Mississippi College Law Review

Volume 20
Issue 1 *Vol. 20 Iss. 1*

Article 11

2000

Electronic Commerce: Confronting the Legal Challenge of Building E-Dentities in Cyberspace

Kris Gautier

Custom Citation
20 Miss. C. L. Rev. 117 (1999-2000)

ELECTRONIC COMMERCE: CONFRONTING THE LEGAL CHALLENGE OF BUILDING E-DENTITIES IN CYBERSPACE

*Kris Gautier**

I. INTRODUCTION

A. E-Commerce

E-commerce has taken the world by surprise. Just a few years ago, there was no such word. Today, e-commerce is throwing its weight around like a champion Sumo wrestler bent on being noticed. In its most basic form, e-commerce is the buying and selling of goods and services over the Internet. In its more complicated form, e-commerce tells a compelling story about individuals and businesses recreating themselves and extending their identities to the world of cyberspace.

E-commerce is quickly becoming a driving force behind the growth of the global e-conomy. It affects nearly every aspect of society. Its momentum can be seen in the simplest communication exchange as well as in the most complex delivery of infotainment. There is no turning back the tide of the e-revolution. One leading authority describes the change as being "so startling in its economic implications that it may reasonably be considered a watershed in the way we do business . . . an abrupt and irrevocable turning point, one that signals a shift in historical direction by obliterating an established set of business practices and replacing them with a new commercial paradigm."[1]

Since e-commerce has been growing in importance, it is important to weigh both the positive and negative effects of e-commerce. Those effects must be weighed upon the scales of justice, not only in the commercial realm, but also in the interests of the poor and needy. As the ability to access and manipulate information becomes the currency of the day, there will be an ever-growing need to keep the digital divide in check. Although the inevitable disparities between "netizens" and "netwits," the "haves" and the "have nots," will continue to widen, our principled nation is being called upon to develop and adopt a comprehensive legal framework for e-commerce. The absence of such laws, or regulations that are improperly applied, could potentially cause injustice to thrive while "liberty for all" withers and dies on the vine of tomorrow's emerging digital landscape.

B. Why E-Commerce Is Important

In spite of these challenges and binding obligations, one can no longer define e-commerce as a product of the United States of America. Although one could

---

* The Author is a Data Networking Specialist with BellSouth in Jackson, Mississippi. He formerly worked as a Network Manager with the Mississippi Department of Education, and has also worked in technology and telecommunications with NCR and MCI WorldCom.

1. Thomas M. Siebel and Pat House, CYBER RULES, STRATEGIES FOR EXCELLING AT E-BUSINESS, 1 (1999).

argue that the birth of the Internet was an American accomplishment, what has evolved since then is inextricably linked to all that transcends a single national identity. America's brand of e-commerce is different from Europe's. And Asia's brand is different from Africa's. Furthermore, the specific rules and regulations associated with each flavor of e-commerce are quickly becoming an item of international tension. In one corner are those who hold the view that e-commerce is global in nature and quilted together as a beautiful patchwork of unique interests and causes. In the other corner, protectionist regimes see the same patchwork as an Achilles' heel, ripe for imposing their own specific brand of economy on another's. The protectionists seek to isolate, insulate, and segregate. The more trusting globalists put their hope in a quasi-universal coexistence, claiming strength through diversity. With such extreme philosophical differences, it is no wonder that our legal system is finding it difficult to resolve many of the core issues associated with operating in cyberspace.

As e-commerce engulfs the globe, some will warn that technical advances are watering down rights and blurring national boundaries. And almost daily, new concerns surface over privacy, trademark violations, patent infringements, freedom of speech, separation of church and state, belief in equality, consumer protection, economic security, and electronic prejudices. In light of these issues, one can see how futile it would be to attempt to prescribe a one-size-fits-all remedy. What's right and honorable in one country might be considered unacceptable or illegal in another.

In spite of the fact that we have yet to uncover many hidden implications that can affect us individually as well as corporately, e-commerce continues to grow and expand exponentially. Some have likened the growth of e-commerce to the concept of dog years. And, if Moore's Law[2] applies to e-commerce, as some have suggested, we should expect to see a millennium's worth of change over the next twenty-five years. For example, industry research is forecasting Internet retailing to reach $40 billion by 2002,[3] while overall electronic commerce, including business-to-business activity, is estimated to reach $1.3 trillion by 2003.[4] This accounts for close to ten percent of the U.S. Gross Domestic Product (GDP).

The fastest growing group on the Net is also the most vulnerable. Jupiter Communications shows that children and teens are the two largest growth sectors of the Internet population.[5] By 2002, 21.9 million children and 16.6 million

2. Moore's Law is named after an engineer who, while working at Intel Corporation, postulated that the speed of processors would double every 18 months. This idea has been applied to the accelerated growth of the World Wide Web.

3. *Electronic Signatures in Global and National Commerce Act on H.R. 1714 Before the Subcomm. on the Courts and Intellectual Property of the House Comm. on the Judiciary*, 106th Cong. (1999) (testimony of Andrew J. Pincus, General Counsel, U.S. Department of Commerce).

4. *See* Kate Gerwig, *Coming Into Focus*, TELE.COM MAGAZINE, May 3, 1999, at 51-54; THE KIPLINGER WASHINGTON LETTER, Vol. 6, No. 31 (The Kiplinger Washington Editors, 1729 H St., NW, Washington, DC 20006-3938), August 6, 1999.

5. *See* Jupiter Communications (an online research company) <http://www.jup.com/jupiter/order/list-studies.jsp>.

teens will be on the Internet.[6] It is estimated that teens will account for $1.2 billion and kids $100 million of the e-commerce dollars spent in 2002.[7] E-businesses are spending their marketing dollars with this trend in mind.

And while the public is focused on consumer developments and consumer-driven companies such as eBay Inc. and Amazon.com Inc., the greatest impact of e-commerce is going unseen. Mom and Pop shops are now competing on a level playing field with "the big boys." The role of buyers and suppliers is changing. And traditional businesses are being infused with new life through added revenue streams, innovations in customer care, and more efficient means for service delivery.

As businesses are pushed and pulled by the unseen changes of e-commerce, employees are being affected. Employees no longer work within the confines of traditional neighborhood businesses within a city or a state. They are now netizens. Their actions can immediately generate ripples throughout the nation and the globe, from New York to Tokyo.

These changes happened suddenly and before anyone could make a calculated decision to participate or opt out. Businesses are finding themselves in the unique position of having to act or fold. There is no longer a realistic alternative. The tradewinds of change are blowing full force and businesses will either sink or swim depending upon how well they adapt to the ride. In many cases, businesses are beginning the process of change as a blind leap of faith, giving little thought to how they will protect their employees, profits, or stakeholders. And it is this aspect of e-commerce that is most troubling. It is affecting real communities with real dollars, euros, and yen whether they like it or not. Since businesses are already adrift, employees will quickly find themselves along for the same ride. And who knows what potential danger lurks within these volatile waters.

As an example of how easy it would be to disrupt the global economy and bring the whole world to its knees, one would only have to be reminded of an event that took place at Network Solutions, Inc.[8] Until recently, Network Solutions has administered the commercial root servers and General Top-Level Domain (GTLD) space for the National Science Foundation and the U.S. Government. On July 17, 1997, at 2:30 A.M. Eastern Daylight Time, a corrupt database with missing top-level domain information was loaded. The bad data spread as the database was copied by machines all over the world. Within four hours the mistake was corrected. It is estimated that the outage affected computer systems in the United States, Asia, Europe, Africa, and the Middle East during some part of the business day. In such a short amount of time, 6.5% of the world's hosts were directly affected by the incident during normal working hours.

---

6. *Id.*

7. *Id.*

8. *See* Martyn Williams, *Network Solutions Apologizes for Domain Name Database Error*, NEWSBYTES MAGAZINE (visited July 25, 1997) <http://www.newsbytes.com/news/9796769.html>.

II. HISTORY OF INTERNET DEVELOPMENT

One cannot discuss e-commerce without first noting the circumstances around its genesis. In the early seventies, the military laid the foundation for one of the most intriguing creations of modern history, the Internet. The Internet was started about twenty-five years ago by the United States Department of Defense. Much of its success can be attributed to Vinton Cerf, often referred to as "the Father of the Internet."[9] Cerf co-authored the language that is today spoken by all connected devices on the Internet, TCP/IP. One might consider IP to be the underlying "global glue" of the Internet.

Back in the days of the Cold War, the original architects of the Internet needed a network that would keep intelligence flowing in the unlikely event of a nuclear attack. Because of this concern, the Internet was intentionally designed with a distributed hierarchy of control. Once top-level domain information was fed from root servers to secondary levels, each portion of the network could function with a certain degree of autonomy. The idea was ingenious. It led to a super-resilient network and eliminated the possibility of a strike on one point of the network that could potentially cripple the whole. As American military interests moved around the globe, the ability to communicate over the Internet followed. Once the power behind this infrastructure was realized, the U.S. government extended its acceptance and use throughout major educational and research communities, including major universities and institutes of higher learning.

During this time, the telecommunications industry went through massive change. AT&T was broken up into several Regional Bell Operating Companies (RBOCs) and the Federal Communications Commission (FCC) created virtual borders all over the United States. These borders, called LATA boundaries, served to delineate between where the RBOCs could and could not sell their services. Traffic crossing LATA boundaries was considered "long-distance." The second cause for change in the telecommunications industry was the demand for data networking. Traditional voice networks were being converted to handle the ever-growing demand for data networking. Newer technologies, such as Frame Relay and Asynchronous Transfer Mode (ATM), were being designed in the labs as the Bellheads and the Netheads began jockeying for position over standards bodies.[10]

In the mid-eighties, as its veil of secrecy was removed, the Internet received a face-lift. Popular graphical user interfaces (GUIs) were introduced to the masses as Microsoft changed its command-line operating system to reflect a more user-friendly "window" on the world. Moving to the GUI made computer use easier for those who were not as technically inclined as others. Microsoft grew

---

9. Founding President of the Internet Society (ISOC) from 1992 to 1995 and co-creator of the Transmission Control Protocol/Internet Protocol (TCP/IP), which enables computers to talk to each other over the Internet. Cerf is currently serving as a Senior Internet Architect at MCI WorldCom and sits on the President's committee to drive the Next Generation Internet Project. It is after him that the phrase "Cerfin' the Net" was coined.

10. Dawn Bushaus, *Bellheads vs. 'Netheads'*, TELE.COM MAGAZINE (visited May 1998) <http://www.teledotcom/0598/features/tdc0598cover1_side1.html>.

stronger and the PC became the standard desktop. Another contributer to the Internet's make over was a young pioneer named Tim Berners-Lee. Working at CERN[11] in 1990, Lee conceptualized the Hyper Text Markup Language (HTML) making it easy for people to publish information and establish links from one computer to another on the Internet. In the early 1990s, Marc Andreesen invented Mosaic at the University of Illinois.[12] Mosaic eventually became the Netscape browser. Soon, children began showing their teachers how to "cerf the net." The proliferation of GUIs and browsers began transforming the Internet into the World Wide Web (WWW).

