
107. *Id.*
108. *Id.*
109. *Id.*
110. *Risk Management for Electronic Banking*, *supra* note 100.
111. *Id.*

distrust will hinder both the growth of banking on the Internet, and the growth of electronic commerce collectively.[112]

A third category of risk identified by the Basle Committee is the legal risk arising from violations of laws, rules, regulations, or prescribed practices.[113] Legal risk also involves the lack of established legal rights and obligations of parties in an electronic transaction.[114] Given the fact that electronic transactions and electronic money are relatively new, no one is sure of the rights and obligations of the parties involved, and what type of consumer protection applies to the transaction.[115] There is also a question regarding the validity of agreements reached through an electronic medium, because technological advances such as digital signature and encryption methods that validate an agreement are still evolving. Further, there is the risk of customer disclosure and inadequate privacy protection. Moreover, the Basle Committee points out that the traditional banking risks may also arise in banking on the Internet, especially with the use of electronic money.[116] Cross-border risks and issues can arise for banks as well.[117] Customers across national borders expose the banks to different and/or additional regulatory requirements.[118]

In assessing the risks above, the Basle Committee sets out possible steps that bank management can take to manage and control risks associated with banking on the Internet and the use of electronic money.[119] The Basle Committee suggests such measures as developing a security policy that lays out the bank's plan and defines the bank's security risk tolerance.[120] Putting various security measures into place, such as encryption, passwords, firewalls, virus controls, and employee screening can help to prevent both internal and external attacks, as well as the misuse of electronic money and financial transactions.[121] In deterring security issues, a bank should consider

---

112. *Id.*

113. *Id.*

114. *Id.*

115. *Risk Management for Electronic Banking*, *supra* note 100.

116. Traditional banking risks include credit risk, liquidity risk, interest rate risk, and market risk. *Id.*

117. *Id.*

118. *Id.*

119. *Id.*

120. *Risk Management for Electronic Banking*, *supra* note 100.

121. A detailed discussion regarding security measures can be found in Bank for International Settlements, *Security of Electronic Money*, Aug. 1996 <http://www.bis.org/publ/cpss18.html> [hereinafter *Security of Electronic Money*].

a combination of security measures as opposed to just one.[122] For example, a firewall[123] can screen, or even prevent incoming messages but it does not fully protect against virus-infecting programs that can be downloaded from the Internet.[124] A better solution would be to implement virus protection protocols and software that also integrates well with the firewall software. The Basle Committee suggested that in dealing with operational, reputational, and legal risks, a bank's management should communicate with staff members about key provisions regarding banking on the Internet, while the technical staff communicates with the bank management on how systems work and are designed.[125] Protocols for the evaluating and testing of products and services should be established and performed regularly, and should include educating customers on those products and services. While electronic banking and electronic money rely on external entities for hardware and software, banks should insist that such providers conduct regular testing and have fallback procedures in case of failure or invasion by criminals.[126] Basically, banks should constantly monitor and test their systems and keep abreast of the latest electronic banking technologies. The BIS and the Basle committee are both providing strong guidelines for nations to follow while at the same time promoting electronic banking.

B. *The Federal Reserve System*

"The Federal Reserve System is the central bank of the United States. It was founded by Congress in 1913 to provide the nation with a safer, more flexible, and more stable monetary and financial system; over the years, its role in banking and the economy has expanded."[127] The Federal Reserve Board, which governs the Federal Reserve System, has been willing to allow financial institutions to move forward with new technology, such as smart cards and electronic banking.

The Federal Reserve Board has taken other steps that will have an effect on the development of electronic banking and electronic money activities in the United States. For example, the Board approved a request by various holding companies and banks, subject to the Bank Holding

---

122. *Id.*

123. A "firewall" is a combination of hardware and software that screens and limits external access to internal systems connected to open networks such as the Internet. *Id.* at 12.

124. *Id.*

125. *Id.* at 13.

126. *Security of Electronic Money*, *supra* note 121 at 15.

127. *About Federal Reserve System* (visited Mar. 25, 1998) <http://www.bog.frb.fed.us/aboutfrs.html>.

Company Act,[128] to obtain a voting interest in Integrion Financial Network, LLC of White Plains, New York ("Integrion").[129] Royal Bank of Canada, Northwest Corporation, and Stichting Prioriteit ABN AMRO Holding and its subsidiaries requested to acquire more than five percent of the voting interest in Integrion.[130] The joint venture also includes twelve national banks,[131] one savings and loan holding company,[132] and Gemini Management Corporation, a subsidiary of International Business Machines Corporation ("IBM"). Integrion was organized to design, develop, and operate a data processing and transmission system, through which customers of banks can engage in home banking and other electronic financial services with the financial institution.[133] The Federal Reserve Board's order focused on the public benefits of allowing such a joint venture.[134] Since the proposed activities were data processing and transmission activities which were permissible for

128. The Bank Holding Company Act authorizes bank holding companies to engage in nonbanking activities provided that such activities are "closely related to [the business of] banking." The act also states that the bank's activities must "produce benefits to the public, such as greater convenience, increased competition, or gains in efficiency, that outweigh possible adverse effects, such as undue concentration of resources, decreased or unfair competition, conflict of interests, or unsound banking practices." Bank Holding Act, 12 U.S.C. § 1843(4)(c)(8) (Supp. 1998).

129. *Federal Reserve Press Release - December 2, 1996* (visited Jan. 14, 1999) <http://www.bog.frb.fed.us/boarddocs/press/BHC/1996/199612022/> [hereinafter *Press Release*].

130. *Id.*

131. The national banks included:

> Bank of America NT & SA; NationsBank, N.A.; Keybank, N.A.; Bank One, Columbus, N.A.; Mellon Bank, N.A.; Barnett bank, N.A.; First Bank, N.A.; PNC Bank, N.A.; Michigan National Bank; The First National Bank of Chicago; Comerica Bank – Ann Arbor, N.A.; and Fleet National Bank. Each of these national banks has applied to the Office of the Comptroller of the Currency of the Currency to invest in Integrion through an operating subsidiary of the bank.

Id.

132. The savings and loan holding company is Washington Mutual, Inc., that had to provide notice of its intent to be involved with Integrion with the Office of Thrift Supervision. *Id.*

133. Customers can connect to Integrion, which serves as a gateway to the financial institution, using such devices as personal computers, touch-tone phones, or any other electronic communication devices. *Id.* The customer can connect through a private communication network, through financial software programs, or through the Internet. *Press Release*, *supra* note 129.

134. *Id.*

bank holding companies,[135] the Federal Reserve Board believed that such a venture would enhance consumer banking convenience by expanding the availability of remote banking services and providing new services.[136] Such a venture is also advantageous for financial institutions, because Integrion offers a secure means of banking online,[137] as well as a selection of software or programs for home banking.[138] As stated by the chairman and CEO of IBM, Integrion will reach sixty million households and give those sixty million people a reason to use the Internet for home banking.[139] Through policy, the Federal Reserve is encouraging the use of electronic banking at this time, while it monitors the effect on the United States economy and its financial systems.

C. *The Federal Deposit Insurance Corporation*

The FDIC has been insuring deposits and promoting safe and sound banking practices since 1934.[140] The FDIC:

---

135. Engaging in data processing and data transmission activities is permissible under section 225.28 of the Federal Reserve Board's Regulation Y, 12 C.F.R. § 225.28 (1998) and section 4(c)(8) of the Bank Holding Act. 12 U.S.C. § 1843 (c)(8) (Supp. 1998).

136. *Press Release*, *supra* note 129.

137. Integrion solves many security issues by providing both public Internet access as well as private networks. *15 North American Banks and IBM Form Company to Offer Electronic Banking and Commerce Services* (visited Sept. 9, 1996) <http://www.ibm.com/News/bankingpr.html>.

138. The customer can choose from whatever financial management software or Internet browser program he or she would like to use. Integrion is intended to be compatible with such software as Microsoft Money, Quicken and Managing Your Money, as well as Internet browsers like Netscape Navigator and Microsoft Explorer. *Id.*

139. Amanda Meffert, *Banking by IBM* (visited Jan. 4, 1999) <http://www.worth.com/articles/Integrion.html>.

140. *FDIC Symbol of Confidence* (visited Feb 17, 1999) <http://www.fdic.gov/consumers/symbol/index.html> [hereinafter *Symbol of Confidence*]. The FDIC was created to "restore stability to a financial system that had seen over 9,000 bank failures and a severe contraction in economic activity in the four years following the stock market crash of 1929." *Id.* "But in passing this legislation, President Roosevelt and Congress became concerned about the potential for deposit insurance to create 'moral hazard,' which is the tendency of people to take on more risk when insured" and reduce their incentive to monitor and discipline banks for excessive risk-taking. *Id.* Consequently, to limit the potential loss to the government, "the legislation limited the amount of insurance—to $2,500 in 1934, $5,000 in 1935—and increased the amount of federal supervisory authority over insured institutions (FDIC 1984)." *Confidence for the Future: An FDIC Symposium* (visited Dec. 26, 1998) <http://www.fdic.gov/publish/symp/backpap/panel1.html> [hereinafter *Confidence for the Future*]. "For the next 50 years, public confidence in the banking system was maintained even through serious recessions and other major economic shocks." *Id.*

> Promotes the safety and soundness of insured depository institutions and the U.S. financial system by identifying, monitoring and addressing risks to the deposit insurance funds. The FDIC also is the primary federal regulator of about 6,000 state-chartered "nonmember" banks (commercial and savings banks that are not members of the Federal Reserve System).141

"The heart of the FDIC's mission is to maintain stability and public confidence in the nation's banking and thrift systems."[142] "The FDIC sign-posted in insured financial institutions across the country has become a symbol of confidence."[143] "Today, the FDIC insures deposits of up to $100,000 in virtually all United States banks and savings associations."[144]

New technologies raise a wide range of supervisory issues. The FDIC does not desire to impose regulatory restrictions that can hinder the development of such emerging technology, but it does recognize the importance of providing guidelines for new products and services.[145] The FDIC has recognized the inherent risks of stored-value card systems, electronic banking in general, and Internet-based banks. These rapidly emerging banking activities on the Internet pose new questions regarding the scope of deposit insurance and its applicability to electronic funds. The purpose of federal deposit insurance is to maintain stability in the financial system and thus promote economic growth.[146] Deposit insurance also protects depositors from losses associated with bank failures and ensures the viability of smaller banks.[147]

One way to keep such confidence is by assuring consumers and merchants that funds are available for a transaction. For a deposit of funds to be recognized by the FDIC, it must qualify as a "deposit" under the Federal Deposit Insurance Act.[148]

---

141. *Symbol of Confidence*, *supra* note 140.

142. *Confidence for the Future*, *supra* note 140.

143. *Id.*

144. *Symbol of Confidence*, *supra* note 140.

145. Nicholas J. Ketcha, Jr., *Examination Guidance on the Safety and Soundness Aspects of Electronic Banking Activities-FDIC Financial Institution Letter FIL-14-97* (visited Feb. 26, 1997) <http://www.fdic.gov/banknews/fils/1997/fil9714.html> [hereinafter *FDIC Letter FIL-14-97*].

146. *Confidence for the Future*, *supra* note 140.

147. *Id.*

148. Under section 3(l) of the FDIA, "the term 'deposit' means"—

> (1) the unpaid balance of money or its equivalent received or held by a bank or savings association in the usual course of business and for which it has given or is obligated to give credit, either conditionally or unconditionally, to a commercial, checking, savings, time, or thrift account,

The FDIC published General Counsel Opinion No. 8 to address the issue of, "whether and to what extent the funds or obligations underlying stored value cards constitute 'deposits' within the meaning of section 3(l) of the Federal Deposit Insurance Act (FDIA) and are therefore assessable and qualify for deposit insurance."[149] General Counsel Opinion No. 8 identifies four types of stored value systems: 1) Bank Primary—Customer Account

---

or which is evidenced by its certificate of deposit, thrift certificate, investment certificate, certificate of indebtedness, or other similar name, or a check or draft drawn against a deposit account and certified by the bank or savings association, or a letter of credit or a traveler's check on which the bank or savings association is primarily liable: Provided, that, without limiting the generality of the term "money or its equivalent", any such account or instrument must be regarded as evidencing the receipt of the equivalent of money when credited or issued in exchange for checks or drafts or for a promissory note upon which the person obtaining any such credit or instrument is primarily or secondarily liable, or for a charge against a deposit account, or in settlement of checks, drafts, or other instruments forwarded to such bank or savings association for collection.

(2) trust funds as defined in this chapter received or held by such bank or savings association, whether held in the trust department or held or deposited in any other department of such bank or savings association.

(3) money received or held by a bank or savings association, or the credit given for money or its equivalent received or held by a bank or savings association, in the usual course of business for a special or specific purpose, regardless of the legal relationship thereby established, including without being limited to, escrow funds, funds held as security for an obligation due to the bank or savings association or others (including funds held as dealers reserves) or for securities loaned by the bank or savings association, funds deposited by a debtor to meet maturing obligations, funds deposited as advance payment on subscriptions to United States Government securities, funds held for distribution or purchase of securities, funds held to meet its acceptances or letters of credit, and withheld taxes: Provided, That there shall not be included funds which are received by the bank or savings association for immediate application to the reduction of an indebtedness to the receiving bank or savings association, or under condition that the receipt thereof immediately reduces or extinguishes such an indebtedness.

(4) outstanding draft (including advice or authorization to charge a bank's or a savings association's balance in another bank or savings association), cashier's check, money order, or other officer's check issued in the usual course of business for any purpose, including without being limited to those issued in payment for services, dividends, or purchases.

Federal Deposit Act, 12 U.S.C. § 1813(l)(1)–(4) (1994).

149. Federal Deposit Ins. Corp. General Counsel's Op. No. 8; Stored Value Cards, 61 Fed. Reg. 40,489, 40,490 (1996). *See also* Federal Deposit Act, 12 U.S.C. § 1813(l)(1)–(4) (1994).

Systems; 2) Bank Primary—Reserve Systems; 3) Bank Secondary—Advance Systems; and 4) Bank Secondary—Pre-Acquisition Systems.[150]

In the Bank Primary—Customer Account Systems, "funds underlying the stored value card could remain in a customer's account until the value is transferred to a merchant or other third party."[151] The merchant or third party then collects the funds from the customer's bank.[152] General Opinion No. 8 states that, "the funds underlying Bank Primary—Customer Account Systems [are] deposits under section 3(l)(1) of the FDIA, 12 U.S.C. 1813(l)(1)."[153]

In Bank Primary—Reserve Systems, a value is downloaded onto a card and funds are withdrawn from a customer's account or paid directly by the customer.[154] These funds are then paid into a reserve or general liability account at the financial institution to pay merchants or other payees as they make claims.[155] General Opinion No. 8 states that funds underlying Bank Primary—Reserve Account Systems are not "deposits" within the meaning of section 3(l)(1) of the FDIA.[156] The opinion stated that such funds are not credited to, or obligated to be credited to a commercial or thrift account.[157]

In Bank Secondary Systems,[158] the electronic value is created by a third party and the funds underlying the electronic value are ultimately held by such third party.[159] In such systems, depository institutions act as intermediaries in collecting funds from customers in exchange for electronic value. In Bank Secondary Systems, the electronic value is provided to the institution to have available for its customers. In Bank Secondary—Advance Systems, the customers exchange funds for electronic value while the funds are held for a short period of time and then forwarded to the third party.[160] General Opinion No. 8 states that funds underlying Bank Secondary—Advance Systems are not "deposits" within the meaning of section 3(l)(1) of the FDIA, because the liability is owed to the third party and the bank is

150. 61 Fed Reg. at 40,490 (1996).
151. *Id.*
152. *Id.*
153. *Id.* at 40,492; *see also* 12 U.S.C. § 1813(l)(1).
154. 61 Fed. Reg. at 40,494.
155. *Id.*
156. *Id.*; *see also* 12 U.S.C. § 1813(l)(1).
157. 61 Fed Reg. at 40,494.
158. In Bank Secondary Systems, the depository institution may have a contingent liability to redeem the electronic value from consumers and merchants. As such electronic value is redeemed, the institution may in turn exchange the electronic value for funds with the third party. *Id.*
159. *Id.*
160. *Id.*

holding the funds in the usual course of business.[161] However, if the funds are for a "specific purpose" and are held by the bank for a specific purpose, then the funds would be considered a deposit.[162]

In Bank Secondary—Pre-Acquisition Systems, the depository institution exchanges its own funds for electronic value from a third party, and then exchanges electronic value for funds with the bank's customers.[163] General Opinion No. 8 states that since the funds underlying Bank Secondary—Pre-Acquisition Systems are received and held by a third party and the depository institution, the funds are not "deposits" within the meaning of section 3(l)(1) of the FDIA.[164]

Regarding "electronic money," the FDIC is unwilling to recognize a deposit of funds underlying most stored value systems as a "deposit."[165] Not recognizing the funds as a "deposit" means that those merchants who use a stored value system are not assured that the transaction is properly funded and that they will be paid for their services or goods. Therefore, the merchants are reluctant to accept transactions using stored value systems, consumer confidence is jeopardized, and electronic commerce is hindered by using this type of electronic money system.

There are inherent risks with the emergence of electronic banking. One way the FDIC attempted to reduce those risks was by establishing electronic banking examination procedures. The examination procedures addressed the safety and soundness aspects, as well as associated risks of electronic banking.[166] The examination procedures were issued to FDIC examiners on January 29, 1997.[167] The FDIC produced guidelines as part of a comprehensive four-part approach to evaluating the wide range of risks that are inherent in electronic based activities. The first approach is the examination procedures with the remaining parts being: 1) a training program to educate FDIC examiners on how to use the examination procedures; 2) another set of procedures that address the technical aspects of electronic banking; and 3) a program to develop internal technical expertise.[168] The examination procedure included three levels of examination based on the sophistication of the institution's electronic

161. 12 U.S.C. § 1813(l)(1).

162. *Id.*

163. 61 Fed. Reg. at 40,494.

164. 12 U.S.C. § 1813(l)(1).

165. Federal Deposit Ins. Corp. General Counsel's Op. No. 8, *supra* note 149.

166. FEDERAL DEPOSIT INS. CORP., ELECTRONIC BANKING: SAFETY AND SOUNDNESS EXAMINATION FOR ELECTRONIC BANKING (Jun. 1998) [hereinafter SAFETY AND SOUNDNESS].

167. *FDIC Letter FIL-14-97*, *supra* note 145.

168. *Id.*

banking capabilities.[169] The examination procedures required an evaluation of six different areas of a bank's electronic banking capabilities.[170] The areas to be evaluated include the bank's planning efforts and implementation,[171] operating policies and procedures,[172] audit procedures,[173] legal and regulatory matters,[174] the bank's administration and system operations,[175] and vendors and outsourcing.[176] The FDIC's examination procedures, which the FDIC uses to review the worthiness of banking institutions for insurance coverage, contain key guidelines in maintaining the safety and soundness of the banking system.[177] These practices ensure that the electronic and conventional banking systems are secure and sound.

The FDIC is also addressing the risk associated with an Internet-based bank, or any institution that represents itself as a legitimate financial institution. The FDIC has recently launched a "Suspicious Internet Banking" web site to help detect potentially fraudulent Internet banking activity.[178] The web site provides the consumer and the industry a "user-

---

169. The three levels were: 1) information-only systems; 2) electronic information transfer systems; and 3) electronic payment systems. SAFETY AND SOUNDNESS, *supra* note 166, at 3.

> Level I systems can simply provide information as defined by the publisher or allow transmission of non-sensitive electronic mail (information-only systems); Level II systems can allow users to share sensitive information and communicate (electronic information transfer systems and Level III systems can facilitate electronic funds transfer and other financial transactions (electronic payment systems).

Id.

170. *Id.*

171. Planning and implementation risks include inadequate decision processes, system design and capabilities not meeting customer demands, increased competition with nonfinancial entities, and uncertain applicability of blanket bond/other insurance coverage to electronic activities. *Id* at 8.

172. Operating policies and procedures risks include managerial incompetence relative to electronic activities, and existing policies that may not address and control confidential electronic information and electronic channels. *Id.*

173. The internal control structure of the institution is critical to prevent, detect, and correct information security breaches. SAFETY AND SOUNDNESS, *supra* note 166, at 8.

174. Each system must be evaluated to determine its capability for initiating, completing, and enforcing legal documents and financial transactions. *Id* at 3.

175. Guidelines relating to access levels and record retention must be established and monitored on a regular basis. Efforts should be made to educate and support the consumers. *Id.*

176. Even if an institution outsources to a third party, the burden is still on management to supervise and control all aspects of the bank's systems. *Id.*

177. *Id.* at 13.

178. *Reporting Suspicious Internet Banking Sites* (visited Dec. 25, 1998) <http://www.fdic.gov/consumer/suspicious/sspcious.html>.

friendly" vehicle for reporting any entity that is misrepresenting itself as a federally insured depository institution.[179]

D. *The Office of the Comptroller of the Currency*

The Office of the Comptroller of the Currency ("OCC") charters, regulates, and supervises national banks to ensure a safe, sound, and competitive national banking system.[180] The OCC is an agency within the U.S. Department of the Treasury that continues to remove barriers in delivering banking services over the Internet.[181]

In the last several years, the OCC has continued to foster financial institutions delivering bank as well as nonbank services. In 1996, the OCC issued a bulletin that set forth guidelines relating to stored-value systems.[182] The bulletin not only describes different kinds of stored-value systems, but it also discusses risks associated with participating in stored-value systems.[183] The OCC approved the involvement of national banks in such stored-value systems as the Mondex system.[184] The Mondex system,[185] which is a smart card system, can transfer value from one card to another card.[186] The card uses a digital signature to authenticate a transaction.[187] It can also be used to make payments over the Internet. Mondex benefits consumers as well as merchants, because Mondex cash is easily reloadable and transferred, and

---

179. *Click on FDIC Web Site to Help Fend Off Fraudulent Internet Banks* (visited Dec. 25, 1998) <http://www.fdic.gov/consumer/consnews/sum98/fending.html>.

180. *Comptroller or the Currency Administrator of National Banks* (visited Feb. 20, 1999) <http:// www.occ.treas.gov>.

181. *See, e.g.*, OCC Guidance on Stored-Value Card Systems, O.C.C. Bulletin 96-48, 5 Fed. Banking L. Rep. (CCH) 49-971 (Sept. 10, 1996)) (source on file with author).

182. *Id.*

183. The OCC divides risks into three categories: 1) transaction risk, that includes the adequacy of internal controls, data integrity, transaction rules, employee performance, and operating processes; 2) strategic risk that includes business goals and strategies; and 3) reputation risk, that includes negative public opinion. *Id. See also OCC Issues Guidance on Smart Card/Stored Value Card Risks*, O.C.C. News Release 96-94 (Sept. 10, 1996).

184. Fisher-Haydis & Yancey, *supra* note 5, at 92.

185. The Mondex is a global electronic cash company formed by the U.K. based National Westminister Bank. USA TODAY, *Mondex Pitches New Way to Spend Money* (visited Dec. 17, 1998) <http://usatoday.com/money/wealth/consumer/mcw002.html>. Mondex is not technically money and it is not legal tender, because there is no requirement to accept it. *Id.*

186. All Mondex cards are considered to be little "purses" with independent stores of value. *Id.*

187. *Id.*

improves the efficiency at the point of sale.[188] The OCC recognized the issuance and redemption of electronic stored value as "functionally equivalent" or a "logical outgrowth" of the business of banking by a national bank.[189]

In 1997, the OCC approved the first virtual national bank charter.[190] Houston based CompuBank, N.A., was approved to deliver products and services to customers primarily through electronic means, and has applied to the FDIC for deposit insurance.[191] Such approval was in alignment with the OCC's decision to allow a national bank to provide electronic data interchange services, as well as electronic fund transfers.[192]

The OCC has recently issued bulletins that stress the importance of risk management in dealing with technology in general,[193] and especially with personal computer banking.[194] The guidance was put out to help the estimated 2600 national banks that engage in some form of personal computer banking.[195] The OCC identified online transactions as the most common source of risk that includes unauthorized interceptions, data alteration, system failures, and computer viruses.[196] The OCC recommends that national banks implement risk management practices that establish policies and procedures, internal controls, and system monitoring.[197] To assist in this effort, the OCC issued guidelines for examiners to follow when

188. *Id.* Making a payment through Mondex takes less than three seconds to complete and the payments are exact. USA TODAY, *supra* note 185. Mondex also reduces the security risks of storing and transporting currency. *Id.* It can even "hold up to five different currencies." *An Overview of Mondex* (visited Jan. 14, 1999) <http://www.amdahl.com/doc/products/smartcard/overview.html>.

189. In evaluating whether the proposed activity was within the "business of banking," the OCC evaluated: 1) whether the activity was "'functionally equivalent' to or a 'logical outgrowth' of a recognized banking activity; 2) whether the activity would 'respond to customer needs or otherwise benefit the bank or its customers;' and 3) whether the activity 'involve[s] risks similar in nature to those already assumed by banks.'" Wilson, *supra* note 14, at 714.

190. *OCC Says OK to First Virtual National Bank Charter*, 16 No. 18 BANKING POL'Y REP. 6, 6 (Sept. 1997) (source on file with author).

191. *Id.*

192. The OCC revised 12 C.F.R. part 7 to include the "activities, functions, products and services provided by banks via electronic means and facilities." 12 C.F.R. § 7.1019 (1998). Prior to the revision, 12 C.F.R. part 7 authorized banks to utilize data processing equipment to analyze financial data for itself and others. *See* 61 Fed. Reg. 4,853 (1996) (codified at 12 CFR § 7.1019 (1998)).

193. *Id.*

194. *OCC Banking Bulletin No. 98-38* (visited Jan. 18, 1999) <http://www.occ.treas.gov/ftp/bulletin/98-38.txt>.

195. *Id.*

196. *Id.*

197. *Id.*

reviewing a bank's technology risk management procedures.[198] The Technology Risk Management guidance is one of the agency's most comprehensive statements on technology issues that provides national banks and examiners with a framework for managing technology as a vital part of the bank's services. The OCC encourages security policies, awareness, and controls that result in reliable access control, user authentication, data integrity, data privacy, and transaction verification.[199] The guidance also suggests system "firewalls" to prevent system penetration.[200] Examiners will evaluate senior management regarding sufficient knowledge and skills, as well as their planning process to manage technology-related risks.[201]

The bulletin also addresses using third party personal computer systems. The bulletin stresses the need to manage and review the third party's financial conditions, its internal control practices, and rights if the third party system should fail.[202] Finally the OCC encourages all national banks to keep abreast of new developments in electronic banking.[203] Such monitoring should include both state and federal changes and implementation of rules and regulations.[204]

The OCC recognizes the importance of the banking industry's showing of leadership in advancements in electronic banking. At the beginning of 1998, the OCC approved the application of a Utah Bank, Zions First National Bank, to be the first financial institution to offer digital signature products to its customers.[205] It has also been working to address consumer concerns by analyzing findings by such groups as the Consumer Electronic Payments Task Force which the Treasury Secretary asked the OCC to chair in 1996.[206] Such findings show that consumers want adequate disclosure about a company and less disclosure about themselves. At the same time, the

---

198. *See OCC Warns Banks on Technology Risks* (visited Dec. 25, 1998) <http://www.occ.treas.gov/ftp/release/98-13.txt> [hereinafter *OCC Warns*].

199. *Id.*

200. *Id.*

201. These risks include risks associated with computer hardware, software applications, and telecommunications services. *Id.* The risks fall into four categories: transactions, strategic, reputation, and compliance risks. *Id.*

202. *OCC Warns*, *supra* note 198.

203. *Id.*

204. *Id.*

205. *OCC Approves a National Bank to Certify Digital Signatures* (visited Dec. 22, 1998) <http://www.occ.treas.gov/ftp/release/984.htm>. Digital signatures are used for electronic authentication of the sender of an electronic message. *Id.* As stated by Comptroller of the Currency, Eugene Ludwig, "The ability to verify and authenticate electronic signatures is essential to the development of electronic commerce and electronic banking." *Id.* The Utah bank plans to focus on certification services involving corporate and government documents. *Id.*

206. *See Consumer Electronic Payment Task Force* <http://www.occ.treas.gov/>.

OCC has recognized the need for limiting government restrictions and providing predictable government involvement whenever it is necessary.[207] The OCC, through its broad range of banking policies, is promoting self-regulation and is diligently working to show that public concerns about privacy and disclosure of information can be addressed without requiring externally imposed government solutions.[208]

V. ELECTRONIC MONEY AND BANK RELATED ISSUES

A. *Nonbank Institutions as Financial Providers*

There are many types of financial institutions, including federal and state chartered depository institutions, check-cashing organizations, insurance companies, and brokerage firms.[209] All of these institutions are subject to extensive state and federal regulations to protect the integrity of our monetary system. The dilemma is that if nonbank entities are not classified and regulated as banks, but are allowed to provide limited bank-like services put our monetary system is at risk because it is through regulation that federal agencies protect the consumer and the United States financial system. Part of the problem is that the federal banking regulations do not provide a consistent definition of the term "bank." For example, the Bank Holding Company Act defines a "bank" as any FDIC insured bank or any institution that accepts demand deposits and engages in the business of making commercial loans.[210] Under the Federal Deposit Insurance Act, a "bank" includes an institution chartered as a bank or any other "banking" institution that is engaged in the business of receiving deposits.[211] Under the National Bank Act, core "banking" functions generally include the receiving of deposits, paying checks, and making loans.[212] If a standard definition is established, the issue then becomes whether nonbank entities qualify as a "bank" and should be required to meet banking regulations.