As data networking increased, government began addressing some of the old rules that seemed outdated and restrictive within the telecommunications industry. The web, much like the telephone, was instrumental in fostering relationships that transcend national boundaries. Virtual communities began springing up around the world.

One cause that received an inordinate amount of government attention was education. Al Gore was instrumental in drafting the Telecommunications Act of 1996.[13] The Telecommunications Act fulfilled two primary objectives, promoting competition and advancing universal service. An initial $2.25 billion tax on business phone bills was designed to subsidize Internet access for all U.S. schools and libraries.[14]

Speaking during a statement at the White House, Al Gore called the FCC's E-Rate decision a "cornerstone" and "historic," saying, "The FCC voted today to give our young people the tools they need to meet the challenges of tomorrow. Today's decision will help to ensure that all of our children—whether rich or poor . . . have the same access to the vast resources on the Internet."[15] Continuing his statement on behalf of the President, he said, "We are closer to a day when children . . . walk into a classroom filled with computers linked to the Internet, and not even give it a second thought."[16] He praised the FCC's efforts and ended his comments by challenging the American public to connect all classrooms and libraries to the Internet by the year 2000.[17]

Long-distance carriers began looking at ways to get around the artificial LATA boundaries created by the FCC. They began building their own "last mile" access points in major metropolitan areas. Soon it was possible to originate a call from Los Angeles to Frankfurt all on the same carrier's network. Traditional regulatory boundaries—though black and white—on paper began to fade as the facts on the ground authenticated the "death of distance." More and more people

---

11. CERN stands for the European Laboratory for Particle Physics Research in Geneva, Switzerland.

12. Elliott Rusty Harold, XML: EXTENSIBLE MARKUP LANGUAGE 9, (1998).

13. 47 U.S.C. § 251 *et seq.* (1996).

14. *See Readin', Writin', and the Internet,* BUSINESS WEEK, June 9, 1997, at 18. In 1999, E-rate was funded at $2.25 billion.

15. Vice President Al Gore, Statement on the FCC E-Rate Decision (May 27, 1999) (transcript available at <http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1999/5/28/1.text.1 >).

16. *Id.*

17. *Id.*

began getting their news from the Internet. About one in five Americans, mostly younger, affluent, and educated, began using the Internet at least once a week for this purpose.[18] The Internet continued to radically alter the way people interacted with computers, each other, institutions, and businesses.

Soon the Internet was used as a virtual boxing ring on the scene of U.S. politics. It became the medium of choice for Ken Starr's Independent Counsel to reveal to the world the details concerning the results of an investigation into the private life of the President. On the same day boxes of reports were officially released to Congress, over twenty million Americans used the Internet to access an e-copy of The Starr Report online. This was the highest number of people ever to use the web to access a single document, a truly historic event.[19]

As the Internet invaded business, new efficiencies were quickly realized. Retailers became e-tailers. Traditional brick and mortar businesses were transformed into click and mortar shops. People began receiving customized treatment. The costs for service delivery and customer care were reduced. One multinational corporation, IBM, realized millions of dollars in immediate savings when it abandoned its traditional method for disseminating information on paper and began publishing soft copies to the web.

E-commerce was soon in full bloom. But along with the immediate benefits came a few "gotchas." Businesses soon found that hackers were making target practice out of their private information. It became glaringly apparent that individuals and corporations were not adequately protected on the web. Vulnerabilities in the web's legal armor started surfacing, taking its toll on big business' bottom line. Security became vitally important. Meager attempts were made to tame the uncontrollable side of the web through technical means, but the establishment of firewalls, the creation of Intranets, and the implementation of secure Extranets were found to be quite complex and potentially constraining on some of the web's best features. Government restrictions on the export of encryption techniques made it difficult to protect intellectual property. Not only were businesses challenged by internal and external threats, consumers were also targeted. Marketing interests made it profitable to collect personal information about customer's buying habits and web clicks. Personal profiles were being built and sold to the highest bidder. Children were being targeted with an irreverent intent to addict and exploit.[20] Hate groups, terrorists, and advocates of illegal activities found the web to be a safe haven. In the meantime, changes in law simply could not keep up. In spite of these risks, businesses bought off on the benefits of e-commerce and the world were completely immersed, if not completely dependent upon the web.

---

18. *Internet News Readership Growing At 'Astonishing' Rate* (visited June 8, 1999) <http://www.cnn.com>.

19. *20 Million Americans See Starr's Report On Internet* (visited September 13, 1998) <http://www.cnn.com>.

20. Blocking software generally filters web site content oriented toward sex, cults, drugs, violence, gambling, alcohol, and tobacco, areas proven to reinforce addictive behaviors.

One might argue that it is up to government to protect consumers and netizens from the wayward ways of the Internet. A desirable solution would allow regulation, taxation, and governing without infringing upon the principles that have made this country such a great economic powerhouse. The solution should foster economic prosperity, promote universal access, commercial exchange, and iron-clad security. But the rights of netizens should be a top priority.

Others argue that regulation of the industry should be left to private industry. No one can deny the direct correlation between the growth of the Internet and physical telecommunications infrastructures. The pipes that connect the world to its causes are owned and operated mostly by private businesses. And as these businesses become committed to mobility, their employees are working more from home and on the road. The trend to accommodate mobility is pushing the reach of the Internet from stationary wireline local area networks (LANs) to wireless devices such as laptops, Palm Pilots, and pagers. Now, one can access the Internet from anywhere in the world.

There is no doubt that the web will continue as a revolutionary catalyst for change in human history. But the lack of a ubiquitous legal framework strong enough to protect sovereign nations, while stimulating the global economy, has yet to materialize. And there is no single group that can police the Internet on behalf of all others. As our mobile society begins to float beyond local and national legal boundaries, so too will the elusive responsibility of protecting consumers and netizens.

III. OUR FLOATING E-DENTITY

This "float" is not only the result of the transformation taking place in the way employees conduct business. The web is moving society toward another dangerous trend. It is mandating that a user's identity be stored "out there." This trend is so dangerous because where "there" is, is not supposed to be important.

With the evolution of local area networking, low-cost network fileservers have encouraged the shift away from the computing model where one's records are stored on a local hard drive to the storing of one's records on a fileserver. Servers, acting as repositories for large amounts of data, operate from any location on the network. The physical location of the fileserver is typically not an issue. This same concept applies to the web. It is now possible to store one's personal records on any web server in the world. As long as one knows the name of the web server, or its number, one can access the information. There is a quality of convenience associated with this model. And the convenience of storing records in this manner overrides most people's concerns about privacy.

In an interview with PC WEEK, Javasoft president Alan Baratz explained the concept of the emerging webtop and its implications. He alludes to "the notion that your existence, rather than being stored on your local machine, is stored in a server on the Net so you can get to yourself from wherever you might happen to be."[21] Since cyberspace exists outside certain geographic and legal boundaries, it

21. *Building on the Java Platform*, PC WEEK, Apr. 14, 1997, at *38.

tends to pull the rug out from under one's locally connected cultural identity and belief systems, exacerbating the problem of identity "float."

If identity begins to float "out there" from one anonymous computer to millions of others, the world will potentially have the same access to "me" as I do. Some of the information about me will be true. And other information could be fabricated. But no matter how accurate this information might be, virtually every person on the planet is moving toward having this ubiquitous alter-image on the web. In cases of impersonation, one may unknowingly possess multiple virtual personae.

This web "existence" consists of personal information that is collected, analyzed, archived, and retrieved by others. This virtual persona often takes on a life of its own. Buying habits, medical records, and financial information form an electronic dossier that constantly builds. Much of an individual's virtual identity is established based on web use. This information is used by marketers to more efficiently target their products. One problem with this approach is that there is no way to determine when online impersonators might be acting in bad faith without authentic user permission. This is a major reason that floating virtual personae must be legally protected. Legal protection is an important ingredient in building bridges of confidence between consumers and cybershops. Legal protection must be extended to our virtual personae much like a letter of agency is extended to a telecom company on behalf of its customers. And, like a lawyer who represents the best interests of his or her own client, one's rights in cyberspace should be based on equality and a verified accountability between a person's words and actions, just like in the offline world.

Some have proposed that each person should be granted a unique stake in cyberspace as a human right. They propose a one-to-one correlation between one's name and one's rights. This idea has some merit since everyone is affected—not just big business.

IV. PROBLEMS WITH FLOATING E-DENTITY

Security and identity are at a crossroads on the Internet. And whether anyone realizes it or not, all are vulnerable to the threats that come along with identity float. One of the main reasons for this problem is the lack of widespread digital authentication practices. Within this vacuum, acts of online impersonation and the fabrication of misinformation are almost encouraged. Some consider it a hobby finding security holes in systems in order to teach people where their systems are weak. And even businesses are willing to fudge on what is right if they can generate a profit without getting caught.

Web content providers have been storing web clicks and other information about personal browsing habits ever since the invention of "cookies." When one visits a web site and selects something of interest, advertising firms and others create online profiles by assigning each consumer who visits their site a unique identification tag. The tag is placed on the consumer's own computer in a text file known as a cookie file. A different cookie "crumb" is generated and tracked each time the web site is "hit" in the future. Advertisers who sponsor providers

of web content can then more accurately determine buying preferences and individual consumer tastes. Cookie trail analysis, or profiling, is great for advertisers and people who need to more accurately market their products, but it pushes the limits of privacy.[22]

When these practices started coming to light, the government jumped into the mix to study the issue a little closer. But the web felt threatened by government intervention and, for the time being, slowed its free-for-all spin into the personal lives of humanity. Spurred on by the desire to avoid further government intervention, "Lexis-Nexis and seven other companies that sell detailed information about Americans agreed . . . to voluntary limits to minimize privacy intrusion."[23] Speaking to the Federal Trade Commission (FTC), Marc Rotenberg, director of the Electronic Privacy Information Center, a Washington-based cyber civil rights group, stated that "the law has not kept up with these developments."[24] Information about buying preferences, household income, and other types of data allow the creation of electronic dossiers on ordinary private citizens. The problem is that individuals may not be able to learn what is in their records so that they can correct false or inaccurate information. Robert Pitofsky, chairman of the FTC, questioned what one would do in the event that "something as innocuous as your last known address [was] . . . misprinted as a prison."[25]

If not watched closely, the improper use of one's e-dentity could lead to electronic isolation, being set apart and treated differently than Netizens who play by the rules in cyberspace. Electronic isolation could jeopardize the future of entire businesses. It has the power to keep the downtrodden moping along dusty trails of poverty and the power to broaden the gap between netizens and the netwits of the world. As people begin extending themselves to the web, they will be treated with dignity and protection only as current law provides functionally equivalent coverage in the online world. For this reason, many businesses and consumers are still wary of conducting extensive business over the Internet. As a predictable legal environment is developed to govern transactions, consumer confidence will increase.

To illustrate the need for greater identity protections and the potential for illegal impersonations to exist on the web, consider this: In August of 1998, the receptionist at MCI WorldCom called me at my desk and informed me that I had some visitors. After telling her I'd be right down, I quickly glanced at my DayTimer. I was puzzled to see that I had no appointments scheduled. As the elevator opened, I scanned the lobby for a familiar face. Two men stood next to the receptionist's desk glaring at me with much suspicion. As I walked up to them, they asked me to verify my name. I nodded and confirmed my name for them. At that point, they retrieved their badges, flashed them in unison, and said,

---

22. *Personal Habits Gathered For Use On The Internet*, CNN INTERACTIVE (visited August 16, 1998) <http://www.cnn.com/TECH/computing/9808/16/website.privacy/>; *see also* Statements by Mark Rotenberg, director of the Electronic Information Center before the Federal Trade Commission on April 15, 1997. The statements can be accessed at <http://www.epic.org/privacy/internet/ftc/epic_comments_497.html>.

23. *Companies Agree to Address Cyber-Privacy Concerns* (visited June 10, 1997) <http://www.cnn.com/TECH/9706/10/info.privacy.ap/index.html>.

24. *Id.*

25. *Id.*

"We are with the Secret Service and we'd like to have a word with you!" At first I thought it was a practical joke. Surely I was having one of those Candid Camera experiences. I asked them if they were kidding, but my comments were met with somber stares and the assurance that "we are very serious, sir."

The confrontation boiled down to a threatening e-mail that had been sent to the White House in my name. I wouldn't have believed it had I not seen it for myself. One of the secret agents retrieved a copy from his coat pocket and showed me the evidence in black and white. I was devastated. I felt angry. I felt endangered. I had been violated by a malicious online impersonator. This personal experience reveals the real vulnerabilities each of us faces because of the web. It highlights how technology has outpaced the ability to prevent its misuse through legal means. Unfortunately, incidents like this will likely become more and more commonplace as technology evolves.

Another privacy glitch that raised eyebrows all over the world was discovered by a Danish software firm.[26] The bug affected Netscape browsers, making it possible for web site operators to read anything stored on the hard drive of a PC logged on to a web site. The bug was unique in that it was found in the browser instead of embedded in a file that had been downloaded. Although the bug was quickly fixed, confidential letters, business spreadsheets, and virtually everything on one's PC could potentially be pilfered.

In another incident, over 2300 customers of two popular web sites were sent anonymous e-mail stating that their credit card numbers had been plucked off the Internet. To show that the matter was serious, the anonymous sender included the last eight digits of the recipient's credit card number in the message. The message went on to state, "[Y]ou are the victim of a careless abuse of privacy and security."[27]

FCC chairman William Kennard most recently highlighted the government's inability to protect its citizens' privacy rights when he lashed out about a recent court order with which he disagreed.[28] The 10th Circuit Court of Appeals held that phone companies do not need customer consent to use personal information; they may now use personal data unless the customer tells them not to do so.[29] Kennard, referring to the court's decision, called it "a sad day."[30] With the burden now on the consumer to opt out, it will be much easier to collect and share information about web activity with the highest bidder. The First Amendment rights of businesses seem to be outweighing the privacy rights of their customers.

---

26. *Netscape Bug Uncovered* (visited February 14, 2000) <http://cnnfn.com/1997/06/12/technology/netscape_pkg/>.

27. *Starwave Wipes Out on Internet Commerce: Security Lapse Allows Web Access To Credit Card Numbers* (visited February 14, 2000) <http://www.isdnwatch.internex.com/mag/star.htm>.

28. *See* U.S. West v. Federal Communications Comm'n, 182 F.3d 1224, 1235 (10th Cir. 1999) (the majority stated that "[a]lthough we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may pass freely").

29. *Id.*

30. *FCC To Appeal Court Ruling Vacating Privacy Regulations*, ASSOCIATED PRESS, *see* <http://cnn.com> (last accessed Aug. 25, 1999).

And the courts seem to be more interested in protecting the Internet and its infrastructure than the individual.

Phone companies and digital merchants are not the only ones finding new opportunities at the expense of individual privacy rights. Internet Service Providers (ISPs) are now gaining the power to handle web transactions on behalf of their subscribers. As subscribers purchase goods and services off the Internet, ISPs will be able to bill digital purchases automatically to their subscribers' accounts. Although this trend allows buyers to purchase digital goods without cumbersome user registration, software downloading, or disclosing credit card information, it allows the ISP to couple its knowledge of an individual's web activity with detailed purchasing histories. ISPs are also gaining ground in controlling subscribers' web content. If contacted about a copyright or trademark violation, ISPs have the authority to "take down" a subscriber's site until the dispute can be settled. In this mode, ISPs are becoming the content police of the new millennium. They are able to regulate content that may or may not be offensive to others. Whether web content is classified as "freedom of speech" or not, the economics of the situation lead one to believe that a great deal of power is trending toward phone companies, digital merchants, and ISPs.

With the potential for virtual personae to float around in cyberspace, there is a need to anchor personal identities, authenticate web activity, and ensure that individual rights are not being violated. One method that has been successful is that of seeking "functionally equivalent" trademark protection in cyberspace, designing and adapting protection in cyberspace using the existing patterns found in the offline world. Although this method has found favor with the business community, its application rewards those who can afford the protection. It could threaten the "little guy." Identity development and branding is something that favors big business. Brand equity currently plays an important role in our traditional offline commercial marketplace. And it is one of the most promising anchors that can stem the tide of chaos on the web and reduce identity float for businesses and individuals.

V. THE NEED FOR ANCHORS IN CYBERSPACE

Randall Davis, professor of Computer Science at the Massachusetts Institute of Technology, has cited the need for a broad framework to ensure the future vitality of the Internet economy.[31] He suggests that approaching the problem from a single viewpoint would be inadequate. The distribution and use of digital information relies upon an interaction between three main components: law, technology, and business.

A. Proposed Legal Anchors

In the legal realm, governmental entities and corporate legal teams have been the most active. Although it would be impossible to cover all of the events that

31. *New Framework Proposed for Protecting Intellectual Property Rights and Public Access to Electronic Information*, NATIONAL ACADEMIES, Nov. 9, 1999 (press release) <http://www2.osl.state.or.us/archives/libs-or/nov99/0019.html>.

have transpired since e-commerce became the world's darling, there are a few key people and initiatives worthy of being mentioned. First is the Federal Trademark Dilution Act of 1995.[32] Senator Patrick Leahy demonstrated much insight by expressing concern over an issue that would not surface as a major problem until the turn of the new millennium. The Congressional Record quotes him as saying, "Although no one else has yet considered this application, it is my hope that this antidilution statute can help stem the use of deceptive Internet addresses taken by those who are choosing marks that are associated with the products and reputations of others."[33]

Leahy's comments struck right to the heart of the matter. While legacy marks had served to anchor the identity of products and reputations in the old economy, Internet addressing slowly emerged as a vehicle for providing the same function on the web. Since the passage of the Federal Trademark Dilution Act, it has been difficult to judge exactly how effective the act has been at boosting consumer confidence and preventing the misuse of trademarks as domain names, but one has to commend Senator Leahy for his insight.

In 1996, a landmark Telecommunications Act[34] was passed in the United States, authorizing the FCC "to levy the equivalent of an annual $2.25 billion tax on business phone bills to subsidize [Internet] access for all schools and libraries."[35] This legislation was the beginning of an attempt to involve business and other stakeholders in the development of the new U.S.- flavored e-conomy.

Also in 1996, the United Nations Commission on International Trade Law (UNCITRAL) formulated a Model Law on e-commerce.[36] The goal of the law was two-fold. It sought to offer national legislators a set of internationally acceptable rules that would remove statutory obstacles from the free flow of legally significant electronic data across international borders. It also sought to facilitate harmonious international economic relations by fulfilling the purposes and functions of traditional paper-based requirements through a "functionally equivalent approach" using electronic commerce techniques. The UNCITRAL approach was adopted to cover alliances formed on land, on the sea, by rail, and in the air.[37] A significant aspect of the UNCITRAL Model Law was its inclusion of e-mail as a form of e-commerce. The Model Law distinguishes between those who are liable for originating e-commerce and intermediaries such as ISPs.[38] Above all, it legitimizes the value of computer-generated records and provides alternatives to paper-based originals as long as the integrity of a message can be proven unaltered from beginning to end.[39]

As schools and libraries went online in the United States, a shock factor that threatened e-commerce reverberated throughout the country. This time, the gov-

32. 15 U.S.C. § 1125 (1996).
33. 141 Cong. Rec. S19312 (daily ed. Dec. 29, 1995) (statement of Senator Leahy).
34. 47 U.S.C. § 251 (1996).
35. *See supra* note 14.
36. *See* <http://www.uncitral.org/english/texts/electcom/ml-ec.htm>.
37. *Id.* at *5.
38. *Id.*
39. *Id.* at *6.

ernment expressed concern over the web's ability to harm young stakeholders in the new e-conomy. The fear was that the government's investment in the web's potential as an educational and informational resource would be wasted if parents were unwilling to avail themselves of its benefits because of its repulsion factor. Calling the internet "an unparalleled educational resource," the U.S. Justice Department filed a legal brief with the Supreme Court in an attempt to ban sexually explicit material from the Internet.[40] The move was admirable, but it failed. The Supreme Court struck down the federal law.[41] In spite of noble efforts made by the Justice Department to protect children from the harmful material, "freedom of speech" was given as the reason for striking down the law. After the ruling, ACLU attorney Stefan Presser was quoted as saying, "Government will not be able to censor what's on the Internet."[42]

President Clinton and Vice President Gore, in issuing the Framework for Global Electronic Commerce in July 1997, cited the problem of an unstable legal environment in online transactions as one reason many businesses and consumers are still wary about e-commerce.[43] In order to correct this problem, Commerce Secretary William Daley was given a presidential mandate to "work with the private sector, State and local governments, and foreign governments to support the development, both domestically and internationally, of a uniform commercial legal framework that recognizes, facilitates, and enforces electronic transactions worldwide."[44]

1. First Steps

A first step toward this goal was for the Commerce Department to stand behind the National Conference of Commissioners of Uniform State Law (NCCUSL) in promoting its Uniform Electronic Transactions Act (UETA).[45] UETA builds upon the UNCITRAL Model Law and seeks to establish a predictable domestic framework that can be used by the rest of the world for legal recognition of electronic records and electronic signatures. It is not contract-oriented, and it is designed to work with and support existing systems rather than dictate a separate system.[46] Several essential elements have been identified as requirements for enabling electronic transactions in the commercial environment.[47] Electronic agreements should have the same legal status as paper agreements.[48] Electronic contracts should be legally binding and enforceable in court against a person or entity that is party to the contract.[49] Techniques for

40. John Gehl and Suzanne Douglas, *U.S. Says Indecent Material Will Ruin Educational Value Of Net*, CHRONICLE OF HIGHER EDUCATION (Jan. 31, 1997).
41. *See* Reno v. ACLU, 521 U.S. 844 (1997).
42. James Vicini, *Supreme Court Strikes Down Internet Indecency* (viewed June 26, 1997) <http://www.reuters.com>.
43. *See supra* note 3.
44. *Id.*
45. *Id.*
46. *Id.*
47. *Id.*
48. *Id.*
49. *Id.*

identifying both parties entering into electronic agreements should be validated through some type of "signed" digital signature.[50] One of the appealing features about UETA is its technology-neutral approach to enabling electronic commerce without requiring anyone to enter into a contract.[51] As businesses, using whatever digital authentication method they prefer, continue to operate in closed systems, UETA offers a transparent, non-intrusive legal framework rather than a prescriptive set of government regulations and mandates.