---

207. Julie L. Williams, *Remarks at the Banking Roundtable Lawyers Council, Washington, D.C.* (May 8, 1995) (visited Dec. 22, 1998) <http://www.occ.treas.gov/ftp/release/98-2d50a.txt.>.

208. *Id.*

209. Wilson, *supra* note 14, at 671.

210. Melanie L. Fein, *In Cyberbanking, When Do Non-Banks Become 'Banks'?*, 15 No. 5 BANKING POL'Y REP. 10, 10 (1996).

211. *Id.*

212. *Id.*

A number of nonbank entities currently offer a variety of bank-like services, including issuing and providing new electronic payment products such as stored value cards and digital cash.[213] Nonbank institutions have the potential to be high-risk operations which regulation must address in order to provide the consumer confidence and safety that traditional banking institutions provide to their customers. Many of these nonbank entities are using electronic money to provide different types of services. Again, DigiCash and CyberCash Inc., have developed Internet payment systems and are continuing to establish a trusted link between the Internet and banks.[214] Therefore, it is likely that nonbank entities will issue electronic value in exchange for United States currency. This situation generates two important questions: 1) Where is the U.S. currency stored that is exchanged for electronic value?; and 2) Is the U.S. currency insured while it is stored?

Just recently, the importance of these questions came into focus when DigiCash filed for bankruptcy protection under Chapter 11.[215] A traditional bank would have FDIC insurance. Currently, any currency held by a nonbank such as DigiCash is not insured by the FDIC and the nonbank retains control over it under a Chapter 11 ruling. Such a situation places our monetary system at risk and would have a negative impact on the growth of electronic commerce and Internet banking, because a lack of consumer confidence is fostered.

Under the current structure, the entity would have to qualify as a bank before federal banking regulators could examine and control the activities of the issuer.[216] As mentioned previously, the FDIC does not treat the funds stored in value cards as deposits and there is currently no indication that the FDIC will insure nonbank entities.[217] In addition, electronic money is yet to be considered legal tender.[218] Assuming the entities issuing smart cards and other electronic value do not qualify as banks, and are not covered by our federal banking regulations, then the question remains whether the bank

213. *See generally Digicash* (visited Jan. 14, 1999) <http://www.digicash.com/digicash/digicash/profile/index.html>.

214. *CyberCash - Free Wallet* (visited May 10, 1998) <http://www.cybercash.com/cybercash/consumers/wallet.html>.

215. *Welcome to DigiCash* (visited Jan. 14, 1999) <http://www.digicash.com/digicash/index.html>.

216. Federal Deposit Act, 12 U.S.C. § 1813 (1994).

217. 12 U.S.C. § 1813(3)(l) (Supp. 1997).

218. *Id. See also* Federal Deposit Ins. Corp., General Counsel's Op. No. 8; Stored Value Cards, 61 Fed. Reg. at 40,490 (1996).

regulatory agencies should extend their governance over such entities, or if some other form of governmental intervention is needed to regulate them.

With these institutions using "electronic money," it is imperative that such nonbanks be regulated and be required to adhere to the same standards as a bank. If electronic money is to become equivalent to legal tender, then it must also be as secure as money is today. Nonbank institutions providing such money and services must rise to the same standards as banks and provide the same level of consumer protection.

B. *Privacy Issues*

There are a number of privacy issues that arise for the financial institutions and the consumers. One issue is whether electronic banking services that are processed through the Internet compound the possibility of confidential account information being obtained or tampered with by third parties.[219] Another issue is the potential disclosure of personal information to third parties due to the consumer's unfamiliarity with new banking products.[220] The financial system relies on current privacy legislation to define the limits of a third party's legal right to access a person's financial information. However, current privacy legislation does not address the heightened privacy concerns raised by the use of electronic money on the Internet.[221] Current legislation includes the Privacy Act of 1974 ("Privacy Act"),[222] the Right to Financial Privacy Act of 1982 ("RFPA"),[223] and the Electronic Communications Privacy Act of 1986 ("ECPA").[224]

The Privacy Act protects an individual's private information, regulates the practices of federal agencies regarding personal information, and balances the individual's need for privacy and the government's need for such information to fulfill certain functions.[225] Each federal agency must

---

219. Robert G. Ballen & Thomas Fox, *The New Business of Banking: What Banks Can Do Now: Legal Issues in the New World of Cyberbanking*, 912 PRAC. LAW. INST. CORP. L. HANDBOOK SERIES 497, 503–4 (1995).

220. *Id.*

221. Catherine M. Downey, *The High Price of a Cashless Society: Exchanging Privacy Rights for Digital Cash?*, 14 J. MARSHALL J. COMPUTER & INFO. L. 303, 308 (1996).

222. In 1974, Congress enacted the Privacy Act, which was the first federal statute recognizing the need to balance an individual's concern for information privacy with the institutional practice of storing information in a computerized record-keeping system. 5 U.S.C. § 552(a) (1974).

223. 12 U.S.C. § 3402 (1982).

224. 18 U.S.C. § 2510 (1986).

225. H.R. REP. No. 95-1383 at 33–34 (1978).

register the existence of every federal data bank in the Federal Register.[226] Furthermore, no federal agency may disclose any record contained in its system to any other person or agency without the written request or consent of the individual.[227]

In 1982, Congress enacted the RFPA to further protect customer financial records.[228] Under the RFPA no government authority may have access to, or obtain copies of, information contained in the financial records of any customer from a financial institution, unless the customer authorizes such disclosure.[229]

The ECPA[230] protects the individual against the interception of electronic communications by an unauthorized person. Titles I and III of the ECPA pertain to common computer-to-computer communications, including the transmission of financial records or funds transfers among financial institutions.[231] Title I focuses on electronic communications, and thus directly applies to most of the data exchanged between parties using the Internet.[232] Title II states that a communications service provider "shall not knowingly divulge the contents of a communication" while in electronic storage when communications arrive electronically, and the service provider retains records solely for processing and storage.[233]

However, the potential for intrusions by unauthorized persons and exposure of a user's financial information is still possible on the Internet, which is beyond the protection of the ECPA. Without adequate privacy protections, transactions conducted on the Internet can be exposed to third parties. One solution is increased usage of encryption.[234] It can be argued that without encryption there will be widespread invasion of privacy, and increased criminal activity. Also, it can be argued that because consumers may not be familiar with the potential disclosure of personal information to

---

226. 5 U.S.C.A. § 552(a) (1998).

227. *Id.* at 3. However, there are several exceptions to the Privacy Act through which federal agencies can gain access to an individual's record to combat criminal activity. *Id.*

228. 12 U.S.C. § 3402 (1998). Furthermore, the Privacy Act allows an individual to copy, correct, and challenge his personal information stored in the data banks of the federal agencies. *Id.*

229. *Id.* In order to obtain a customer's financial records from a financial institution, the federal government must follow the procedural requirements of the RFPA and submit a written certification indicating its compliance. *Id.* However, the customer faces difficult obstacles in challenging or blocking the disclosure of his financial records, and must usually wait until after such disclosure to dispute the government's intrusion. *Id.*

230. 18 U.S.C. §§ 2510–18 (1994).

231. *Id.*

232. *Id.*

233. *Id.* § 2511(3)(a) (1994).

234. *See infra* text accompanying note 254.

third parties, regulatory agencies must take affirmative steps to protect the consumer.[235]

C. *Security Risks*

The Internet is "inherently insecure,"[236] and the typical person using the Internet is unaware of the risk, since a large portion of today's activities on the Internet is based on information retrieval. However, financial institutions face the difficulty of processing transactions in this same environment. Transactions occurring on the Internet are over a public network that is open and available to anyone, including criminals. A knowledgeable person could trap, change, and redirect information and transactions that occur on the Internet. The average person could not perform this type of criminal act because it takes special knowledge, software, and hardware tools to do so, but the number of people with these skills is growing every day. A cyber criminal may transfer funds into another account, make unauthorized purchases, or even obtain money from others. With voluminous transmissions and open travel over the Internet, all data transfers potentially can be read or monitored by a third party. In particular, there are "sniffer" systems that are available to anyone, that can be set up on any network at any port that look for and collect certain types of data.[237] While these systems are legitimately used in network management, the systems can also be used in illegitimate activities such as theft of credit card numbers or passwords.

Any connected data storage systems, and any data stored on an Internet server may be susceptible to compromise, if proper security precautions are not taken. Data integrity is also in jeopardy because the Internet can potentially allow those with specific knowledge and tools to alter or modify data during transmission.[238] There are other security risks associated with banking on the Internet. These include risks associated with authentication, non-repudiation, and access control.[239]

It is essential to be able to verify that a particular communication, transaction, or access request is legitimate and accurate.[240] This verification

235. Ballen & Fox, *supra* note 219 at 503.

236. FDIC, Division of Supervision FIL-131-97: *Security Risks Associated with the Internet* (Dec. 1997) <http://www.fdic.gov/banknews/fils/1997/fil97131.html> [hereinafter *Security Risks*].

237. *Id.*

238. *Id.*

239. *Id.*

240. *Id.*

process is known as authentication.[241] "[A] computer system . . . on the Internet is identified by an Internet Protocol ("IP") address which works [much like] a telephone . . . number."[242] The key difference is that this number is set dynamically each time a user connects to the Internet.[243] Because it is dynamically set, the physical destination and origin of transactions are difficult to verify or authenticate using conventional methods.[244] Thus, the door opens for any person to intercept or pose as someone else on the Internet. An intruder can use a technique called "spoofing"[245] to gain access to the system and pose as an authorized user, or can use a software program that generate passwords from the information gathered from an unauthorized access to a program.[246] Because of these possible interceptions, authentication controls are necessary to identify all parties to a communication.

Nonrepudiation is essential for validating data.[247] "Nonrepudiation involves creating proof of the origin or delivery of data to protect the sender against the recipient denying that the data has been received or to protect the recipient against false denial by the sender that the data has been sent."[248] Therefore, "to ensure that a transaction is enforceable, steps must be taken to prohibit parties from disputing the validity of, or refusing to acknowledge, legitimate communications or transactions."[249]

Risks associated with access control of systems must also be addressed by a financial institution. Access control refers to protecting the integrity of the network and its supporting systems from unauthorized access by using the most innovative software and hardware technology available.[250] "Risks include the destruction, altering, or theft of data or funds; compromised data confidentiality; denial of service (system failures); a damaged public image; and resulting legal implications."[251] Constant monitoring of the system is required because hackers, unscrupulous vendors, former or disgruntled employees, or even agents of espionage may try to invade the system.[252]

---

241. *See also Security Risks, supra* note 236; Randy V. Sabett, *Cryptography, Smart Cards, and Future Banking technology* (visited Jan. 1, 1999) <http://venable.com/litlab/eblcr5.html>.

242. *Security Risks, supra* note 236.

243. *Id.*

244. *Id.*

245. *Id.* "IP spoofing" is to have one computer set up to act as another computer. *Id.*

246. *Security Risks, supra* note 236.

247. *Id.*

248. *Id.*

249. *Id.*

250. *Id.*

251. *Security Risks, supra* note 236.

252. *Id.*

Once an intruder has gained access, they could change advertised rates on financial transactions or possibly even shut down an entire system. As we work to protect the integrity of the Internet and this new emerging banking system, there are intruders working to take advantage of whatever weaknesses there are in the network. There are software programs that run security scans on Internet servers, firewalls, and internal networks, which can help an intruder identify and attack a system by finding its weak link.[253] Because of the security risks described above, a financial institution should implement several security measures that are presently available.

One such security measure is encryption.[254] Encryption, or cryptography, is a method of converting information to an unintelligible piece of data and then, through decryption, changing it back to its original understandable form.[255] "The information is encrypted (encoded) and decrypted (decoded) by . . . 'cryptographic keys.'"[256] The encryption renders the information unreadable because it appears as a series of unorganized characters. Thus, the encryption technology provides assurance of data privacy, confidentiality, and integrity, with some methods providing protection against forgery and tampering.

There are symmetric and asymmetric cryptographic key systems. "With a symmetric key system (also known as secret key or private key system), all parties have the same key" to encrypt and decrypt messages.[257] The distribution of a key to each party in a transaction over a large network is impractical for widespread use. In an asymmetric key system (also known as a public key system), there are two keys, with one being secret (a "private key") and one being public (a "public key").[258] The private and public keys are mathematically related so that the corresponding public key can only decrypt the private key. Similarly, the corresponding private key that is specific to a party or computer system can only decrypt the public key. This system, therefore, authenticates the private key holder. More importantly, "it is nearly mathematically impossible for the holder of any public key to use it to figure out what" or who holds the private key.[259] The strength of the key is

253. *Id.*

254. *Id.* "Encryption techniques directly address the security issues surrounding data privacy, confidentiality, and data integrity. Encryption technology is also employed in digital signature processes, which address the issues of authentication and non-repudiation." *Id.*

255. *Security Risks*, *supra* note 236.

256. *Id.* "These 'keys' are actually values, used by a mathematical algorithm to transform the data. The effectiveness of encryption technology is determined by the strength of the algorithm, the length of the key, and the appropriateness of the encryption system selected." *Id.*

257. *Id.*

258. *Id.*

259. *Security Risks*, *supra* note 236.

determined by the length of the key. Therefore, a longer key makes it harder for high-speed computers to break the code.[260]

A digital signature is another type of cryptography that can be used as a security measure by a financial institution. Digital signatures authenticate the identity of the sender by using the private key.[261] The digital signature is derived from the content of the message itself, establishing a link such that the message cannot be repudiated.[262] "To generate a digital signature, the original, unencrypted message is run through a mathematical algorithm that generates what is known as a message digest."[263] "The message digest is then encrypted with a private key, and sent along with the message."[264] The recipient decrypts the message digest, and if the resulting message digest matches the one sent with the message, the message has not been altered.[265] Thus, data integrity has been verified. Because the message digest was encrypted with a private key, the sender can be identified and connected to the specific message and the digital signature cannot be reused.[266]

"Certificate Authorities" and digital certificates are other ways to address security concerns, particularly in the area of authentication. "A 'Certificate Authority' is a trusted third party that verifies the identity of a party to a transaction."[267] The identities of all parties must have been proven to the "Certificate Authority" beforehand. Digital certificates are messages that are signed with the "Certificate Authority's" private key.[268]

An individual bank's activities will dictate the level and type of security measures required. This may, for instance, include encryption, digital signatures, certificate authorities, and digital certificates.[269] With technology and implementation standards changing daily, the necessary legal infrastructure will continue to evolve and possibly lead to further regulation.

In November 1997, the Electronic Financial Services Efficiency Act of 1997 ("Act") was introduced, granting legal validity and equal treatment to qualifying forms of electronic authentication.[270] Any form of electronic

---

260. *Id.*

261. *Id.*

262. *Id.*

263. *Id.* A message digest is a unique character representation of the data. *Security Risks, supra* note 236. This process is known as the "hash." *Id.*

264. *Id.*

265. *Id.*

266. *Id.*

267. *Security Risks, supra* note 236.

268. *Id.*

269. *Id.*

270. *Id. 21st Century Banking Alert, No. 97-11-13* (visited Jan. 29, 1998) <http://www.fflisj.com/bancmail/21starch/ 971113.html> [hereinafter *21st Century Banking*]. House Report

authentication would be valid and legal according to this Act, if it "reliably establishes" both the identity of the maker, sender, or originator of a document, communication, or transaction and the fact that the document, communication, or transaction, has not been altered.[271] Therefore, any record would be valid and legal according to the Act with a qualified electronic authentication, unless state law prohibited it.[272] For the authentication to be valid, it must be:

> (i) unique to the person making, sending, or originating a document or communication;
>
> (ii) capable of verification;
>
> (iii) under the sole control of the person using it; and
>
> (iv) linked to data or a communication transmitted in such a manner that if such data or communication has been altered, the authentication becomes invalid.[273]

In particular, the Act authorizes that a digital signature, accompanied by a certificate issued by a third party, can be used in lieu of a paper based written signature in any communication that requires a signature within a federal agency, a United States court, or other instrument of the United States government.[274] The Act also established a National Association of Certification Authorities ("NACA") as the central association with which any person or group must register, in order to qualify as an authentication service provider.[275] Despite movement toward providing authentication standards, the Act does leave some issues unresolved, including the liability of the certification provider and the role of NACA. This emerging technology, while providing additional security for financial institutions, is still in its infancy, during which many new developments and regulations will surface.

2937, the Electronic Financial Services Efficiency Act of 1997, was introduced by Representatives Richard H. Baker (R-LA) and David Drier (R-CA). *Id.*

271. *Id.*

272. *Id.* A significant number of states have enacted or are considering enacting digital signature or other electronic authentication laws. *Id.*

273. *21st Century Banking*, *supra* note 270.

274. *Id.*

275. *Id.*

D. *Consumer Protection*

1. Regulation E and the Electronic Funds Transfer Act

Regulatory agencies are expected to provide the financial structure that protects the average consumer as well as the financial systems. However, in order for this to work, banks must comply with these regulations. Regardless of whether a bank uses a third party provider for Internet banking services, it must comply with applicable federal and state laws and regulations when it comes to consumer protection.[276] These regulations help provide consumer protection and confidence. Many consumer protection laws regarding wire transfers come from the Electronic Fund Transfers Act of 1978 ("EFTA").[277] The Federal Reserve Board promulgated Regulation E ("Regulation E") to implement the EFTA.[278] Regulation E covers all electronic funds transfers ("EFT").[279] Both the EFTA and Regulation E are consumer protection laws that amount to a "consumer bill of rights" in electronic banking.[280] The EFTA and Regulation E provide for consumer protection through disclosures, liability limits, documentation, and error resolution procedures.[281] The EFTA and Regulation E require that: 1) consumers are given an initial and periodic disclosure statements of the terms and conditions of the electronic funds transfer service; 2) there are safeguards with respect to pre-authorized debits and credits; 3) limitations are imposed on consumer liability for unauthorized use of credit and banking services; and 4) financial institutions investigate and resolve billing errors through error resolution procedures.[282]

On May 2, 1996, the Federal Reserve Board issued a proposed rule for the application of Regulation E to stored value systems.[283] Applying

---

276. Dan C. Aardal, *Consumer Protection Issues in Home Banking, Electronic Banking Developments: U.C.C. and Selected Regulatory Perspectives*, 1996 ABA SEC. BUS. L. at 25, 31 (1996).

277. 15 U.S.C. § 1693 (1994).

278. Electronic Fund Transfers, 12 C.F.R. § 205 (1998).

279. An electronic funds transfer ("EFT") is defined as "any transfer of funds that is initiated through electronic, terminal, telephone, or computer or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit an account." *See* 12 C.F.R. § 205.3(b); *see generally* Michael A. Fixler, *Cyberfinance: Regulating Banking on the Internet*, 47 CASE W. RES. L. REV. 81, 90 (1996).

280. Aardal, *supra* note 276, at 31.

281. *Fed Study Recommends Alternatives to Reg E for Stored-Value Cards*, 16 No. 8 BANKING POL'Y REP. 13, 15 (1997).

282. Barbara E. Matthews, *Reg E and Stored Value Cards: Fed is on Right Track*, 15 No. 14 BANKING POL'Y REP. 4 (1996). *See also* Aardal, *supra* note 276, at 1–2.

283. *Id.*

Regulation E to electronic money, especially through stored value systems, has the potential of interfering with the use of electronic money, but it also provides consumers with certain protections whenever a consumer's account is accessed electronically. The proposed rule focused on the type of stored value system rather than the entity issuing the card.[284] The Federal Reserve Board divided stored value systems into three types: "online accountable," "offline accountable," and "offline unaccountable."[285] Online accountable system is a system that only requests a transfer at the bank's central database.[286] These systems were deemed to be subject to Regulation E with modification for the particular nature of the system. Whereas offline accountable system is one in which the transactions took place offline but the bank had the ability to determine the impact of the transaction on the customer's balance.[287] The offline accountable systems have been regarded as being minimally regulated, with the focus turning to adequate disclosure to consumers. The third type identified was the offline unaccountable system which are those systems in which the transaction took place offline and there is no central database at the bank.[288] This type of system is deemed to be not regulated by Regulation E. The proposed rule outlining these types of stored value systems were the first steps toward providing consumer protection for electronic transactions. Such efforts will foster the application of existing or creation of new consumer protection laws for banking on the internet.[289]

2. Consumer versus Bank Liability

The question of consumer liability for unauthorized transfers was debated in Congress and resulted in a compromise between banks and

---

284. *Id.*

285. *Id.*

286. John L. Douglas, *Electronic Money*, 17th Annual Corporate Counsel Institute (unpublished) December 10, 1998. Online accountable systems were those systems where the bank retained an account in the name of the customer, which was debited only when the information related to the transaction was noted by the bank. *See generally* Richard L. Field, *1996: Survey of the Year's Developments in Electronic Cash Law and the Law Affecting Electronic Banking in the United State*, 46 AM. U. L. REV. 967, 976 (1997).

287. For an online accountable system, there is no authentication or authorization for the transaction but there is still a central database that records values and keeps those transactions apart from the card. *See generally* Field, *supra* note 286.

288. *Id.* The system allows for the stored value card involved to be used independently when there is no centralized bank that maintains all the transactional information. *Id.* In other words, the transactional information and reconciliation of the transactions occur on the card. *Id.*

289. 12 C.F.R. § 205.6(b) (1998).

consumer groups' positions.[290] An unauthorized transfer is a transfer initiated by someone other than the customer and without actual authority from the customer.[291] The banks supported a "negligence" standard in which a consumer has no liability unless the consumer's negligence contributed to the loss.[292] Consumer groups pushed for a flat fifty dollars liability limit similar to the limit imposed for credit card fraud.[293] Section 909 of the EFTA and Section 205.6 of Regulation E represent the compromise of these two groups by holding consumers liable for "unauthorized" electronic fund transfers, but that liability is sharply limited.[294] Aside from two exceptions, a consumer's liability for an unauthorized transfer is limited to the lesser of fifty dollars or the amount obtained in the unauthorized transfer.[295] However, a consumer is held liable for unauthorized transfers which resulted from the consumer's own negligence.[296]

Another area in which there are limits on consumer liability is in an unauthorized transfer from a breach of home banking security.[297] For example, a "hacker"[298] can break into a database containing access card numbers and personal identification numbers, which are maintained by the bank or a third party service provider, and use them to make transfers. Also a consumer may transmit a transaction from home to the bank and the transaction is intercepted by an unsuspected third party. In such situations, analysis of the EFTA and Regulation E would suggest that the bank will be held liable.[299] Such breach of security constitutes unauthorized electronic fund transfer in which the customer has limited liability. Therefore, with the prospect of being liable for breaches of system security, it is imperative that

---

290. *See generally* Aardal, *supra* note 276.

291. *Id.* § 12 C.F.R. 205.2(m) (1998). An unauthorized transfer is defined in Section 205.2(1) of Regulation E. *Id.* 12 C.F.R. § 205.2(l). If a transfer is performed by someone who is not authorized then the customer has limited liability. *Id.*

292. *Id.* § 205.6(a).

293. *Id.* § 205.6(b).

294. Aardal, *supra* note 276, at 32.

295. *Id.*

296. *Id.* at 33. Such negligence includes safeguarding a Personal Identification Number (PIN). *Id.* at 34. Therefore, a bank can highly recommend that a customer safeguard a PIN but can not hold that consumer liable if the consumer writes that PIN on the top of the access card. *Id.*

297. Aardal, *supra* note 276, at 35.

298. A hacker is somebody who knows the ins and outs of an operating system, a network, or computer language. A "bad" hacker defaces web sites with electronic graffiti, or steals user names, passwords or credit card numbers from an operating system or network. Adam L. Penenberg, *Forbes Digital Tool: Entertainment – Hacking the Corporate Ladder* (visited Feb. 17, 1999) <http://www.forbes.com/tool/html/97/oct/1010/feat.htm>.

299. Aardal, *supra* note 276, at 35.

banks focus on security issues at all levels. The bank has the burden of proving that the transaction was authorized.[300] The consumer then can point out that the bank should bear liability for breaches of security, since it was the bank who selected the computer program, the mode of telecommunications, the third party service providers who may be involved, and the components of the home banking system.[301] Thus, it becomes important that the bank have strong agreements with home banking service providers, processors, software vendors or developers to limit the bank's liability due to failures attributable to third parties.[302]

A consumer is also protected from a bank's failure to make an electronic fund transfer through section 910 of the EFTA. Section 910 of the EFTA protects the consumer by holding that the bank is liable for the failure to make an electronic fund transfer and for all damages proximately caused by such failure to make such a transfer.[303] Shifting liability to the bank is crucial in developing consumer confidence in using electronic payment systems and performing banking transactions over the Internet.

VI. CONCLUSION

Entering the new millenium, the Internet has become a remarkable convergence of break through technology for numerous information-based and monetary-based industries such as banking. A whole new arena of electronic commerce is emerging, which is reshaping and revolutionizing our banking practices. As the printing press, the automobile, the telephone, and the airplane brought the world together, so is the Internet transcending borders. But, with advancement comes difficult strategic choices in determining the path of a system as open as the Internet without hindering progress. It is within this medium that regulatory agencies must become leaders in setting precedent in dealing with the challenges of privacy, security, and jurisdictional issues. Banks have gained the confidence of the consumer in the past. The challenge now is to gain that some level of consumer confidence in banking on the Internet. Therefore, it is vital that regulations and standards dealing with security measures, such as encryption and digital signatures, continue to evolve. Banks are faced with many

300. Section 909(b) of the EFTA places the burden of proving such a transaction was authorized on the bank. *Id.* at 36.

301. *Id.*

302. *See* Wilson, *supra* note 1, at 33.

303. *Id.* A bank is liable to a consumer for all damages proximately caused by the bank's failure to make an electronic fund transfer in the correct amount or in a timely manner or due to insufficient funds that resulted from such failure to transfer such funds. *See* Aardal, *supra* note 276, at 36.

challenges, including the emergence of electronic money and criminals on the Internet. Also, the lines between a traditional financial institution such as a bank and nonfinancial institutions are becoming blurred, and banks are now competing for the consumer's business. All these changes reflect the impact of the Internet on our banking practices.

It is very necessary to establish a strategy and a roadmap for electronic banking. Banking, unlike the remainder of electronic commerce, is a highly regulated industry. It is important that nonbank entities fall under a formal regulatory structure. With this structure two key items can occur. First, a uniform set of enforceable regulations on banking worthiness can be established. This will enhance customer confidence. Second, a strategic plan can be developed on a global level by the G-10 and its member nations, that can use the decades of banking experience to steer the new inexperienced electronic banking industry away from potential pitfalls and banking failures. It is good to remember what happened on October 17, 1987 ("Black Monday"). Part of the failure in the stock market was caused by an uncontrolled "programmed sell-off."[304] If regulations are not established for all types of Internet banking, both banks and nonbanks will be open to the same type of mass electronic flooding of systems, or an electronic "run" on banks. A bank could be out of business in a matter of hours.

Together the private and public sectors can establish a new electronic banking and commerce environment that will enable new opportunities to promote growth of and expand our world economy by reaching new customers, lowering operating costs, and extending financial institutions and nonfinancial institutions to new levels of service, delivery, and innovation.

Jacqueline Marcucci

304. CNNfn - *The blackest of Mondays – Oct. 13, 1997* (visited Feb. 6, 1999) <http://cnnfn.com/markets/9710/13/crash_main/>.

http://www.personal-jurisdiction.com

TABLE OF CONTENTS

I. INTRODUCTION

One of the most monumental events of the last half-century has been the marriage of computing power and communication technology. The product of this union has evolved into what is commonly called the "information superhighway."[1] The newfound ability to access vast amounts of information,[2] coupled with the ability to communicate with man and

1. Al Gore, *Communications; Networking the Future; We Need a National 'Superhighway' for Computer Information*, WASH. POST, July 15, 1990, at B3. This term quickly became part of the vernacular to describe the revolution of online communication.

2. The indexing of the Internet via "hyperlinks" allows for "information to be accessed and organized in very flexible ways, and allow[s] people to locate and efficiently view related information even if the information is stored on numerous computers all around the world." ACLU v. Reno, 929 F. Supp. 824, 836 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997). *See also infra* Part III.A.

machine across global distances is revolutionizing the way we live. No industry, profession, or enterprise has remained untouched by this phenomenon.[3] As each segment of society is confronted by the challenges and opportunities brought on by the information revolution, it needs to adapt and reinvent itself to meet the demands and capabilities of this medium. The Internet in the legal arena is no different.[4]

When litigation concerns online contact, personal jurisdiction will be considered a threshold issue. The Internet is a community without walls or boundaries that encourages people to indiscriminately communicate and conduct business over state and national borders. If litigation ensues from such contact, the propriety of jurisdiction over an out-of-state defendant will invariably arise. Because the conventional methods of communication have been altered, it must be determined whether the traditional tests employed by the courts to determine personal jurisdiction issues still apply in this new era of online communication.

This article will examine how the courts have dealt with personal jurisdiction in the context of online communication. First, the modern framework of personal jurisdiction as set forth by numerous United States Supreme Court decisions is examined. Second, this article will briefly describe the Internet and analyze the unique nature of the Internet as a communicative device. Finally, this article will examine how the courts have dealt with this issue and formulate some of the factors used by the courts in making personal jurisdiction determinations.

One of the most important aspects of our legal system is its ability to adapt to new and emerging areas. The elasticity of the law is what provides it with enduring strength. Therefore, to best understand the future of online personal jurisdiction, one must consider the design of existing law and determine how the courts will adapt these principles to new and emerging areas.