In general, the Department of Commerce has been encouraging other governments to adopt the following principles:

> (1) eliminate paper-based legal barriers to electronic transactions by implementing the relevant provisions of the 1996 UNCITRAL Model Law on Electronic Commerce
>
> (2) reaffirm the rights of parties to determine for themselves the appropriate technological means of authenticating their transactions
>
> (3) ensure any party the opportunity to prove in court that a particular authentication technique is sufficient to create a legally binding agreement
>
> (4) treat technologies and providers of authentication services from other countries in a non-discriminatory manner.[52]

Although the Commerce Department has a persuasive viewpoint, there are two different legal models for electronic authentication developing internationally.[53] The model promoted by the United States focuses on eliminating barriers to electronic agreements and electronic signatures without granting special legal status to any particular type of authentication.[54] The second model involves a greater degree of government regulation whereby electronic authentication methods are dictated and prescriptive technical requirements must be followed in order to ensure that electronic signatures on contracts will be legally binding.[55] The European Union's Electronic Signatures Directive is an example of the second approach.[56]

The United States may be to blame for helping Europe find its independent e-dentity. In July 1997, while attending a European Union-sponsored conference on Internet commerce, E.U. leaders met in Bonn to announce that they would work toward a regulatory framework to promote electronic commerce in Europe and in the wider international environment. Europe declared it would "work towards global consensus through active involvement in current international cooperation and negotiations, within the World Trade Organization (WTO) and

---

50. *Id.*
51. *Id.*
52. *Id.*
53. *Id.*
54. *Id.*
55. *Id.*
56. *Id.*

the Organization for Economic Cooperation and Development (OECD) to establish a stable, rule-based environment for electronic commerce."[57] In statements given by U.S. and E.U. leaders, it was also declared, "Europe will pursue international agreements concerning future management of the Internet DNS [ ]."[58] It was at this time that President Clinton proposed the creation of a free-trade zone on the Internet.[59] He wanted a free trade agreement within a year of the proposal and within the context of the WTO. Although E.U. Ministers stopped short of calling it a "free-trade zone,"[60] the idea found merit with enough people to become a formal part of the Bonn Declaration.[61]

It was also at this time that sweeping agreements were made to pursue the development of an international legal framework with coordinated positions on security for global information networks.[62] Though driven primarily by European initiatives, the United States agreed to model all global information networks after OECD guidelines. In a real sense, after the WTO and the OECD were endowed with such important responsibilities, the integrity of our national security hangs in the balance between these two external institutions. As a result, a special envoy from the United States was assigned to the OECD. It was the OECD that the President had in mind when he referred to his plan for the creation of a de facto global communications standard in which key algorithms needed for unscrambling messages would be placed in escrow with separate authorities.[63] The plan was shot down by opponents who said it "could have a detrimental effect on international trade and the world's ability to use the Internet for international commerce."[64]

Speaking before the U.S. House of Representatives Trade Subcommittee, Deputy Trade Representative Jeffrey Lang called on Europe "to join the United States in finalizing a global financial services accord by December [1997]."[65] He gave timelines for concluding a Multilateral Agreement on Investment with Europe by the spring of 1998 and for critical negotiations designed to manage global trading at the newly formed WTO in 1999.[66] Lang also requested approval of Congress for new "fast-track authority" to help the U.S. keep pace with the E.U. and have a greater influence in the development of the international economy.[67] Fast track was never granted.

---

57. Conference, *Global Information Networks Ministerial Conference* (held in Bonn, Germany July 6-8, 1997) <http://www2.echo.lu/bonn/commerce.html#HD_NM_23>.

58. *Id.*

59. *Group Oks Free Internet* (viewed July 8, 1997) <http://cnnfn.com/digitaljam/wires/9707/08/internet-wg/>.

60. *Id.*

61. *Id.*

62. John Gehl and Suzanne Douglas, *EU Ministers Issue Declaration on the Internet*, EDUPAGE (visited July 11, 1997)
<http://www.ee.surrey.ac.uk/Contrib/Edupage/1997/07/10-07-1997.html#3>.

63. John Gehl and Suzanne Douglas, *Clinton Advisor Defends Encryption Plan*, N. Y. TIMES (Jan. 29, 1997).

64. *Id.*

65. *US-European Economic Cooperation - Joint US-EU Effort Needed To Further Trade Reform*, (July 24, 1997) (statement of Jeffrey Lang, Deputy Trade Representative)
<http://www.usia.gov/current/news/lÖ?/products/washfile/newsitem.shtml>.

66. *Id.*

67. *Id.*

2. Alliance Formed

In October 1998, the OECD approved a Declaration on Authentication for Electronic Commerce affirming the principles set forth by the Department of Commerce.[68] The OECD declaration was followed by affirmations from the Global Business Dialogue on Electronic Commerce (GBDe), France, Japan, Korea, Ireland, Australia, and the United Kingdom. In keeping with the momentum that had been building, Senator Patrick Leahy sponsored an amendment authorizing a study by the National Research Council of the National Academy of Sciences.[69] The study, funded by the National Science Foundation, concerned the effects on trademark holders of adding new top-level domain names and recommendations on related dispute resolution procedures. The amendment was enacted as part of the Next Generation Internet Research Act.[70]

The results of the study are likely to have an enormous impact on the future of e-commerce in America. The report showed that novel business models, education, and new technologies would protect intellectual property more effectively than legislative changes.[71] Coupled with existing copyright laws, these methods would provide the widest non-intrusive protection for owners and distributors of digital information while maximizing access and use by the public. It was suggested that more time be given for businesses to adjust to the new challenges posed by the new e-conomy.[72] Legislators were warned to be slow to revamp intellectual property laws and public policy, exhausting research on the issues before making any major moves.[73] The study suggested that policy-makers should not focus on surface technologies, but rather on the underlying issues that influence market behavior, including consumer attitudes and new ways to distribute and profit from digital information.[74]

The report highlighted how the evolution of computer networks and the World Wide Web has changed the meaning of "publishing."[75] In the offline world, publication is public, irrevocable, and fixed. In the online world, a publication may be temporary, restricted from public access through technical means, changeable, and easily withdrawn from circulation.

Knowing whether a work has been published is legally significant for those who distribute it. In the process of distributing digital property, the first sale rule does not apply as it does in the offline world. The first sale rule allows the buyer of a copyrighted item to dispose of that same item without permission of the copyright holder.[76] Because of the vast number of reachable personalities online, the distribution of a single copy of work could adversely affect market demand

68. *See Ottawa Conference on Electronic Commerce* (Oct. 9, 1998) <http://www.ottawaoecdconference.orÖsh/announcements/e-oecdrelease.htm>.

69. The National Research Council is a private, nonprofit institution that provides independent advice on science and technology issues under congressional charter.

70. S. 2046, 106th Cong. (2000).

71. *See supra* note 31.

72. *Id.*

73. *Id.*

74. *Id.*

75. *Id.*

76. *See* 17 U.S.C. § 109(a) (1994).

much quicker than works distributed in hard copy by conventional means. That is why some argue that access to digital works should be restricted online in the same manner as in the offline world.

One of the ways information providers are managing access is through licensing. But licensing changes the balance of private ownership and public access. It lacks the elements of copyright law found in public policy and generally allows little room for negotiation. Because licenses are contracts, there is the potential for contract law to become a widespread substitute for copyright law in the new e-conomy. To combat this trend, the report recommends education highlighting the benefits of copyright and patent protections rooted in the U.S. Constitution. The report suggests that transient use of digital information acts as an eroding factor on our permanent social and cultural heritage. Businesses that make the right changes will play an important role in preserving culture. The music industry was singled out as a good business model for marketing, selling, and distributing products and services electronically. With the advent of MP3[77] threatening to siphon off millions of dollars from original artists, the industry found the backing it needed to take a leap forward. The music industry chose to avoid technically complex and legally burdensome ways of conducting e-commerce.

Business leaders have been forced to go back to the drawing board to determine the extent to which copying for private use can be justified without violating the law. The report suggests that archiving digital information has a preserving effect on our nation's cultural heritage.[78] But because copying is directly related to the way computers work on the web, relying upon legal restrictions that attempt to control copying are not recommended. The creation of a national task force was proposed.[79] The group would be responsible for developing legal and procedural frameworks for governing how electronic deposits are to be used in the future. The Library of Congress has already begun providing leadership in this area and will continue to do so.

Just before William Daley took the helm at the U.S. Department of Comerce, a new international framework was put in place for intellectual property. The Uruguay Round of the General Agreement on Tariffs and Trade (GATT) negotiations produced the Trade-Related aspects of Intellectual Property rights (TRIPS) agreement.[80] The TRIPS agreement outlined provisions for protecting patents, copyrights, trademarks, and relevant World Intellectual Property Organization (WIPO) treaties in our global trading system. Two relevant treaties, drafted in 1996 and put in place at WIPO, were the Copyright Treaty, and the Performances and Phonograms Treaty.[81] These treaties were intended to extend copyright protection to written materials and sound recordings on the Internet.

---

77. MP3 represents a standard format for storing digital music on the web.

78. *See supra* note 31.

79. *Id.*

80. *See* 19 U.S.C. § 3511 (1996) (the TRIPS agreement was part of the GATT Treaty entered into by the United States on April 15, 1994 following the Uruguay Round of the multinational trade negotiations).

81. These treaties were agreed to in Geneva on December 20, 1996 and entered into by the United States April 12, 1997. *See* 1997 WL 447232. The treaties were later implemented as part of the Digital Millennium Copyright Act of 1998. *See* 17 U.S.C. § 1201 *et seq.* (1998).

In an effort to comply with the WIPO treaties, Secretary Daley worked with the U.S. Congress to pass the Digital Millennium Copyright Act of 1998, also known as the WIPO Copyright Treaties Implementation Act.[82] His convincing argument included the vision that "one day people with a computer may have immediate access to every song ever sung, every movie ever made, every creative work ever created."[83] The House of Representatives approved the bill on August 5, 1998, and it received unanimous support in the Senate, passing 99-0.[84] President Clinton signed the bill into law in October 1998, resulting in the most significant revision of U.S. copyright law in two decades.[85] On September 14, 1999, the United States' instrument of ratification for the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) were deposited with the Director General at WIPO Headquarters in Geneva.

Besides addressing the use of blocking software for federally funded schools and libraries as a means for regulating Internet content, one unique aspect of this legislation is that it seeks to ensure that other nations will provide copyright protection for electronic commerce at an equivalent level.[86] By giving copyright owners the right to "authorize" the availability of their works to the public through electronic means, one can facilitate greater access to arts and entertainment, help artists and businesses expand into wider markets, and thwart on-line piracy.