II. PERSONAL JURISDICTION: A MODERN FRAMEWORK

The doctrine of personal jurisdiction limits the parties upon whom a court may impose a binding and enforceable judgment.[5] A court will always have jurisdiction over the plaintiff in an action because by filing the lawsuit in a particular forum, the plaintiff consents to the jurisdiction of that court.[6] On the

3. *See generally* Gore, *supra* note 1.

4. *See* John F. Delaney & Adam Lichstein, *The Law of the Internet: A Summary of U.S. Internet Caselaw and Legal Developments*, 505 PRAC. L. INST. PAT., COPYRIGHTS, TRADEMARKS, & LITERARY PROP. COURSE HANDBOOK SERIES 79 (Jan. 1998); LANCE ROSE, NETLAW (Osborne 1995).

5. McGee v. International Life Ins. Co., 355 U.S. 220, 222 (1957). *See* Kulko v. California, 436 U.S. 84, 91 (1978).

6. Naum v. Brown, 604 F. Supp. 1186, 1188 (E.D.N.Y. 1985).

other hand, defendants who need not consent to the jurisdiction of the court will be safeguarded by the principles of personal jurisdiction. These principles protect defendants from being unwillingly placed under the jurisdiction of a foreign court in a manner that is unjust and inequitable.[7] The current state of personal jurisdiction law is a blend of statutory law and constitutional limitations. For a court[8] to impose *in personam*[9] jurisdiction over a defendant, both the long arm statutes of the forum state and the due process requirements of the Fourteenth Amendment must be complied with.[10]

A. *Long Arm Statutes*

Each state has a long arm statute that dictates the instances in which nonresident defendants will be subject to the jurisdiction of its courts. Such

---

7. Hanson v. Denckla, 357 U.S. 235, 251 (1958) (citing International Shoe Co. v. Washington, 326 U.S. 310, 319 (1945)).

8. The *Federal Rules of Civil Procedure* indirectly apply a state's long arm statute to the federal courts. Under the Federal Rules:

> Service of a summons or filing a waiver of service is effective to establish jurisdiction over the person of a defendant
> (A) who could be subjected to the jurisdiction of a court of general jurisdiction in the state in which the district court is located, or
> (B) who is a party joined under Rule 14 or Rule 19 and is served at a place within a judicial district of the United States and not more than 100 miles from the place from which the summons issues, or
> (C) who is subject to the federal interpleader jurisdiction under 28 U.S.C. § 1335, or
> (D) when authorized by a statue of the United States.

FED. R. CIV. P. 4(k)(1).

Though jurisdiction is proper in a number of instances, it is most commonly found pursuant to the long arm statute of the state in which the district court is located. *Id.*

9. Personal jurisdiction over a defendant, who does not consent to the jurisdiction of the court, can be obtained in one of three ways. *In personam* jurisdiction is jurisdiction over a defendant "where the entire object of the action is to determine the personal rights and obligations of the defendants." Pennoyer v. Neff, 95 U.S. 714, 727 (1877). *In rem* jurisdiction is jurisdiction in a "proceeding . . . taken directly against property, and has for its object the disposition of the property." *Id.* at 734. *Quasi in rem* jurisdiction is jurisdiction "based on attachment or seizure of property present in the jurisdiction." Shaffer v. Heitner, 433 U.S. 186, 196 (1977).

10. Burger King Corp. v. Rudzewicz, 471 U.S. 462, 463–64 (1985). *See also* Savin v. Ranier, 898 F.2d 304, 306 (2d Cir. 1990) (stating "In diversity cases, federal courts must look to the forum state's long-arm [sic] statute to determine if personal jurisdiction may be obtained over a nonresident defendant. If jurisdiction is appropriate under the relevant statute, the court must then decide whether exercise of jurisdiction comports with due process.").

a statute cannot broaden the reach of the court beyond what is constitutionally permissible, but it can narrow the jurisdiction of a court and limit it to even less than what is constitutionally acceptable.[11] Long arm statutes will commonly fit into one of two categories. The first type of statute is one in which the state is looking to expand its jurisdiction to the limits allowed by its constitution.[12] Such a statute will provide a court with jurisdiction over any nonresident defendant so long as such jurisdiction is not inconsistent with the United States Constitution.[13] The second type of long arm statute is one that limits the power of the courts beyond what the Constitution protects, thereby giving nonresident defendants greater immunity from suit.[14] These limiting statutes may allow for jurisdiction over a nonresident defendant only in specific instances.[15] For example, many states allow jurisdiction only when the nonresident defendant has contracted with a party in the forum state or has committed a tort in the forum state.[16]

Because each state has its own individualized long arm statute, there is no uniformity. Nonetheless, regardless of a particular state's long arm statute, jurisdiction must, at a minimum, be consistent with the Due Process Clause of the United States Constitution. An assertion of jurisdiction that is valid under a state's long arm statute but in violation of the Due Process Clause will still be unconstitutional and nonbinding.[17]

---

11. Johnson Creative Arts, Inc. v. Wool Masters, Inc., 743 F.2d 947, 950 (1st Cir. 1994) (stating "The state statutes . . . cannot provide for service of process on a defendant outside the respective states unless the defendant has had the contact with that state that is required by the fourteenth amendment.").

12. *See, e.g.*, CAL. CIV. PROC. CODE § 410.10 (Deering 1989); R.I. GEN. LAWS § 9-5.33 (1997).

13. An example of such a statute is California's, which simply states that "[a] court of this state may exercise jurisdiction on any basis not inconsistent with the Constitution of this state or of the United States." § 410.10.

14. *See, e.g.*, N.Y. C.P.L.R. 302(a) (McKinney 1990).

15. *See id.*

16. *See, e.g.*, N.C. GEN. STAT. § 1-75.4 (1997) (invoking personal jurisdiction "[i]n any action claiming injury to person or property or for wrongful death within or without this State arising out of an act or omission within this State by the defendant.").

17. Lorelei Co. v. County of Guadalupe, 940 F.2d 717, 720 (1st Cir. 1991)

> [T]he federal court must determine whether the state's "long arm" or "doing business" statute authorizes it to exercise personal jurisdiction over the foreign defendant. If it does, the court must then determine whether the exercise of personal jurisdiction under the circumstances is consistent with due process under the fourteenth amendment.

Id.

B. *Due Process*

The Due Process Clause of the Fourteenth Amendment, in protecting the rights of a defendant, limits the ability of a court to impose jurisdiction over a nonresident defendant who is not served process in the forum state or who does not consent to the jurisdiction of the forum state.[18] It has long been established that this protection is not absolute in that *in personam* jurisdiction over a nonresident defendant will be proper so long as "the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'"[19] Over half a century ago, the United States Supreme Court introduced the *minimum contacts* test to determine when a relationship between the defendant and the forum state rises to a level at which jurisdiction over the defendant would be fair and just.[20] In questioning whether such *minimum contacts* exist, the courts will measure the "quality and nature" of the defendant's contact with the forum state in the context of the goals and ideals that the Due Process clause was designed to insure.[21]

In *International Shoe Co. v. Washington*,[22] the United States Supreme Court established the *minimum contacts* test, the backbone of any personal jurisdiction formulation.[23] In his groundbreaking opinion, Chief Justice Stone distinguished between three types of relationships that a party may have with a forum state, each with different personal jurisdiction ramifications.[24] First, a party may have a connection with the forum state so substantial in nature that jurisdiction in that state will be justified in actions arising from the party's activities within the forum or from matters "entirely distinct from those activities."[25] For a defendant to be subject to such jurisdiction, commonly known as "general jurisdiction,"[26] there must be contact with the forum that is "continuous and systematic" in nature.[27] A second type of jurisdiction will arise even when the defendant lacks the substantial contacts necessary to give rise to general jurisdiction, but the defendant nonetheless has some association with the forum state. When a limited relationship exists and "the maintenance of the suit does not offend

18. Pennoyer v. Neff, 95 U.S. 714, 733 (1877).

19. International Shoe Co. v. Washington, 326 U.S. 310, 316 (1945).

20. *Id.*

21. *Id.* at 319.

22. 326 U.S. 310 (1945).

23. *Id.* at 316.

24. *Id.*

25. *Id.* at 317.

26. "General jurisdiction" is the term used to explain "[w]hen a State exercises personal jurisdiction over a defendant in a suit not arising out of or related to the defendant's contact with the forum." Helicopteros Nacionales De Columbia S.A. v. Hall, 466 U.S. 408, 414 n.8 (1984).

27. *Id.* at 414–15.

'traditional notions of fair play and substantial justice,'" jurisdiction over a nonresident defendant will be proper if the contact gave rise to the liability sued upon.[28] Such jurisdiction is known as specific jurisdiction.[29] Unlike these two relationships, which give rise to a finding of *minimum contacts*, the Court recognized a third category in which a defendant has "no contacts, ties, or relations" with the forum state.[30] In such an instance, there are no *minimum contacts*, and personal jurisdiction is not constitutionally justified.[31]

International Shoe, which required the existence of *minimum contacts* to ensure "fair play and substantial justice,"[32] was subsequently manipulated by the Court. Thirty-five years later, in *World Wide Volkswagen Co. v. Woodson*,[33] the United States Supreme Court held that a New York automobile dealer was not subject to jurisdiction in Oklahoma when an automobile sold by the dealer in New York was driven to Oklahoma and was involved in an accident there.[34] A critical element of the Court's analysis was whether the defendant "should reasonably anticipate being haled into court" in the forum state.[35] The primary purpose of inquiring into the reasonableness and fairness of the forum is "to protect[ ] the defendant against the burdens of litigating in a distant or inconvenient forum."[36]

Only when foreign litigation is foreseeable to the defendant will personal jurisdiction be reasonable.[37] Foreseeability requires more than merely entering a product into the stream of commerce;[38] rather, it requires that the defendant "purposefully avails itself of the privilege of conducting activities within the forum State."[39] Such "purposeful availment" will give notice to the defendant of its susceptibility to suit in a foreign state, thus providing the minimum assurances required by the Constitution.[40]

---

28. *International Shoe*, 326 U.S. at 316 (quoting Milliken v. Meyer, 311 U.S. 457, 463 (1940)).

29. "Specific jurisdiction" is the term used to explain "when a State exercises personal jurisdiction over a defendant in a suit arising out of or related to the defendant's contacts with the forum." *Helicopteros*, 466 U.S. at 414 n.8 (1984).

30. *International Shoe*, 326 U.S. at 319.

31. *Id.*

32. *Id.* at 316 (quoting Milliken v. Meyer, 311 U.S. 457, 463 (1940)).

33. 444 U.S. 286 (1980).

34. *Id.* at 298–99.

35. *Id.* at 297.

36. *Id.* at 292.

37. Kulko v. California, 436 U.S. 84, 97–98 (1978).

38. *World Wide Volkswagen*, 444 U.S. at 297.

39. Hanson v. Denckla, 357 U.S. 235, 253 (1958).

40. *Id.*

The courts use an assortment of factors to determine whether it is reasonable to require a defendant to litigate in the forum state. These considerations include the comparative burden on the defendant and plaintiff in obtaining effective and convenient relief, the interest that the forum state has in adjudicating the dispute, and judicial efficiency.[41] The reasonableness of requiring a defendant to defend himself in a foreign court is an important factor that determines whether personal jurisdiction exists. If it is unreasonable to require a defendant to litigate an action in the forum state, the court will lack jurisdiction, even if the defendant purposefully directed his activities toward that state.[42]

Personal jurisdiction will usually be found when a "defendant purposefully avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws."[43] Once a party takes advantage of doing business or conducting other activities in the forum state, he automatically submits himself to the obligations of that state, and is subject to suit in that state.[44] The need to maintain a predictable legal system that provides a defendant clear notice that he may be summoned to court in a foreign state[45] is so important that the purposeful availment requirement has become a "'*sine qua non* for *in personam* jurisdiction.'"[46]

Purposeful availment is measured by the "quality and nature" of the contact made and is not a quantitative mechanical test.[47] A single act in the forum state can give rise to jurisdiction if the activity is such that it shows the party's intent to avail itself of the benefit of making contact with the state.[48] Once such contact is made, it is no longer deemed "random," "fortuitous," or "attenuated," and the defendant "should reasonably anticipate being haled into court there."[49]

The *minimum contacts* test was not designed as a rigid and indiscriminate factual examination. Every facet of the contact, and its effect on a finding of jurisdiction, must be analyzed to determine whether asserting jurisdiction is constitutionally justified. At the very least, a court

---

41. *World Wide Volkswagen*, 444 U.S. at 292. *See also* Burger King Corp. v. Rudzewicz, 471 U.S. 462, 476–77 (1985).

42. *Burger King*, 471 U.S. at 477–78.

43. *Hanson*, 357 U.S. at 253.

44. International Shoe Co. v. Washington, 326 U.S. 310, 319 (1945).

45. *World Wide Volkswagen*, 444 U.S. at 297.

46. CompuServe, Inc. v. Patterson, 89 F.3d 1257, 1263 (6th Cir. 1996) (quoting Southern Mach. Co. v. Mohasco Indus., 401 F.2d 374, 381–82 (6th Cir. 1968)) (emphasis in original).

47. *International Shoe*, 326 U.S. at 319.

48. McGee v. International Life Ins. Co., 355 U.S. 220 (1957) (finding that a California court had jurisdiction over a Texas insurance company based on a single policy sold in California).

49. Burger King Corp. v. Rudzewicz, 471 U.S. 462, 474–75 (1985).

can impose its authority over a nonresident defendant when *minimum contacts* are found such that requiring a party to defend a suit in the forum state is reasonable.[50] If the defendant's contacts with the forum state are inconsequential, then regardless of how reasonable such a suit may be, jurisdiction will be improper.[51] Likewise, even if substantial contacts exist, if it is unreasonable for the defendant to litigate the matter in the forum state, jurisdiction will not be imposed.[52]

The courts have not totally disregarded the extent to which technology factors into the personal jurisdiction equation. In 1957, Justice Black recognized a trend that was "expanding the permissible scope of state jurisdiction" over foreign defendants because of the increased nationalization of our economy and the ease of "modern transportation and communication."[53] In the past four decades the technological advances in computing, communication, and transportation have increasingly diluted the significance of our state borders and nationalized our economy. As Justice Black recognized, an expansion of personal jurisdiction has followed.[54] Nonetheless, the Court has repeatedly warned that it is a mistake to think "state lines are irrelevant,"[55] or that the nationalization of our economy "heralds the eventual demise of all restrictions on the personal jurisdiction of state courts."[56]

As the increased use of online communication suspends the reality of our geographic limitations, the personal jurisdiction barrier will only become a finer line. The technological advances that Justice Black envisioned have increased exponentially, and discerning what *minimum contacts* and reasonableness are in the realm of the online world is the next challenge before the courts.

---

50. *Id.* at 472–73.

51. *International Shoe*, 326 U.S. at 319.

52. Insurance Co. of N. Am. v. Marina Salina Cruz, 649 F.2d 1266, 1271 (9th Cir. 1981) (finding a sliding scale with regard to these elements, in that "[t]he smaller the element of purposeful interjection, the less is jurisdiction to be anticipated and the less reasonable is its exercise.").

53. *McGee*, 355 U.S. at 223. *See also* Hanson v. Denckla, 357 U.S. 235, 250–51 (1958).

54. *See McGee*, 355 U.S. at 223.

55. World Wide Volkwagen Co. v. Woodson, 444 U.S. 286, 293 (1980).

56. *Id.* at 294 (quoting Hanson v. Denckla, 357 U.S. 235, 251 (1958)). The Court in 1987 made it clear that constitutional personal jurisdiction requirements are still a valid concern. Asahi Metal Indus. Co. v. California, 480 U.S. 102, 114–16 (1987). In *Asahi*, the Court found that a California court did not have jurisdiction over a Japanese manufacturer of tire tube valve stems, because of the severe burden on the defendant to defend itself in a foreign legal system. *Id.*

III. THE INTERNET AS A WHOLE NEW PARADIGM

The Internet is the intangible grouping of many individual computers and small computer networks into a decentralized "network of networks."[57] Just as people can communicate over long distances, computers have the ability to communicate with each other in their own unique language. This long-distance communication is done by randomly relaying messages from computer to computer, through an infinite number of intermediaries, until the desired recipient is reached.[58] Unlike the schoolyard game of "telephone," computers communicate in a digital format that guarantees a rapid and flawless transmission.

The average person may not appreciate the intricate, technological marvels of online communication, but everyone can appreciate the uniqueness of this medium and recognize why it will have a strong impact on our lives. Among the distinguishing characteristics of the Internet are its vast cadre of ever increasing information, its use of multimedia, its global insensitivity, and its low-cost and high-speed access.[59] The Internet is not merely an improvement of existing technology or an enhancement of our communication capabilities—it is a whole new phenomenon.[60] To understand the impact that the Internet has had and will increasingly have on our society, one must acknowledge a paradigm shift from our established models of communication and realize the uniqueness of Internet communication. By seeing how atypical the Internet is, we can recognize its power and attraction.

A. *Information Glut*

The Internet is not a typical database that can store vast amounts of information. Unlike a database, which will always have some limit on capacity, the Internet is truly infinite. By networking many computer databases together, the Internet allows one to retrieve information from many varied data sources. Since its inception in 1969 as a joint project of government and academia, the number of computers linked to the Internet

57. ACLU v. Reno, 929 F. Supp. 824, 830 (E.D. Pa. 1996) (providing an in-depth explanation of the technology and usages of the Internet).

58. *Id.* at 831–32.

59. *See generally The Economics of the Internet: Too Cheap to Meter?*, ECONOMIST, Oct. 19, 1996.

60. The term "online communication" encompasses all electronic communication of which the Internet is merely one form. This author has chosen not to distinguish between the different forms of online communication and to use the terms interchangeably.

has grown exponentially.[61] In 1981, there were 300 computers linked to the Internet; in 1989, there were 90,000, and by 1996, there were nearly ten million host computers.[62]

Just as with any "real world" medium, the uses for the Internet run the gamut of our social culture. With the click of a button, one can "surf"[63] material as diverse as the latest political developments in Slovakia, the trajectory of Halley's Comet in 2061, or the best methods of contraception. It is the ease of access and varied nature of the material that make the Internet so alluring.

On the Internet, information is accessed via a novel method of indexing called hyperlinking. Hyperlinking allows an Internet user to click, with a mouse, on a word, picture, or image and to immediately be linked to a different document.[64] Unlike existing methods of indexing, hyperlinking does not limit the relationship of information to a predetermined linear format. One's imagination is his or her limitation, not the alphabet, chronology, or any other indexing system. For example, one viewing the Declaration of Independence on the Internet can click upon the words "John Hancock" and be immediately transferred to a biography of our founding father or an article about signatures. Another click on the name of the article's author will transfer the viewer to the *New York Times* bestseller list on which that author is found. This method of indexing allows for a fast paced flow of information and unlimited opportunity.

B. *Multimedia*

In the quest for access to information and communication, society has used many media, each one with its distinct benefits and drawbacks. Newspapers, magazines, and other printed materials are strictly one-dimensional media because they communicate solely through print, a single sensory and tangible medium. The written word has effectively allowed us to communicate for centuries, yet it has significant limitations. The high costs of printing and distribution are barriers to a continuous information feed. Radio, though still one-dimensional, breaks the cost and distribution barriers and allows for a continuous and contemporaneous flow of information. Television is a multidimensional medium that allows for a continuous information flow but is limited by expensive production costs.

---

61. *Reno*, 929 F. Supp. at 831.

62. *Id.*

63. "Surfing" is the act of jumping from one document to another via hyperlinks contained in each document. *See* American Libraries Ass'n v. Pataki, 969 F. Supp. 160, 166 (S.D.N.Y. 1997).

64. *See supra* text accompanying note 2.

The Internet takes the best qualities of each of our communicative media. It is essentially a low-cost print, audio, and visual information device. One can read and print the latest stock reports, listen to the closing bell, and watch the frenzied activity on the floor of the New York Stock Exchange, all without changing communication devices. Additionally, the communication can be tailored to one's particular interests. In the fifteenth century, movable type changed the way we communicate; in the 1900s, radio changed the way we communicate; in the 1950s, television changed the way we communicate; and in the twenty-first century, the Internet will change the way in which we communicate.

C. *Global Insensitivity*

The Internet is global in two senses: first, it has no governing body or partisan allegiance, and second, it is unrestricted by terrestrial borders or physical limitations. An uninformed person may ask: Where is the headquarters of the Internet? While this question may be valid in any other sphere, in regard to the Internet, it is unanswerable. The *New York Times* has its headquarters in midtown Manhattan and CNN in Atlanta, but the Internet is strictly intangible. "There is no centralized storage location, control point, or communications channel for the Internet, and it would not be technically feasible for a single entity to control all of the information conveyed on the Internet."[65] There is no central location, there is no governing body, and there are no limitations. Information can be posted on the Internet by any person, on any continent, in any language, and in any format; that information can be accessed in a like manner.

D. *Advertising*

In the past decade, the Internet has become an increasingly popular mode of communication. This increased popularity and exponential growth can be directly attributed to the commercialization of the Internet. Corporate America has recently discovered what academics have known for nearly thirty years—namely, that the Internet is an efficient and economic communicative device. Internet advertising is powerful because it is inexpensive, global, and asynchronous. A business advertising on the Internet can set up a website with information about its product or service at a fraction of the cost of television, radio, or print advertising. Additionally, the website, unlike other media, allows Internet users to access that "Internet ad" from anywhere in the world and at any time of the day.

---

65. *Reno*, 929 F. Supp. at 832.

The global nature of the Internet does have some drawbacks in regard to its inability to target certain individuals or geographic locations. That is, one cannot limit website access strictly to viewers in New York or Lebanon, nor can the website be limited to viewers over the age of eighteen or under the age of sixty-five.[66] A business wishing to advertise over traditional media can limit its geographic scope and target audience. For instance, advertising in a local newspaper will reach the local market but avoid the national market. Even a national print or television campaign will not reach an international audience. Likewise, a spot on a late-night talk show only reaches certain viewer demographics. On the other hand, the Internet will allow all users from any location to access your "Internet ad." While global exposure has its benefits, the legal consequences of such exposure must be realized.[67] For example, in the realm of personal jurisdiction, a small business owner in Florida who advertises on the Internet may not realize that he may be subject to personal jurisdiction and may need to litigate a lawsuit anywhere in the country because of that ad. It is in this context that many personal jurisdiction issues have arisen.

IV. INTERNET JURISDICTION

When it comes to determining Internet-related personal jurisdiction issues, a business owner about to foray into the cyberworld will ask whether his website might expose him to the jurisdiction of a foreign court. The answer to this question is yes, no, and maybe. Certainly, personal jurisdiction can be evoked based exclusively on online contact, such as a website, but personal jurisdiction cannot be imposed if the tests employed in the "real world" are not met. Unfortunately, there is no perfunctory test to determine whether personal jurisdiction exists; rather, such a determination is dependent on the nature of the website and the online contact.

The court's opinion in *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*[68] sets forth an elucidating framework for analyzing online personal jurisdiction issues.[69] Other courts have cited this framework with increased frequency.[70] A premise of this structured analysis is that not all online

66. *Id.* at 831. *See also American Libraries*, 969 F. Supp. at 171.

67. *See* Christopher W. Meyer, *World Wide Web Advertising: Personal Jurisdiction Around the Whole Wide World?*, 54 WASH. & LEE L. REV. 1269, 1297 (1997).

68. 952 F. Supp. 1119 (W.D. Pa. 1997).

69. *Id.* at 1124.

70. *See* Mieczkowski v. Masco Corp., 997 F. Supp. 782, 786 (E.D. Tex. 1998); Blumenthal v. Drudge, 992 F. Supp. 44, 55 (D.D.C. 1998); Blackburn v. Walker Oriental Rug Galleries, Inc., 999 F. Supp. 636, 638 (E.D. Pa. 1998); Resuscitation Techs., Inc. v. Continental Health Care Corp., No. IP 961457CM/S, 1997 WL 148567, at *5 (S.D. Ind. Mar. 24, 1997);

contact is of the same "nature and quality."[71] Online, there are active contacts with a foreign state, which will give rise to personal jurisdiction, and there are passive contacts, which will not give rise to personal jurisdiction. Active contact is online communication that fosters an ongoing business relationship, whereas passive contact is online communication that does "little more than make information available to those who are interested in it."[72]

There is no brightline test to distinguish between online contact that is active and passive. The courts look to all aspects of the contact to determine whether such contact should be considered active, giving rise to personal jurisdiction. In making such a determination, the level of "interactivity and [the] commercial nature" of the contact is of paramount importance.[73] As discussed *infra*, the greater the level of interactivity on a website, the greater the chance that the website will be considered active and give rise to personal jurisdiction.[74] Likewise, a website with little or no interaction between the user and the website will be considered passive and will not give rise to personal jurisdiction.[75] In summary, when a court is presented with an online personal jurisdiction issue, it must look to the specific facts of the case and determine whether the online contact is active or passive. Upon a finding of active contact, personal jurisdiction is proper. If the contact is deemed passive, no personal jurisdiction shall be found.

What conduct is considered active and what conduct is considered passive can best be understood by examining the factual polarity of *CompuServe, Inc. v. Patterson*[76] and *Bensusan Restaurant Co. v. King*.[77] *CompuServe*, a Sixth Circuit decision, depicts the quintessential active contact and typifies the instance in which personal jurisdiction is proper.[78] On the other hand, *Bensusan*, from the Second Circuit Court of Appeals, provides an example of what the courts consider to be a passive website that will not give rise to personal jurisdiction.[79] With these cases as reference

---

Weber v. Jolly Hotels, 977 F. Supp. 327, 333 (D.N.J. 1997); SF Hotel Co., v. Energy Invs., Inc., 985 F. Supp. 1032, 1034 (D. Kan. 1997).

71. *Zippo Mfg.*, 952 F. Supp. at 1124.

72. *Id.*

73. *Id.*

74. *Id.*

75. *See* Bensusan Restaurant Corp. v. King, 937 F. Supp. 295 (S.D.N.Y 1996), *aff'd*, 126 F.3d 25 (2d Cir. 1997); Weber v. Jolly Hotels, 977 F. Supp. 327 (D.N.J. 1997).

76. 89 F.3d 1257 (6th Cir. 1996).

77. 126 F.3d 25 (2d Cir. 1997).

78. *CompuServe*, 89 F.3d at 1257.

79. *Bensusan*, 126 F.3d at 25. To date only three United States circuit courts of appeals have decided this issue. The Sixth Circuit in *CompuServe*, 89 F.3d at 1257, the Second Circuit in

points, an examination of the spectrum between them will provide an understanding of the factors to which the courts look in determining online personal jurisdiction issues.

A. *Active Contact*: CompuServe, Inc. v. Patterson

The first opinion by a circuit court on the issue of online personal jurisdiction was *CompuServe,* in which it held that an Ohio court had jurisdiction over a Texas defendant based strictly on the defendant's online contacts with the State of Ohio.[80] The defendant, Mr. Patterson, was a subscriber and shareware[81] provider to CompuServe, Inc., an Ohio corporation.[82] As a shareware provider, Mr. Patterson had signed an online contract, known as the Shareware Registration Agreement, which provided that any litigation regarding the agreement would be construed and governed in accordance with Ohio law. The relationship between Patterson and CompuServe existed for three years, during which time Patterson uploaded thirty-two software programs to CompuServe's computers in Ohio.[83] Once uploaded, Patterson's shareware programs could be downloaded and purchased by any CompuServe subscriber. In effect, Patterson used CompuServe's computer network as "a distribution center to market his software" programs.[84] Patterson advertised these programs on the CompuServe network, payment for the programs were made to CompuServe, and the programs were available exclusively on the CompuServe network. For over three years, Patterson sold programs to only twelve residents in Ohio and received less than $650 in fees. In December of 1993, Patterson claimed that CompuServe had incorporated some of his trademarked terms into its own software product. Patterson contacted CompuServe via e-mail about its alleged trademark infringement and eventually demanded $100,000 to settle the claim. CompuServe filed a complaint seeking a declaratory judgment that it did not infringe upon Patterson's trademark. The district

---

Bensusan, 126 F.3d at 25, and the Ninth Circuit in *Cybersell, Inc. v. Cybersell, Inc.*, 130 F.3d 414 (9th Cir. 1997) and *Panavision Int'l, L.P. v Toeppen*, 141 F.3d 1316 (9th Cir. 1998).

80. *CompuServe*, 89 F.3d at 1268–69.

81. Shareware is software that an Internet user downloads for a trial period, paying the author a fee only if he or she decides to continue using the software. Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 n.6 (W.D. Pa. 1997).

82. *CompuServe*, 89 F.3d at 1260. CompuServe is the second largest provider of Internet computing and information services. *Id.*

83. *Id.* at 1260–61. Mr. Patterson's program was a software program that was designed to help people navigate the Internet. *Id.* at 1261.