In an effort to move forward in the digital age, Secretary Daley has composed five guiding principles for the U.S. Department of Commerce.[87] These principles not only reveal the specific strategies that will be pursued, but they also identify the players with whom our government will join in the task of building the new e-conomy.

First, the future of the Internet must be built around solutions that work globally.[88] This principle does not mean employing one solution around the world, but rather finding different policies and procedures that will work anywhere in the world regardless of their technical genre.

Second, e-commerce has the potential to level the playing field.[89] Amateur artists, lacking the financial backing and marketing power of large commercial organizations, can sell their goods and services on the Internet with the same global coverage as those who do have money and power. In order to nurture this inherent balance, the privacy of participants and the integrity of their transactions must be retained. Recognizing the importance of privacy as "a basic American

82. 47 U.S.C. § 101 (1998); *see* Nancy Weil, *House Passes Internet Copyright Bill* (visited February 15, 2000) <http://www.computerworld.com/home/news.nsf/all/9808053right>.

83. William M. Daley, Remarks at the World Intellectual Property Organization Conference On Electronic Commerce and Intellectual Property in Geneva, Switzerland, (Sept. 14, 1999) <http://osecntl3.osec.doc.gov/publiÖs/8F9980ED4E458D5C85267EC006BE841>.

84. Nancy Weil, *House Passes Internet Copyright Bill* (visited February 15, 2000) <http://www.computerworld.com/home/news.nsf/all/9808053right>.

85. *Id.*

86. *See supra* note 81.

87. *See supra* note 83.

88. *Id.*

89. *Id.*

value," Vice-President Gore has called for the creation of an Electronic Bill of Rights for all Americans.[90]

Third, a new digital legal system is needed. It should be anchored in long-established trademark rules that will curb the abuse of trademarks by cybersquatters, address privacy concerns, update contract law, and ensure consumer protection. At the end of 1998, management of the domain name registration process was being transitioned to the Internet Corporation for Assigned Names and Numbers (ICANN).[91] Additionally, the U.S. began relying upon WIPO, a United Nations agency, for advice concerning the creation of dispute resolution procedures for trademark and domain name holders.[92] These moves highlight the government's eagerness to press forward in developing the new e-conomy without the typical bureaucratic red tape and unnecessary judicial processes often associated with large government programs. Instead, the international private sector has been entrusted with a central role in making policy decisions based on sound business practices.

Fourth, the American Patent and Trademark Office will continue to work with WIPO to realize a global patenting system.[93] This collaboration will entail revising patent law to bring a convergence to the administrative aspect of the world's patent offices.

Fifth, the skills of scientists and engineers need to be leveraged to realize the possibilities technology can play in protecting the information that flows over the Internet.[94] This approach may address intellectual property concerns in ways more efficient than legal means.

Secretary Daley's guidelines provide a glimpse into the future of how the American flavored e-conomy might pan out. The Department of Commerce will be depending upon information provided by the private sector and foreign governments. But one would be naïve to think that this worldview would be accepted wholeheartedly without criticism or dissension. In fact, it is almost inevitable that a certain amount of contention will come from well-intentioned individuals in Congress who believe their vision of cyberspace would be better for America.

B. Identification and Authorization

On November 10, 1999, the House passed the E-signature in Global and National Commerce Act.[95] It passed 356 to 66—enough votes to avoid a veto. H.R. 1714 is intended to provide a broad framework that will set national standards for electronic signatures and records. It endows electronic signatures, records, and e-agreements with as much legal validity as paper contracts. It

---

90. *White House to Propose Internet Privacy Law for Kids* (visited July 31, 1998) <http://www.allpolitics.com/1998/07/31/ap/privacy/>. *See also, Government gives Internet until year's end on privacy rules*, (visited July 21, 1998) <http://www.cnn.com>.

91. *See supra* note 83.

92. *Id.*

93. *Id.*

94. *Id.*

95. H.R. 1714, 106th Cong. (1999).

addresses consumer confidence by encouraging the use of biometrics as a way of authenticating users online. And it acknowledges the need to support e-transactions in "closed" systems where they mostly occur.

Speaking before the Courts and Intellectual Property Subcommittee, House Committee on the Judiciary, Andrew J. Pincus, General Counsel at the U.S. Department of Commerce, pointed out "a number of significant flaws that would have to be addressed before the Administration could support this."[96] Pincus stated that H.R. 1714 should exclude government transactions, applying only to the elimination of barriers to e-transactions between private entities.[97] The fear is that these measures might be counterproductive in light of other initiatives such as the Government Paperwork Elimination Act (GPEA).[98] GPEA states that government should not dictate authentication standards to the private sector and requires that agencies adopt multiple optional means whereby citizens and businesses can transact business with them.[99] GPEA also states that government cannot dictate its preferred standards or methods to the private sector.[100]

In another area, section 102 of H.R. 1714 "places significant . . . inappropriate limits upon the State's ability to alter or supercede the federal rule of law."[101] And therefore, it should be limited to "a temporary federal rule" until the States have time to adopt UETA, thereby sunsetting H.R. 1714.[102] As written today, the "State's laws would remain subject to federal preemption even when those States adopt the UETA."[103] Title I section 102(b)(1) and (2) of H.R. 1714 places excessive limits on governmental authority and appears to preclude any regulation of private parties' authentication practices. This provision could potentially prevent the government from engaging in limited regulation of some private parties' authentication methods and practices, especially where public interests may be affected.

Declaring the need to preserve the states' authority to adapt consumer protection regimes to the electronic environment, Pincus blasted H.R. 1714's "party autonomy provision" found in section 101(b).[104] H.R. 1714 gives too much authority to the Secretary of Commerce to bring actions against non-conforming state laws. The recommendation is for this authority to be instituted by the Attorney General on behalf of the Secretary of Commerce. Lastly, according to Pincus, H.R. 1714 could override federal law as well as state law in its scope.[105]

The arguments over H.R. 1714 demonstrate just how difficult it will be to transition from our current legal system to one that can effectively deal with the challenges posed by the new e-conomy. So far, most of the legislation aimed at supporting e-commerce has been generated on an as needed basis. And even this

96. *See supra* note 3.
97. *Id.*
98. 44 U.S.C. § 3501 (1995).
99. *Id.*
100. *Id.*
101. *See supra* note 3.
102. *Id.*
103. *Id.*
104. *Id.*
105. *Id.*

approach has been an intense uphill battle for those who have deemed it worth the effort. Looking at the guidelines provided by Secretary Daley and the Commerce Department, one can see that broad strokes were intended. On the other hand, the details formulated by Congress in H.R. 1714 have been specific and narrow in scope.

H.R. 1714 gives new credibility to e-agreements. If one considers the most binding agreements used on the web today, one would find that they are "signed" with the simple click of a mouse, often without even being read. One example is the agreement that pops up when a user installs a new software program on a computer. If the program is a Microsoft product, the user normally has to agree to abide by the terms and conditions of a license that may or may not qualify as a UETA license.

In a similar fashion, to register a domain name, one has to agree to the terms and conditions set forth by the registrar. Typically, these agreements are full of indemnity clauses. They are often built on policies that can change at any time at the sole discretion of the registrar. And to make matters worse, the laws of the state of the registrar often govern the agreements. For the moment, it seems as though the cards are stacked against those who habitually gloss over the trivial.

Several technical means are being employed to facilitate user authentication on the web. The use of digital certificates is causing a shift toward individual online accountability. These mini e-agreements are considered legally binding in H.R. 1714.[106] Without special safeguards, one risks being impersonated online.

One of the most interesting provisions of H.R. 1714 encourages the use of biometrics.[107] Biometrics is becoming a popular way of authenticating users in cyberspace, allowing them to access computer networks by comparing the user's unique characteristics (*i.e.* fingerprints) against an image that has been programmed into the computer. Enhancing digital authentication practices is a good first step toward ensuring proper accountability online, but to suggest that biometrics will guarantee online privacy is to be extremely naïve. The emphasis is quite surprising, considering the repercussions one would expect from a wholesale loss of privacy and anonymity in cyberspace.[108] Elizabeth Boyle, president of I.D. International of New York, says "the security payoff with [biometrics] is huge if you want to open your organization up to the Web."[109] New offerings from Identix, KeyWare Technologies, and Advanced Recognition Technologies include face, voice, fingerprint, and handwriting recognition. Novell's DigitalMe product offers a glimpse into e-commerce's not-too-distant future. It describes a model where networked participants authenticate to the Internet and dish out permissions to providers of goods and services with whom they want to conduct business. In this scenario, the individual becomes the center for controlling and initiating all e-transactions over the web.

---

106. H.R. 1714, 106th Cong. (1999).

107. *Id.*

108. Anonymity stimulates healthy participation by those who act anonymously with the understanding that their identities will remain private.

109. Scott Berinato, *Biometrics Tools Guard Networks*, PC WEEK (Apr. 14, 1997).

A digital identification (ID) provides an electronic means of verifying one's online identity. Verisign, Inc., offers different levels of digital assurances that may be purchased. Class 3 digital IDs provide a high level of identity assurance by requiring an appearance before a notary. More and more web sites are offering services based on the validation of their subscribers' digital IDs. No longer does one have to login to the network with a username and password, because transparent authentication can be made behind the scenes using a secure digital ID installed in the web browser.[110]

Traditional password-oriented authentication methods are not strong enough to provide the legitimacy needed to conduct trusted transactions in today's e-commerce environment. Biometrics is taking the place of traditional password implementations, improving the reliability and security associated with conducting business online. Coupled with smart card technologies, biometrics will gain approval as a formidable guard against online impersonations.[111] One example of biometrics in action comes from Illinois. In an effort to discourage welfare fraud and abuse, the Illinois Department of Public Aid is requiring biometric identification as a condition of eligibility for all Aid to Families with Dependent Children (AFDC) benefit recipients. Governor Jim Edgar noted that retinal eye scanning and electronic fingerprinting would combat fraud to assure that only the truly needy receive benefits.[112]

It may not be too speculative to suggest that computer systems will soon conduct business on users' behalf over the web and speak on users' behalf in any language. Of course, users' will need to ensure that computer systems are properly authorized to make such decisions. But with biometrics and the proper e-agreements in place, this authorization will soon be possible.

On a related issue, the President and First Lady recently sponsored a White House Millennium Evening with guests Dr. Eric Lander, head of the Genome Project at MIT University, and Vinton Cerf, the Father of the Internet. The discussion centered on the moral and ethical implications involved in collecting DNA into databases for research purposes. Clinton, Lander, and Cerf explored ways that the Internet and the Genome Project could collaborate.[113] Cerf explained how it is possible to separate, extract, and store information about a consumer's buying habits.[114] He stressed the need for U.S. law to keep individual privacy rights at a high priority.[115] But he went on to state that DNA information is unique in that it cannot be separated from the individual. Unique DNA information "represents" an individual.[116]

---

110. *Why Do I Need A VeriSign Digital ID?* (visited Feb. 13, 2000) <http://www.verisign.com/repository/brwidint.html>.

111. Kristi Essick, *Biometrics, e-cash to gain ground in '98, Gartner says* (visited Feb. 13, 2000) <http://www.infoworld.com/cgi-bin/displaylcommerce.pl?/980129gartner.htm>.

112. Jan Farmer, *New Technology To Prevent Welfare Fraud* (visited April 21, 1997) <http://206.163.150.6>.

113. *Millennium Evening At The White House: Informatics Meets Genomics*, (visited May 10, 2000) http://www.pub.whitehouse.gov/uri-res/12R?urn:pdi://oma.eop.gov.us/1999/10/13/9.text.1>.

114. *Id.*

115. *Id.*

116. *Id.*

Calling it the "ultimate fingerprint," Cerf implied that DNA could serve as a biometric authentication signature.[117] He went on to give an example of man and machine working together, citing a story about computers that can be implanted to detect blood sugar levels and automatically trigger injections of insulin in the proper amounts for sufferers of diabetes.[118] In a related development, scientists at the University of Wisconsin-Madison have actually created a "DNA computer" from strands of synthetic DNA they coaxed into solving relatively complex calculations.[119] The potential use of DNA as a means for authenticating e-commerce transactions could be just around the corner.

1. Security Concerns

As one can imagine, this type of activity opens up security concerns. In early 1997, FBI director Louis Freeh, testifying before the Senate Judiciary Subcommittee, issued a stern warning that widespread use of computer encoding technology could wreak havoc on crime fighting efforts and the prevention of terrorism.[120] This fear prompted the Clinton Administration to uphold policies outlawing the export of strong encryption.[121] Nothing could be exported with more than 56-bit encryption keys unless a business was willing to plod through a lengthy approval process.[122] And absolutely no encryption could be exported to terrorist nations.[123] In the wake of the alleged breach of security at the Los Alamos Labs, the Clinton Administration proposed a new national security plan to deter cyber-terrorism and guard the country's critical computer systems. The plan establishes a central intrusion-detection network and creates a scholarship program to educate and recruit budding information technology experts for the government.[124] The most controversial part of the new plan is the creation of a federal intrusion-detection network, or FIDNet to monitor 22 government computer systems for signs of attack.[125]

In an ironic twist, while cracking down on cyber-terrorists, the Clinton Administration has had a change of heart on encryption. Some analysts estimate that companies have been forced to create domestic and exportable versions of their software resulting in as much as fifty percent more cost.[126] In order to stimulate the new e-conomy, measures related to the export of strong encryption have been relaxed.[127] Although the list of terrorist nations is still off limits, technology companies driving the new e-conomy could not be happier.

---

117. Having seen the implication quite clearly, I e-mailed Vinton Cerf and pointed out that his "ultimate fingerprint" comment obviously could have enormous biometric implications. I received a short e-mail reply from him the next day that simply stated, "big smile – v."

118. *Id.*

119. *Rick Callahan, Scientists Create 'DNA Computer'* (visited Feb. 13, 2000) <http://www.canoe.ca/TechNews0001/13_dnacomp.html>.

120. Aaron Pressman, *Computer Coding Could Cripple Cops, FBI Warns* (visited February 15, 2000).

121. Keith Perine, *Clinton Reveals U.S. Cyberterror Strategy* (viewed Feb. 15, 2000) <http://dailynews.yahoo.com/h/is/20000107/bs/20000107123.html>.

122. *Id.*

123. *Id.*

124. *Id.*

125. *Id.*

126. Jim Kerstetter, *Crypto Community Celebrates New Export Rules*, PC WEEK ONLINE (visited Jan. 19, 2000) <http://www.zdnet.com/pcweek/stories/news/0,4153,2423792,00.html>.

127. *Id.*

In the e-business community, the innocent use of software by employees could potentially jeopardize the entire company's future. A good example of this is an incident that sent shock waves throughout Wall Street and the telecommunications industry on May 22, 1999. An employee, "acting on his own initiative," reserved an Internet address that sparked rumors concerning an MCI WorldCom deal with paging company SkyTel Communications.[128] When the Internet address "skytelworldcom.com" was made public, MCI WorldCom backed away saying the domain request was "not an indication of any official company intention."[129] With the cat out of the bag, the official $1.8 billion deal was made public on May 28, 1999.[130]

In the world of e-business, employees and employers form partnerships built on varying degrees of privacy. In one sense, employers are obligated to provide protection for employees in the workplace. This includes being responsible for providing a safe work environment, free from harassment and inequity. But employers also have the right to protect themselves. They need to be concerned about all employees, not just those who may be labeled disgruntled. Businesses are having to protect themselves more and more from their own employees. One way many businesses are choosing to protect themselves is by closely monitoring the electronic activities of their employees. The courts have already made it clear that employers can track an employee's web activity.[131] One common off-the-shelf software package that employers can use is called Little Brother for Windows.[132] Little Brother can track what employees see, how long they see it, how often they see it, and how they use the information. Unlike Surfwatch, which blocks Internet sites deemed unacceptable, Little Brother quietly builds a log of all web activity that can then be reviewed by management. The courts have continually affirmed the right of employers to use this software in spite of the outrage it may provoke.[133]

2. The Use of Patent Law

Businesses, who are accustomed to having patent principles protect rights in products, have found that these same principles cause problems when applied in cyberspace. Although it is conceivable that a single patent lawsuit could squelch the rapid pace at which the web is driving the U.S. e-conomy, it is more likely that patent lawsuits may not be in the best interests of consumers.

Another problem with relying on patent law to resolve disputes in connection with e-commerce is the speed at which technology practices change. Since tech-

128. *MCI Drops SkyTel Net Address* (visited February 13, 2000) <http://news.cnet.com/news/0-1004-200-342911.html?tag=st.ne.1004-200-343083>.
129. *Id.*
130. John Borland, *MCI WorldCom Buys SkyTel for $1.8 Billion* (visited Feb. 13, 2000) <http://news.cnet.com/news/0-1004-200-343083.html?st.ne.fd.mdh.ni>.
131. *See infra* note 131.
132. Don Knapp, *Is Little Brother Watching You?* (visited Feb. 13, 2000) http://www.cnn.com/TECH/9703/04/computer.spies/>.
133. *Id.*

nology seems to double every eighteen months, it is becoming harder for patent lawyers to sue over infringements. In many cases, it takes longer to get a court date than it does to sue over a patent violation while the technology in question is still relevant.[134] Businesses know this and are embracing legal models that are more cost-effective and consumer-focused. Fewer are willing to use their patents as weapons in court because there is a growing realization that patents may not hold up under strict scrutiny for prior art,[135] or be worth the cost of a lengthy battle. Others will take the plunge and tangle themselves up in court until the technology is obsolete and the consumer has moved on to the competition.[136] Tim Bernes-Lee, inventor of the World Wide Web, has also come out against defending one's turf in cyberspace through patent law.[137] He warned that patents pose a danger to the universality of the web.[138] He sees how the misuse of patent law could stifle the extension of consumer benefits in the United States and around the globe.[139]

3. Branding

Another way businesses are trying to anchor themselves in cyberspace is through image branding. Branding has everything to do with identity development. Cultures and sub-cultures of society attach loyalty and a level of comfort to brands. Much of the franchising success of McDonald's can be attributed to this phenomenon. The effect of branding is much like drinking a cup of coffee. It is the "taste" of one's corporate or individual identity that can linger in the hearts and minds of people as a good or bad image, feeling, logo, word, or a combination of them all. Unfortunately, image branding is also closely tied to whimsical perceptions in the market. Because of this, branding has as much to do with market "spin" and "reality distortion" as it does with reality. The Better Business Bureau and other consumer advocacy groups stand ready to ensure a certain amount of truth in advertising when businesses get carried away with promising too much vaporware (products which are announced far in advanced of release and which may or may not be released).

Even so, businesses and individuals can choose to project themselves to the world in many different ways and must consider multiple contexts when crafting identity messages. If the messages fall on unfertile soil, the effort will not bear fruit. Corporate identity development involves anchoring the company with trademarks, service marks, special words, phrases, and symbols. These anchors are often targeted toward specific groups that might differ in age, ethnicity, or income. Some companies have been very successful at building "brand equity" in the offline world. Registered trademarks that fall into this category include

134. *See infra* note 130.
135. Mel Duvall, *Patent Pushers: Sell, Not Sue*, INTERACTIVE WEEK MAGAZINE (visited May 10, 2000) <http://www.zdnet.com/intweek/stories/news/0,4164,2292762,00.html>.
136. *Id.*
137. *Id.*
138. *Id.*
139. *Id.*

FedEx, Xerox, and Velcro. These companies have invested millions of dollars into image, reaping rich rewards through high name recognition and customer loyalty. Now they, along with the rest of corporate America, face the new challenge of defending and anchoring their identities in cyberspace.

In the virtual world of cyberspace, the traditional rules of the branding game have changed. To say that the waters have become a little muddied would be an understatement. Branding managers must now concern themselves with protecting corporate identity from electronic isolation through technical means, resisting acts of electronic prejudice, thwarting malicious hack attempts, reducing disruptive acts of impersonation, avoiding the misuse of trademarks, and identifying and prosecuting those who intentionally distribute misinformation. Corporate identities must be linked to new systems of online interactions that will accommodate trusted consumer e-transactions.

4. Cybersquatting

One of the most pernicious attacks on e-commerce has been cybersquatting. When the Internic (a domain registration service) began its first-come first-serve policy, the first person who selected a domain name received it. If the $70 registration fee was paid, no questions were asked. Traditional businesses never noticed what was happening to their brand equity or their future. While they were sitting around twiddling their thumbs, netizens were picking up names all over the web. Once traditional businesses realized that the web was a necessity for their survival, they went out looking for ways to establish their identities in cyberspace, only to find people sitting on their trade names.

In order to function on the Internet, the domain name would have to be purchased from the cybersquatter. This practice has become more lucrative for some than selling jewelry. As an example, the domain name "www.AsSeen OnTV.com" was registered for $70 and sold for $5,000,000.[140] Speaking of the deal, Mr. Daniel Fasano, Chairman and Chief Executive Officer of LA Group, Inc. stated,

> www.AsSeenOnTV.com is the premier domain name for the television direct to retail and Infomercial industry. The name has the highest level of public recognition because it is commonly used on signs and advertising in traditional brick and mortar retail stores like Wal-Mart, Kmart and others. In addition, it has been a tag line used in commerce for over fifty years. When you consider the enormous cost in developing brand awareness of an Internet portal, we're confident that this domain name will pay for itself many times over.[141]

In August 1999, the Senate passed the Anticybersquatting Consumer Protection Act.[142] It was quickly criticized for containing numerous problems.

---

140. *LA Group, Inc. Purchases Domain Name "www.AsSeenOnTV.com"*, BUSINESS WIRE (visited Feb. 15, 2000) <http://biz.yahoo.com/bw/000118/ny_la_grou_1.html>.