84. *Cybersell*, 130 F.3d at 417.

court dismissed CompuServe's complaint for lack of personal jurisdiction over Patterson, but the Sixth Circuit reversed.[85]

Judge Brown, writing for the court, rejected Patterson's position that "contacts with Ohio, which have been almost entirely electronic in nature" are insufficient to support personal jurisdiction over a nonresident defendant.[86] The court recognized that online communication "represents perhaps the latest and greatest manifestation of these historical, globe-shrinking trends;" however, the court refused to allow the nature of the medium to alter the due process examination used in conventional personal jurisdiction analysis.[87] If anything, "there is less perceived need today for the federal constitution to protect defendants from 'inconvenient litigation' because all but the most remote forums are easily accessible for the pursuit of both business and litigation."[88] Physical presence, the court emphasized, is not necessary "'[s]o long as a commercial actor's efforts are "purposefully directed" toward residents of another State.'"[89] In finding that Patterson had "purposefully availed himself of the privilege of doing business in Ohio,"[90] the court characterized Patterson as a "third party provider of software who used CompuServe . . . to market his wares."[91] This depiction of Patterson's relationship with CompuServe was "crucial" to finding that minimum contacts existed.[92] Having a contract or even injecting a product into the "stream of commerce, without more, would be at best a dubious ground for [personal] jurisdiction."[93] Only by finding a deliberate, repeated, and ongoing commercial relationship was the court able to find that a substantial connection between Patterson and Ohio existed, despite a "'minimal course of dealing'" and a paucity of tangible and physical evidence of Patterson's relationship with Ohio.[94]

The *CompuServe* decision is based primarily on the fact "that Patterson purposefully availed himself of the privilege of doing business in Ohio."[95] The court emphasized Patterson's purposeful link with Ohio but made little

85. *CompuServe*, 89 F.3d at 1259–61.

86. *Id.* at 1262, 1268–69.

87. *Id.* at 1262–63. *See also* Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) (stating "Different results should not be reached simply because business is conducted over the Internet").

88. *CompuServe*, 89 F.3d at 1262 (citing World Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 293 (1980)).

89. *Id.* at 1264 (quoting Burger King Corp. v. Rudzewicz, 471 U.S. 462, 476 (1985)).

90. *Id.* at 1266.

91. *Id.* at 1264.

92. *Id.*

93. *CompuServe*, 89 F.3d at 1265.

94. *Id.* at 1264–65.

95. *Id.* at 1266.

inquiry into whether it was reasonable to require Patterson to defend himself in Ohio.[96] The *CompuServe* court chose to ignore the *Worldwide Volkswagen* reasonableness inquiry; however, it is important to recognize that other courts have found the issue of reasonableness to be determinative.[97] Additionally, the *CompuServe* court, in trying to limit the scope of its opinion, specifically stated that it did not decide whether a shareware provider would be subject to suit in the state of the shareware purchaser, or whether a subscriber to an online service can be sued by the service provider in its home state.[98] What is clear from the *CompuServe* decision is that an active commercial venture that has "knowing and repeated" online contacts with a foreign state will be subject to the jurisdiction of that state even if the sole basis for such jurisdiction is the online contacts.[99]

B. *Passive Contact*: Bensusan Restaurant Co. v. King

At the other end of the spectrum is the "passive" website, which merely makes information available for those who wish to access it.[100] Such were the facts in *Bensusan*, a case decided and upheld primarily on the basis of the New York long arm statute, but which is nonetheless instructive.[101]

In *Bensusan*, a New York-based chain of jazz clubs known as the "The Blue Note" brought an assortment of trademark related claims against a Missouri club also known as "The Blue Note."[102] The claims, filed in federal court in New York, asserted personal jurisdiction based upon the fact that the defendant had set up a website on the Internet's World Wide Web. The website, in addition to providing general club information and a schedule of events, also furnished the telephone number of the club box office for charging and reserving tickets by phone. While tickets could be ordered and purchased by phone, the actual tickets had to be picked up at the box office on the night of the show.[103]

The district court, in granting the defendant's motion to dismiss for lack of personal jurisdiction, held that the mere fact that the defendant's website

---

96. *Id.* at 1267–68. The extent of the court's inquiry is a conclusory statement that when purposeful availment exists, it can be inferred that the suit is reasonable. *Id.*

97. *CompuServe*, 89 F.3d at 1267–68. *Compare* Expert Pages v. Buckalew, No. C–97–2109–VRW, 1997 WL 488011, *1 (N.D. Cal. Aug. 6, 1997) *with* Smith v. Hobby Lobby Stores, Inc., 968 F. Supp. 1356 (W.D. Ark. 1997).

98. *CompuServe*, 89 F.3d. at 1268.

99. Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997).

100. *Id. See also* Weber v. Jolly Hotels, 977 F. Supp. 327, 333 (D.N.J. 1997).

101. Bensusan Restaurant Corp. v. King, 126 F.3d 25, 29 (2d Cir. 1997).

102. *Id.* at 26.

103. Bensusan Restaurant Co. v. King, 937 F. Supp. 295, 297 (S.D.N.Y. 1996).

could be accessed from the forum state does not give rise to jurisdiction, even if the consequences of such access are foreseeable.[104] The simple creation of a general access website, like entering a product into the stream of commerce, may have nationwide impact, but without additional contact "is not an act purposefully directed toward the forum state."[105] To find otherwise would subject the operator of a website to national if not worldwide jurisdiction, which "is not consistent with traditional personal jurisdiction case law nor acceptable . . . as a matter of policy."[106]

The beauty of *Bensusan* is its simple fact pattern. There were no other facts, aside from the defendant's website, upon which the court could base personal jurisdiction. The Blue Note club in Missouri had no other contacts with the State of New York.[107] Unlike the defendants in many other cases the Missouri club in *Bensusan*, received no revenue from New York, did not advertise in New York, and had no 800 number that was accessible in New York. Its sole contact with New York was the website upon which it advertised. This, the court held, did not give rise to personal jurisdiction in a New York court.[108]

C. *The Middle Spectrum*

Bensusan and *CompuServe* are important because they provide some measure of clarity in the otherwise murky realm of online personal jurisdiction law. These two cases may be viewed as reference points on a hypothetical personal jurisdiction spectrum. At one end of the spectrum is *CompuServe*, which holds that knowing and repeated electronic contacts with a foreign state will give rise to personal jurisdiction. At the other end is *Bensusan*, which holds that a strictly passive website will not give rise to personal jurisdiction over a nonresident defendant. These reference points will decide cases in which the fact pattern can be clearly characterized as an active or passive online contact.

Unfortunately, not all cases have *Bensusan*'s uncomplicated facts or *CompuServe*'s extensive contacts. Many online contacts will be somewhere in the middle of the personal jurisdiction spectrum. In this middle spectrum, the courts must determine whether online contact, coupled with other factors

---

104. *Id.* at 300. The *Bensusan* decision in both the district and appellate courts was determined on the basis of New York's long arm statute.

105. *Id.* at 301.

106. Hearst Corp. v. Goldberger, No. 96 Civ. 3620 (PKL) (AJP), 1997 WL 97097, at *1 (S.D.N.Y. Feb. 26, 1997).

107. *Bensusan*, 937 F. Supp. at 301.

108. *Id.*

such as toll-free numbers,[109] print or direct mail advertising,[110] or even the filing of a lawsuit[111] will be considered sufficient contact with the foreign state to give rise to personal jurisdiction.

The courts are still exploring the chasm between Bensusan and CompuServe. What follows is a look at the factors that some courts have found to be significant in deciding whether an online contact should be considered active or passive. A single factor will rarely be dispositive of the issue, but we can glean from court opinions what factors are important in finding that the required *minimum contacts* exist with the forum state.

1. Contracts

The United States Supreme Court held that the mere existence of a contract between the defendant and a resident of the forum state would not automatically give rise to personal jurisdiction.[112] Though a contract in itself may not give rise to personal jurisdiction, the existence of a contract is an indication of the expectations of the parties, which consequently may give rise to personal jurisdiction.[113] The factors surrounding the formation of and compliance with the contract will often be more important than the contract itself. "[P]rior negotiations and contemplated future consequences, along with the terms of the contract and the parties' actual course of dealing" are determinative, not the fact that a contract exists.[114]

An example of the role that a contract plays in finding jurisdiction in a non-online setting is *Burger King Corp. v. Rudzewicz*.[115] The defendant, a Michigan resident, was sued in a Florida court for breaching a franchise agreement with the Burger King Corporation. The Court found that the defendant was subject to the jurisdiction of a Florida court despite the fact that "the defendant did not *physically* enter the forum State."[116] The existence of a franchise contract was indicative of a "substantial and

---

109. Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161, 165 (D. Conn. 1996) (exercising jurisdiction based on an Internet website that included a toll-free 800 number).

110. Heroes, Inc. v. Heroes Found., 958 F. Supp. 1, 5 (D.D.C. 1996) (finding jurisdiction based upon the defendant's Internet website and the defendant's newspaper advertisement).

111. *Hearst*, 1997 WL 97097, at *12 (discussing whether litigation related e-mail will give rise to jurisdiction). *See also* CompuServe, Inc. v, Patterson, 89 F.3d 1257, 1266 (6th Cir. 1996) (considering the fact that the defendant sent e-mail messages about his claim as an indication that the defendant "originated and maintained" contact with the forum state).

112. Burger King Corp. v. Rudzewicz, 471 U.S. 462, 478 (1995).

113. Edias Software Int'l, L.L.C., v. Basis Int'l Ltd., 947 F. Supp. 413, 418 (D. Ariz. 1996).

114. *Burger King*, 471 U.S. at 479.

115. *Id.* at 462.

116. *Id.* at 476.

continuing relationship" between the parties.[117] By seeking out the inherent benefits of such a relationship, the defendant had reached out to the forum state in a manner that "can in no sense be viewed as 'random,' 'fortuitous,' or 'attenuated.'"[118]

In adapting the *Burger King* holding to online situations, the court in *CompuServe* found that sufficient contact with the forum state existed when the defendant had an online service and shareware provider contract with CompuServe located in Ohio.[119] Likewise, in *Thompson v. Handa-Lopez, Inc.*,[120] the court looked toward the existence of a contract as grounds for finding personal jurisdiction.[121] In that case, the defendant was a California company that operated an arcade website called "Funscape's Casino Royale," on which one could play such games as blackjack, poker, keno, slots, craps, easy lotto, and roulette.[122] To play the games, one would have to agree to an online contract and use a credit card to purchase tokens, known as "Funbucks." The contract included a provision stating that all disputes would be governed by the laws of California. If a player won a game, he or she would be paid with "Funbucks," which could be redeemed for cash or prizes. When the plaintiff, a Texas resident, attempted to claim $193,728.40 in winnings, the defendant refused to pay, and, after suit was filed, moved to dismiss for lack of personal jurisdiction.[123] The district court found that jurisdiction in Texas was proper because the defendant "entered into contracts with the residents of various states *knowing* that it would receive commercial gain."[124] The fact that the enrollment contract provided for California law to apply was inconsequential to the court in light of the interests that the State of Texas had in protecting its citizens.[125]

Though evidence of a contract, online or otherwise, will not be conclusive of the personal jurisdiction issue, it will be a significant factor in determining whether sufficient contacts exist to give rise to personal jurisdiction.[126]

---

117. *Id.* at 485–87.

118. *Id.* at 480 (citing Hanson v. Denckla, 357 U.S. 235, 253 (1958)).

119. CompuServe, Inc. v. Patterson, 89 F.3d 1257, 1264 (6th Cir. 1996) (comparing the contracts with CompuServe to the franchisee's contract with Burger King).

120. 998 F. Supp. 738 (W.D. Tex. 1998).

121. *Id.* at 744.

122. *Id.* at 741. As of February 5, 1999, the Defendant's website could be found at <http://www.funscape.com>.

123. *Id.*

124. *Id.* at 744.

125. *Thompson*, 998 F. Supp. at 745 (the court avoided finding jurisdiction based solely on the contract by identifying the contract as providing a "choice of law," rather then a "forum selection.").

126. Burger King Corp. v. Rudzewicz, 471 U.S. 462, 478–79 (1985).

2. Interactivity

A second factor considered by the courts is the defendant's commercial interaction with the forum state. In *Zippo Manufacturing*, the court stated that "the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site."[127] While the exact level of interactivity necessary is unclear, a website must be more than strictly passive.[128]

A case from the Eastern District of Texas provides a good example of how an interactive website can give rise to personal jurisdiction, even when the contact is unrelated to the cause of action.[129] In *Mieczkowski v. Masco Corp.*,[130] a products liability suit was filed in Texas against the defendant, Rose Furniture Company, a North Carolina entity. The plaintiff had purchased a bunk bed in North Carolina and a year later moved to Texas. Subsequently, the plaintiff's son was asphyxiated when he got caught between the bed railings. The defendant had no offices, employees, agents, or property in Texas, nor did the defendant advertise in Texas. The defendant had, during a six-year period, sold over five million dollars worth of merchandise to Texas residents, but this alone, the court determined, would not give rise to personal jurisdiction.[131] What gave rise to jurisdiction was the defendant's maintenance of an interactive website that was accessible by Texans.[132]

The court relied on the fact that the defendant's website[133] was quite extensive.[134] The website's "Shop Online" section provided the user with an extensive list of furniture selections from which individual pieces of furniture could be chosen. Once a specific piece of furniture was selected, the viewer would see a picture of the furniture, informational material regarding the construction of the furniture, and the price of the selected furniture. To order, one had the choice of either printing an order form or

---

127. Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) (citing Maritz, Inc., v. Cybergold, Inc., 947 F. Supp. 1328 (E.D. Mo. 1996)).

128. *Id.*

129. When a court finds personal jurisdiction over a defendant based on contact unrelated to the dispute it is commonly referred to as *general* jurisdiction. *See supra* text accompanying note 25.

130. 997 F. Supp. 782 (E.D. Tex. 1998).

131. *Id.* at 783–85.

132. *Id.* at 787–88.

133. As of February 5, 1999, the defendant's website could be found at <http://www.rosefurniture.com>. *Id.* at 786 n.4.

134. *Id.* at 787.

communicating with an online sales representative in the "Internet Sales Division." Additionally, one could check the status of a purchase online.[135]

In finding jurisdiction, the court stated that such a website was clearly "designed to solicit business in a manner that exceeds traditional notions of advertising."[136] When a party solicits rather then merely advertises, he may be subjecting himself to personal jurisdiction in that forum. This distinction was crucial in *Maritz v. Cybergold, Inc.*,[137] a trademark infringement case from the Eastern District of Missouri.[138] In that case, the defendant, a California company, operated an Internet website[139] that provided information about a forthcoming mailing list. Upon registering with the website, a user was provided with a personal mailbox to which advertisements, tailored to the specific interests of each user, would be forwarded.[140] From the time the website was set up to the time that the lawsuit was filed, the website was accessed by Missouri users 131 times.[141]

The court found Cybergold's relationship with the State of Missouri significant enough to supply the required *minimum contacts*.[142] The court rejected the characterization of the defendant's website as a "passive site"[143] and found that the defendant was soliciting names and addresses for the use of its mailing list.[144] The court found that by interacting with the website visitors, "Cybergold automatically and indiscriminately respond[ed] to each and every Internet user who accesses its website."[145] It was this automatic interaction between the website and the foreign state that caused the online communication to cross the line between passive and active contact, thereby giving rise to personal jurisdiction.[146]

---

135. *Mieczkowski*, 997 F. Supp. at 787.

136. *Id.*

137. 947 F. Supp. 1328 (E.D. Mo. 1996).