141. *Id.*

142. S. 1255, 106th Cong. (1999).

The bill would make "every fan a criminal" and could cause the use of certain filenames on the World Wide Web to be illegal.[143] It could threaten HTTP hyperlinking. It could give special privileges to "famous" names. It could stifle the use or registration of any identifier, including e-mail addresses and screen names in chat rooms. It could disrupt linking by imposing liability on site operators with unauthorized links to other sites. And it could threaten constitutionally protected web content and make it illegal to register take-over names such as "skytelworldcom.com."

In spite of these problems, the House approved its own version of the bill—H.R. 3028—in October.[144] The legislation brought criticism from the Clinton Administration. Speaking on behalf of the President, Joe Lockhart said that a more international approach to stop cybersquatting should be implemented using ICANN to oversee the operation. "We believe that fundamentally we'd be walking down the wrong road if we legislated a cybersquatting law and then the 200 or so Internet countries around the world started legislating their own rules and laws. The right way to do it is through this international process and we're working very hard to get that done."[145] Civil libertarians have opposed the new legislation, arguing it threatens free expression on the Internet, possibly outlawing parody and protest sites.[146] President Clinton signed the Anticybersquatting Consumer Protection Act, but the signing went unnoticed by many as it was buried down in the Intellectual Property and Communications Omnibus Reform Act—a large federal spending bill.[147]

In another incident, the World Wrestling Federation filed a complaint on December 2, 1999, a day after a new anticybersquatting procedure went into effect. On January 14, 2000, the Federation was declared the winner in the first case decided under a new global system to curb cybersquatting.[148] A U.N. agency based in Geneva ordered Michael Bosman of Redlands, California, to give the Federation the domain name "www.worldwrestlingfederation.com" or see his Internet registrar reissue it to the wrestlers anyway. The decision was handed down from a WIPO panel headed by California lawyer Scott Donahey. The panel ruled that the name "is identical or confusingly similar to the trademark" of the federation.[149]

VI. DOMAIN NAMES AND TRADEMARKS MERGE

As more people begin to contemplate the economic ramifications associated with anchoring their identities in cyberspace, there will be a greater sense of

143. *Id.*
144. H.R. Res. 3028, 106th Cong. (1999); *See* Jim Abrams, *Domain Names Protection Bill Passed* (visited Feb. 15, 2000) <http://news.cnet.com/news/0-1005-200-1453578.html?dtn.head>.
145. *Id.*
146. *Id.*
147. S. 1948, 106th Cong. (1999).
148. Geir Moulson, *WWF Wins First Cybersquatting Case*, ASSOCIATED PRESS, (Jan. 15, 2000) <http://dailynews.yahoo.com/h/ap/20000115/tc/wwf_internet_4.html> (the complaint was filed with the WIPO, not in an American court).
149. *Id.*

urgency to understand the use of domain names and trademarks. Those who grasp the functional differences between the two will be better positioned to cope with the new challenges of e-commerce. And many will look to the legal community for help in making sense of it all.

There are a few key points about the branding functions of trademarks and domain names that are worth mentioning. In the digital world, one cannot function without a domain name. The general rule in the domain name registration process is that there can only be one unique domain name for any given character string.[150] Therefore, there can only be one legitimate "microsoft.com" in the world. A domain name serves as the primary gateway for one's online existence. It is a door to the global e-conomy and the future.

Technically speaking, the domain name is only one component of a much larger domain naming system known as the Domain Name System (DNS).[151] DNS is a hierarchical database containing records that describe the name, IP address, and other information about computer devices all over the world. DNS furnishes a name-to-address directory service for network applications, mapping globally unique IP addresses (such as 207.68.156.53) to globally unique names (such as "microsoft.com"). DNS literally represents the heart and soul of the World Wide Web.

When businesses first started extending themselves to the web, it became quite popular to select domain names that matched the company name. IBM selected "ibm.com" to indicate they had opened up for business on the commercial side of the web. Soon thereafter, domain names were registered to highlight trademarked products, words, and even phrases that mimicked brand significance in the offline world. A couple of examples include Universal Resource Locators (URLs) such as "itstherealthing.com", "flythefriendlyskies.com," and "builtFordtough.com." As advertising dollars were focused toward reaching those in the new e-conomy, web site addresses began showing up on television, in print media, and even on the sides of trucks. This practice made it easy for consumers to find goods and services on the web. But it was at this point that domain names took on a new role. Domain names not only provided globally unique mapping functions for DNS, they also began serving a primary branding function by anchoring identities in cyberspace.

Trademark laws don't map to domain name structures very well. To own a trademark, one must adhere to a completely separate trademark registration process with its own set of rules. For instance, it is possible for different people or companies to own and use identical trademarks in the same country as long as the products and services are not confusingly similar. An example of this is the Apple trademark. It is owned by Apple Computer Company and by those who

150. In some cases, domain name registrations in countries outside the United States require proof that your business is incorporated within that country's borders before you can gain rights to the domain name there.

151. Diane Davidowicz and Paul Vixie, *Securing the Domain Name System*, NETWORK MAGAZINE, Jan. 2000, at 92.

own the Beatles' record label. This functional disparity means that a domain name may serve as a trademark, but a trademark may not serve as a domain name.[152]

Trademarks do have a significant branding value on the web. Unlike domain names, trademarks are often represented as graphical symbols or logos. On the web, logos may carry more value than domain names. There is much truth to the old adage "a picture is worth a thousand words," proven for years in the offline world through the use of company logos on stationary and business cards. But trademarks can lose their ability to influence the public if they become too common. Nike experienced this problem.[153] So, they decided to replace their world famous swoosh with a smaller one that includes Nike co-founder Bill Bauerman in the silhouette.[154] One would not have the same worries in cases where domain names were serving as trademarks in the online environment. If the trademark became watered down, the domain name would still be useful in providing its DNS mapping function.

Bob Anderson, deputy assistant commissioner for trademarks in the U.S. Patent and Trademark Office (USPTO), made a perceptive comment when he stated, "There is this tension between the trademark world and the Internet world."[155] What it really boils down to is a blurring of the lines between the rights of those who hold domain names and those who hold trademarks. Both have honorable reasons to be tense. One typically wants to do business on the web with the same freedom of speech that exists in the offline world. The other is typically fearful of losing an investment in brand equity. With the stakes so high on both sides of the equation, it is likely that this picture will get much uglier. Trademark and domain name protection should be a high priority for those working on the global legal framework. Identity fraud and impersonations can wreak havoc on consumer confidence. It is imperative that those with whom consumers conduct e-business be legitimate players.

Resolving the problem of trademark and domain name ownership is critical. Too much is at stake to flounder for years before acting. No one said it would be an easy task. Disputes over brand infringement can be quite complicated. Ownership of a trademark does not mean automatic rights to the domain name. And domain name ownership does not guarantee that trademark ownership will quickly follow. Many questions are still left unanswered about who should take the lead in resolving these issues. These questions are too important for rule-makers to force the issue or to rush to conclusions. They need to be handled with a sense of urgency, coupled with close scrutiny to protect consumer confidence and prevent brand dilution.

---

152. David Pescovitz, *Laying Down the Law on Domain Names*, (visited Feb. 13, 2000) <http://cnn.com/TECH/computing/9908/25/domain.myth.idg/>.

153. *Nike Founder Honored with Shoe Line*, NATIONAL POST (visited December 28, 1999) <http://nikebiz.com/story/pressin4.shtml#honor>; *see also* <http://www.oregonlive.com/business/99/10/bz100108.html>; <http://cyber.law.harvard.edu/metaschool/fisher/domain/tm.htm>; http://www.lexlaw.com/webdoc2.htm>.

154. *Id.*

155. Joseph Menn, *Trademark Issues Scuttle Plan for Web Names*, DENVER POST (visited May 25, 1999) <http://www.denverpost.com/enduser/trademark0510.htm>.

Businesses are responding differently to the issues. Even though the current law only protects trademark owners, businesses apparently feel secure in spite of the fact that no law protects a domain name from infringement. Other businesses are not willing to take that risk. They are beginning to register their domain names as trademarks. However, most companies simply do not protect their domain names with trademarks.[156]

In cases where a business' domain name has already been taken by a cybersquatter, it may be too late. Businesses encountering this situation have few options. Trademark law prohibits the use of similar marks when two conditions are met.[157] The mark must be similar and its use must cause a degree of confusion in the market.[158] To make matters worse, the chances of wrestling the domain name out of the hands of a cybersquatter drop off significantly if the name is not used at all. The logic flows like this: if the domain name is not used, it is impossible for the name to cause confusion in the market. Therefore, there is no case, and one's best option is to seek an injunction preventing the domain name owner from using the name to cause confusion in the market. The only other option is to pay a large sum for the name or accept the consequences of inaction.

One's e-business objectives and market spin toward the web should be anchored in the new branding functions of trademarks and domain names. Businesses can hope for a single registration process that combines protections for domain names and trademarks into one. But until new directory technologies emerge to support a globally unique graphical model of branding, these issues will continue to be litigated.

VII. ICANN - PRIVATIZED INTERNATIONAL GOVERNANCE

Elizabeth Heichler, Managing Editor of the IDG News Service in Boston, listed what she considered to be the top ten information technology news stories of 1998.[159] Some of the more interesting selections included the liberalization of the European telecommunications market, AOL's purchase of Netscape, WorldCom's acquisition of MCI, and the Department of Justice bringing a formal antitrust suit against Microsoft. But there was one event that stood head and shoulders above the rest. In fact, it may have a bigger impact on the future of e-commerce than any of the others mentioned. The event was simply listed as "U.S. Kicks the Net Out of the Nest."[160]

---

156. *See infra* note 157.

157. Brett N. Dorny, *Your Money or Your Name* (visited Feb. 15, 2000) <http://cnn.com/2000/TECH/computing/01/19/money.name.idg/index.html>.

158. 15 U.S.C. § 1051 *et seq.* (1994).

159. Elizabeth Heichler, *Top 10 Stories of 1998* (visited February 13, 2000) <http://www1.pcworld.com/pcwtoday/article/0%2C1510%2C9156%2C00.html>.

160. *Id.*

On June 10, 1998, the U.S. government issued a Statement of Policy on Management of Internet Names and Addresses.[161] This document, known as the White Paper, invited the private sector to form a global consensus entity to take over the responsibility for Internet protocols, domain names, Internet protocol (IP) addresses, and the Internet root server system.[162] Four months later, a non-profit private corporation known as the Internet Corporation for Assigned Names and Numbers (ICANN) accepted the invitation and began one of the world's bravest experiments in privatized international governance. Businesses all over the world would come to rely upon this group for the smooth functioning and continued growth of the Internet. ICANN would not be alone in this endeavor. The new "Net Regime," as ICANN is called by the Europeans, is collaborating on policy development with the United Nations under the auspices of WIPO.[163] WIPO's involvement was intentionally built into the process from the beginning. One reason was to ensure that the new procedures would be applied consistently in local, national, and international jurisdictions in order to build business and consumer confidence in communications and e-commerce.