138. *Id.*

139. As of February 5, 1999, the Defendant's website could be found at <http://www.cybergold.com>. *Id.* at 1330.

140. *Id.*

141. *Id.* Though the site was actually accessed 311 times, the court discounted the 180 contacts made by the plaintiff. *Maritz*, 947 F. Supp. at 1330.

142. *Id.* at 1334.

143. *Id.* at 1333.

144. *Id.* at 1335.

145. *Id.* at 1333 (comparing an interactive website to the receiving of a inquiry letter and the mailing a response via traditional mail).

146. *Maritz* went one step beyond *Mieczkowski* and found an active contact even though the interactivity was not with a live representative. *See* Humphrey v. Granite Gate Resorts, Inc., 568 N.W.2d 715, 721 (Minn. Ct. App. 1997) (finding a website advertising a forthcoming online gambling service to be interactive).

3. Quantity of Contact

It has long been recognized that we must look to the "quality and nature" of the contact with the forum state rather than to a "mechanical or quantitative" measure of such contact.[147] A single contact with the forum state that is substantial in nature may supply the required *minimum contacts*, whereas repeated contacts which are only minimal in nature may not.[148] Nonetheless, the number of contacts that are made with the forum state will be indicative of whether the defendant purposefully availed itself of the privilege of conducting business in the forum state. This is especially true online, where the number of hits a website receives is the primary method of measuring the popularity and effectiveness of a website.

In looking at the quantity of contacts, the *Maritz* court found that a defendant's website which received 131 hits from Missouri residents was subject to jurisdiction in Missouri, in part because the number of hits suggested that the defendant purposefully availed itself of the privilege of doing business in Missouri.[149] Likewise, the 248 hits from Minnesota that were received by an Internet site advertising a future online gambling service were important in finding that the State of Minnesota had jurisdiction over the nonresident corporate defendant which operated the website.[150] In playing the numbers game, the Minnesota Court of Appeals found that if 131 hits were enough for Missouri to find purposeful availment, then 248 hits would *a fortiori* show such an intent.[151]

In using the quantity of contacts such as hits as a factor in determining whether jurisdiction is proper, there are a number of problems. First, as with any statistic, such numbers are malleable. Do you look at the number of hits received by a site individually, or do you look at the hits as a percentage of Internet users in that state? Alternately, do you look at the number of hits in relation to how popular other websites are, or do you look at what percentage of the hits at a specific website come from the forum state?[152] Second, the amount of hits a website receives is not indicative of the amount of people with whom the website communicates. Often, one will reach a website by mistake and just "surf" on, yet such a contact is still considered a

147. International Shoe Co. v. Washington, 326 U.S. 310, 319 (1945).

148. McGee v. International Life Ins. Co., 355 U.S. 220 (1957).

149. *Maritz*, 947 F. Supp. at 1333.

150. *Humphrey*, 568 N.W.2d at 718–19.

151. *Id.*

152. *See, e.g.*, *id.* at 718 (using the fact that computers in Minnesota were among the 500 computers that most often accessed the defendant's website, as a factor in finding jurisdiction over the defendant).

"hit."[153] Finally, parties to an action can easily inflate the number of hits a site receives by contacting the site themselves. Indeed, in *Maritz*, there was evidence that over half the recorded hits were caused by the plaintiff, and the court therefore discounted the inflated number of hits from 311 actual hits to 131.[154] Using the number of hits a website receives as a method of determining jurisdiction is a poor way to measure a defendant's contact with the forum state and has fortunately not been used by many courts.

4. Financial Success

Some courts, in making a determination of whether *minimum contacts* exist, have looked toward the success of the Internet site. In *Expert Pages v. Buckalew*,[155] the court denied jurisdiction over a defendant who had infringed the copyright of Expert Pages, a website which provides information regarding expert witness and litigation consulting.[156] The court found that the defendant's "business does not appear to have been terribly successful," for he never had more than twelve paying customers.[157] The court found that to require such an unsuccessful endeavor to defend itself in a foreign state would be an undue burden upon the defendant and would violate due process principles.[158] On the other hand, in *CompuServe,* the court rejected the argument that such a "*de minimis* amount of software sales" should not give rise to personal jurisdiction.[159] The court specifically stated that it is "not their number or status [of the contacts] that determines whether they amount to purposeful availment."[160]

While the financial success of a party, by itself, may not be an important factor, the financial success of the defendant may indirectly play a role in determining whether it is reasonable to require the defendant to litigate the matter in a foreign state. Obviously, a financially successful defendant will find the cost of foreign litigation less burdensome than a cash-strapped, upstart enterprise. In *Digital Equipment Corp. v. Altavista Technology, Inc.*,[161] a complicated trademark infringement case, the court dealt with this issue by stating that the costs involved in litigating a suit in a

153. Robert J. Samuelson, *Out of Print: Infatuation with the Information Superhighway, Part 10*, NEWSWEEK, Sept. 11, 1995, at 59.

154. *Maritz*, 947 F. Supp. at 1330; *see supra* text accompanying note 137.

155. No. C-97-2109-VRW, 1997 WL 488011, *1 (N.D. Cal. Aug. 6, 1997).

156. *Id.* at *5.

157. *Id.* at *4.

158. *Id.*

159. CompuServe, Inc. v. Patterson, 89 F.3d 1257, 1265 (6th Cir. 1996). The defendant had made only $650 worth of sales to 12 residents of the forum state. *Id.* at 1261.

160. *Id.* at 1265 (citations omitted).

161. 960 F. Supp. 456 (D. Mass 1997).

foreign state "may well be the price of its agreeing to do business involving the Internet."[162] While such a viewpoint may be realistic, it is especially harsh when the defendants are small companies or individuals who are not "experienced and sophisticated businessmen."[163]

5. Electronic Mail

One of the most common forms of online communication is the use of electronic mail, or e-mail, as it is commonly called. Where the defendant has been in contact with parties in the foreign state via e-mail, the courts have been willing to find personal jurisdiction over the defendant. The reason for this is twofold. First, e-mail does not exist in a vacuum. It is usually only one method of communication that supplements other telephone, written, or in-person contact. Even if e-mail alone does not provide sufficient contact with the forum state, the totality of the relationship with the forum state will. Second, e-mail, unlike a website, is targeted toward a specific person or group of people. When one sends an e-mail message to a specific person or group, it will be easier for a court to find purposeful activity directed toward the forum state than it would with an open-ended Internet website.[164]

Electronic mail, even if sent regarding pending or future litigation, may give rise to personal jurisdiction. In *CompuServe*, the court, in finding jurisdiction, took into account the e-mail messages that the defendant sent to CompuServe about his claim.[165] Likewise, in *Hearst Corp. v. Goldberger*,[166] the court closely examined the defendant's litigation-related e-mails before finding a lack of jurisdiction.[167]

6. Passive Plus

The instances in which websites gave rise to personal jurisdiction usually present other factors upon which courts can rely to support a finding of personal jurisdiction.[168] Such was the case in *Inset Systems, Inc., v.*

---

162. *Id.* at 471.

163. Burger King Corp. v. Rudzewicz, 471 U.S. 462, 484 (1985) (citation omitted).

164. Cody v. Ward, 954 F. Supp. 43, 47 (D. Conn. 1997) (finding jurisdiction based upon the defendant's telephone calls and e-mail messages to the plaintiff); *see also* Hall v. LaRonde, 66 Cal. Rptr. 2d 399, 400 (Cal. Ct. App. 1997) (finding jurisdiction based on e-mail contact).

165. *CompuServe*, 89 F.3d at 1266.

166. No. 96 Civ. 3620 (PKL) (AJP), 1997 WL 97097 at *1 (S.D.N.Y. Feb. 26, 1997).

167. *Id.* at *4, *5, *21.

168. Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414, 418 (9th Cir. 1997). In any case where jurisdiction is found "there has been 'something more' to indicate that the defendant

Instruction Set, Inc.,[169] which reached "the outer limits of the exercise of personal jurisdiction."[170] Inset and Instruction were two software developers located in Connecticut and Massachusetts, respectively. When a trademark infringement issue arose over Instruction's use of "inset.com," as a domain name, Inset filed suit in a Connecticut court. The court found personal jurisdiction based on the defendant's strictly passive Internet site and the toll-free number posted thereon.[171] In recognizing the uniqueness of the Internet, the court stated that "unlike television and radio advertising, the [Internet] advertisement is available continuously to any Internet user."[172] The fact that Internet advertising is a continuous medium which, at that time, had the ability to reach 10,000 Connecticut users, coupled with the defendant's toll-free number, was in the court's eyes indicative of the defendant's intent to solicit business and "purposefully avail[ ] itself of the privilege of doing business within Connecticut."[173]

Similarly, in *Heroes, Inc. v. Heroes Foundation*,[174] the court found that the Heroes Foundation, a New York charity that helps fight cystic fibrosis, was subject to the jurisdiction of a District of Columbia court based in part because of its Internet website.[175] Heroes Foundation was sued for trademark infringement by Heroes, Inc., a Washington, D.C.-based charity that assists families of firefighters and police officers killed in the line of duty.[176] The court found that the defendant purposefully availed itself of the privilege of doing business in the forum state by expressly soliciting donations and providing a toll-free number on its Internet website.[177] The text of the website was:

> How Can I Help?
>
> You can help by donating to the Heroes Foundation. For information on how to make a donation, call (800) 789-HERO(4376). No donation is too small, and every donation counts. With your help, we can find a cure to this deadly disease.[178]

---

purposefully (albeit electronically) directed his activity in a substantial way to the forum state." *Id.*

169. 937 F. Supp. 161 (D. Conn 1996).
170. Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1125 (W.D. Pa. 1997).
171. *Inset Sys.*, 937 F. Supp. at 165.
172. *Id.* at 165.
173. *Id.*
174. 958 F. Supp. 1 (D.D.C. 1996).
175. *Id.* at 5.
176. *Id.* at 2.
177. *Id.* at 5.
178. *Id.* at 4.

Such a website, the court found, would satisfy the *minimum contacts* test and give rise to personal jurisdiction.[179]

However, not all courts will find jurisdiction in such instances. In *Shapiro v. Santa Fe Gaming Corp.*,[180] an attorney claiming to be the "critical impetus" in discovering a short swing violation of section 16(b) of the Securities and Exchange Act of 1934 sued for his attorney's fees in an Illinois court.[181] The court found no jurisdiction over a Nevada corporate plaintiff even though the company maintained a website and a toll-free number.[182] The court held that having a website and toll-free number, even one that is solicitous in nature, is not a lethal combination that automatically submits a defendant to personal jurisdiction.[183] Likewise, in *Graphic Controls Corp. v. Utah Medical Products, Inc.*,[184] the court found that the defendant's Internet site and toll-free number "do not demonstrate [the defendant's] purposeful availment of the benefits and protections provided in each or any of such fora."[185] This matter is clearly still in conflict among the district courts.

The most recent circuit court opinion on this issue is *Cybersell, Inc. v. Cybersell, Inc.*,[186] a Ninth Circuit decision. In *Cybersell*, the court refrained from finding specific jurisdiction based solely upon the maintenance of an Internet website.[187] The court found that an essentially passive website "does not qualify as purposeful activity invoking the benefits and protections" of the forum state.[188] In this case, an Arizona Internet marketing service sued a Florida Internet consulting service for trademark infringement and related actions in an Arizona court. The defendant, Cybersell of Florida, maintained a website[189] on the Internet that contained the allegedly infringing materials. The website allowed the browser to enter his or her name, address, and an indication of whether he or she was interested in Cybersell's services. One could not sign up over the Internet, nor was there a toll-free number on the website. No one in Arizona, aside

179. *Heroes*, 958 F. Supp. at 5. What is especially intriguing is that the court seems to hold that such activity will even give rise to general jurisdiction. *Id.* at 4–5.

180. No. 97–C 6117, 1998 WL 102677, at *1 (N.D. Ill. Feb. 27, 1998).

181. *Id.*

182. *Id.* at *2.

183. *Id.*

184. No. 96–CV–0459E(F), 1997 WL 276232, at *1 (W.D.N.Y. May 21, 1997), *aff'd*, 149 F.3d 1382 (Fed. Cir. 1998).

185. *Id.* at *3.

186. 130 F.3d 414 (9th Cir. 1997).

187. *Id.* at 415.

188. *Id.* at 420.

189. *Id.* at 415. The defendant's website address could be found at <http://www.cybsell.com>. *Id.* As of February 20, 1999, this website is unavailable.

from the plaintiffs, ever accessed the website. The court found Cybersell's website to be essentially passive in that the defendant never encouraged people to access the site and therefore never "invok[ed] the benefits and protections of Arizona law."[190]

Cybersell remains true to the holding of *Bensusan* that a strictly passive website will not give rise to personal jurisdiction in a foreign state. *Cybersell* also goes a step beyond *Bensusan* in deeming the website strictly passive despite the fact that the browser's name and address could be entered on the website as an indication of interest in the services provided. This case should not be read to require online activity similar to the facts in *CompuServe* before personal jurisdiction can be established. What it does indicate is the court's distaste for finding personal jurisdiction based solely on an essentially passive website that includes a toll-free number.

V. CONCLUSION

In trying to fit new technology into existing law, the courts have extended the principles of *International Shoe* to the outer limits. The courts that do find purposeful availment based on minimal online contact fail to take the geographic insensitivity of the Internet into account.[191] The Internet does not yet allow for targeted postings, which would permit access to a website only in certain geographic areas, and one cannot purposefully avail oneself of something that is not optional. By finding personal jurisdiction based on such minimal contacts, the courts will in effect limit Internet advertising only to those enterprises that can afford to litigate matters in foreign and distant jurisdictions.

When Chief Justice Stone wrote his opinion in *International Shoe*, it is doubtful that he envisioned his principles being applied to a medium such as the Internet. What he did recognize was that any personal jurisdiction doctrine would need to be flexible and adaptable to changing circumstances. Even if the *minimum contacts* of the cyber era are found to be different than the *minimum contacts* of fifty years ago, the guiding principles and doctrines of *International Shoe* and its progeny will certainly endure.

In the next decade, the issues surrounding online personal jurisdiction must be watched from both a legal and technological perspective. As the issue of personal jurisdiction makes its way through the appellate courts, a more organized structure and formulation will be developed, which will allow for a clearer application of the law. Personal jurisdiction is a threshold issue that the United States Supreme Court has continuously addressed;

190. *Id.* at 419.

191. *See* Meyer *supra* note 66, at 1301–02.

hopefully, in the near future, it will feel compelled to address its application to the world of online communication.

Online personal jurisdiction must also be monitored from a technological vantagepoint. The Internet, despite its massive size, is still in its infancy. Anyone who has followed the computer and communication industry will recognize that what is new and novel today may be obsolete and antiquated tomorrow. In this era of rapidly changing technology, new devices and programs may be developed that will resolve many of the personal jurisdiction issues that we have today. Until such time, we must apply existing law to this new area and remain truthful to the time-honored principles of personal jurisdiction.

Motty Shulman