The White Paper states:

> The U.S. Government will seek international support to call upon the World Intellectual Property Organization to initiate a balanced and transparent process, which includes participation of trademark holders and members of the Internet community who are not trademark holders, to develop recommendations for a uniform approach to resolving trademark/domain name disputes involving cyberpiracy, recommend a process for protecting famous trademarks in the generic top level domains, and evaluate the effects, based on studies conducted by independent organizations, . . . of adding new gTLDs and related dispute resolution procedures on trademark and intellectual property holders. These findings and recommendations could be submitted to the board of the new corporation [ICANN] for its consideration in conjunction with its development of registry and registrar policy and the creation and introduction of new gTLDs.[164]

As the ICANN Board endorses WIPO recommendations concerning domain names and trademarks, the implementation of these recommendations are working themselves into every e-business' core branding program. This fact is one of the main reasons the White Paper requests WIPO's assistance be "balanced and transparent."[165]

---

161. Statement of Policy on Management of Internet Names and Addresses, 63 Federal Register, 31741 (1998).

162. *See supra* note 3 (prepared testimony of Michael M. Roberts, Interim President and Chief Executive Officer of the Internet Corporation for Assigned Names and Numbers).

163. *Global Group Debates New Domain Name Scheme* (July 28, 1998) <www.computerworld.com>; *Europeans OK New Net Regime* (Nov. 6, 1998) <www.cnn.com/TECH/computing/9811/06/euronetreg.idg/>.

164. *See supra* note 3 (prepared testimony of Francis Gurry, Assistant Director General and Legal Counsel of the World Intellectual Property Organization); *see also* Management of Internet Names and Addresses, 63 Federal Register, 31,741-43 (1998).

165. *See* sources cited *supra* note 164.

In the beginning, ICANN's initial activities progressed with very little intervention from Congress. But it was not long before ICANN was accused of wielding its authority in a reckless manner. On June 22, 1999, a letter found its way onto the desk of ICANN's Interim Chairman, Esther Dyson, written by Representative Tom Bliley, Chairman of the U.S. House Commerce Committee:[166]

> I am writing to express my concern about recent steps taken by the Internet Corporation for Assigned Names and Numbers ("ICANN") as part of its role in the transition to privatize management of the Internet's Domain Name System ("DNS") . . . . I remain troubled about the manner in which the interim board members were selected, and have new questions about the manner in which the interim board is operating. I also am greatly concerned about the interim board's imposition of a $1 per domain name registration fee, the funding of a rather large ($5.9 million) ICANN budget through such a fee, and the setting of highly regulatory accreditation requirements for those who wish to offer domain name registration services . . . .
>
> Such decisions likely exceed the authority that the White Paper originally contemplated for the private organization whose role ICANN now is attempting to fulfill. Rather than promote the Internet's evolution, your organization's policies actually may jeopardize the continued stability of the underlying systems that permit millions of people to use, enjoy and transact business on the Internet . . . .
>
> Moreover, I understand that during the most recent ICANN board meeting in Berlin last month, the interim board reportedly threatened to terminate the authority of the incumbent domain name registrar—Network Solutions, Incorporated ("NSI")—to continue registering domain names if NSI fails to enter into a registrar accreditation agreement with ICANN by June 25, 1999. What makes this situation more distressing is the simple fact that these steps are being decided upon and implemented by an unelected board that conducts portions of its official meetings in private. In this light, I do not believe the process followed by ICANN's interim board during its recent work toward the privatization of the DNS has been sufficiently transparent.[167]

The tone of the letter, for all intents and purposes, was justified. Besides acting in secret, jeopardizing the stability of the Internet, exceeding its authority, and threatening those who don't play by the rules, ICANN had not met expectations. What makes Chairman Bliley's comments so alarming is the fact that the sovereignty of nations and the e-conomies of the world depend upon the proper functioning of the Internet's domain name space. Chairman Dyson responded:

---

166. *ICANN Responds to House Commerce Committee Questions*, BUSINESS WIRE (visited Feb. 15, 2000) <http://www.isoc.org/internet/issues/dns/990709.shtml> (NOTE: this cite is only to a summary of the letter—not the verbatim letter).

167. *Id.*

> ICANN's only authority is derived from the consensus of all those organizations, consumers, and businesses who make the Internet possible and take a active interest in using, enjoying and doing business on the Internet. ICANN has no statutory or regulatory "authority" of any kind. It has only the power of the consensus that it represents, and the willingness of members of the Internet community to participate in and abide by the consensus development process that is at the heart of ICANN.[168]

In answer to the reason for having secret meetings, Chairman Dyson explains, "[t]he Internet community, amongst who ICANN is charged with developing consensus, has shown widespread acceptance of the need for ICANN's board and staff to engage in non-public conversations, in order to make progress."[169]

Representative Bliley is not the only one who has recognized the need for a balanced transition to ICANN. There is an air of caution being expressed by many. Senator Patrick Leahy warned Congress:

> I understand the Internet Corporation for Assigned Names and Numbers (ICANN) and the World Intellectual Property Organization (WIPO) are considering mechanisms for resolving trademark and other disputes over assignments of domain names in an expeditious and inexpensive manner. This is an important issue both for trademark holders and for the future of the global Internet. While I share the concern of trademark holders over what WIPO has characterized as "predatory and parasitical practices by a minority of domain registrants acting in bad faith" to register famous or well-known marks of others—which can lead to consumer confusion or downright fraud—the Congress should tread carefully to ensure that any remedies do not impede or stifle the free flow of information on the Internet.[170]

As one could imagine, ICANN has attracted as many other critics as it has supporters. In April 1999, Jay Fenello, President of Iperdome, Inc., spoke of the need to fight for fair and open processes at ICANN, the protection of minority interests, and most importantly, the protection of civil liberties.[171] His Personal Domain Name Holders Association (PDNHA) was created to give individuals a voice in the legislative branch of ICANN for this purpose.[172] He went on to say,

> U.S. citizens have come to expect certain rights and civil liberties from our government. Unfortunately, this unique American perspective has collided with the governance philosophies found in the other 240+ countries throughout the world. Consequently, many of our most closely held beliefs about governance have not been incorporated into ICANN. Things like no taxation without representation, due process, consent of the governed, etc.[173]

---

168. *Id.*
169. *Id.*
170. *Id.*
171. *Iperdome To Organize Netizens For Internet Governance*, (Iperdome Press Release) (April 22, 1999) <http://www.iperdome.com/releases/990422.htm>.
172. *Id.*
173. *Id.*

On September 24, 1999, Fenello announced he was suspending operations.[174] Iperdome, as one of the oldest and most active prospective registries, found no place at the table in the government's privatization experiment. A distraught Fenello was quoted as saying,

> Iperdome has participated in good faith in the U.S. Government's efforts to privatize the administration of Internet resources. In recent months, it has become apparent that these efforts were to no avail, as the process has been captured, and is unlikely to fairly resolve outstanding issues of new Top Level Domains.[175]

Even consumer rights advocate Ralph Nader jumped on the bandwagon and criticized ICANN for catering to corporate interests.[176] And, unsolicited, he went one step further, proposing ways that ICANN could be based on a multilateral government charter.[177]

Another person who is cautious about the current transition to ICANN is University of Miami Law Professor, A. Michael Froomkin. Froomkin served as an expert advisor for WIPO and now seems critical of ICANN. In his article entitled *A Contract with the Internet*, Froomkin explores many of the same concerns shared by Chairman Bliley.[178] Concern is expressed over the transparency of ICANN, the potential for its subsidiary bodies to become captured by corporate and trademark interests, the lack of visible bottom-up decision-making, and its structural similarity to the un-accountable International Olympic Committee (IOC).[179]

On July 22, 1999, Mike Roberts, ICANN's interim president and CEO, testified before the House Commerce Committee at a hearing entitled *Is ICANN Out of Control?*[180] Roberts' testimony revealed that ICANN was $800,000 in debt and relying on private donations to pay the bills. When ICANN's proposed $1 tax per domain name idea was squelched, so was the potential to make $6 million per year from registrants. ICANN openly received "loans" from key corporate stakeholders, including MCI WorldCom at $500,000 and Cisco Systems at $150,000. The loans were "part of an international effort to provide temporary financial support for ICANN until . . . permanent funding [could be] . . . put in place."[181]

Not only did ICANN have financial challenges, it also faced resistance from those in the internet industry. Commerce Secretary Daley probably thought he would never see the day when Network Solutions, Inc. (NSI) and ICANN would agree to anything. As the incumbent sole-source contractor with the National

---

174. *Id.*
175. *Id.*
176. Jennifer Mack, *Nader Proposes Limits to ICANN*, (visited Feb. 15, 2000) <http://www.zdnet.com/zdnn/stories/news/0,4586,2342438,00.html>.
177. *Id.*
178. A. Michael Froomkin, *A Contract with the Internet* (visited Feb. 16, 2000) <http://personal.law.miami.edu/~froomkin/contract.htm>.
179. *Id.*
180. Elizabeth Clampett, *ICANN Gets Financial Boost* (Aug. 20, 1999) <http://www.internetnews.com/bus-news/article/0,2171,3_186621,00.html>.
181. *Id.*

Science Foundation, NSI was reluctant to turn over its keys to the engine of the Internet, the authoritative root servers. But Secretary Daley did not give up hope. He proclaimed September 29, 1999, "a landmark day for the Internet."[182] This was the day NSI and ICANN entered into an agreement. As part of the deal, NSI had to recognize ICANN's authority over the shared domain name registry, provide equal access to the shared registry, allow ICANN to charge registration fees, maintain the Whois database, and keep the authoritative root servers physically located at NSI. NSI is now competing against other ICANN-accredited registrars for the same business.

There are many that are sticking by ICANN in spite of its reputation. Zoe Baird, President of the Markle Foundation, announced at ICANN's board meeting in October 1999, a commitment to spend $100 million building public awareness of policies in the digital age that impact free speech, free competition, and the ideals of democratic representation.[183] At least half of the money will be earmarked for ICANN's use. Some of the money will be given to the Carter Center, founded by former President Jimmy Carter, to help create a mechanism to oversee an international election of Internet users and to make sure the process is open and fraud-free. Acknowledging ICANN's lack of financial resources and range of voices, Baird said, "Management of the Internet by a private entity will not be stable or legitimate if that entity does not adequately include the public voice."[184] The initiative will involve other entities such as Common Cause, the American Library Association, the Center for Democracy and Technology, and the Harvard Law School Berkman Center for Internet and Society. Common Cause will be advising ICANN on building an international democratic voting process. The library group will be setting up "virtual voting booths" around the world. And the Center for Democracy and Technology will produce public awareness brochures.

ICANN will have to deal with a growing list of diverse partners. And many partners, for the first time, will experience the shock of being involved in a unique experiment in international governance that relies upon consensus instead of special interests. The Bellheads and the Netheads are no longer the only ones vying for a dominant position at the steering wheel of the new e-conomy. The International Trademark Association (INTA) is another important player in the mix.

In her testimony before the House Judiciary Subcommittee, Anne Chasser, President of INTA, complained that trademark protection was being relegated to the backburner. She went on to explain her position stating,

---

182. Randy Barrett, *NSI, ICANN Smoke Peace Pipe,* INTERACTIVE WEEK, (visited Feb. 15, 2000) <http://www.zdnet.com/intweek/stories/news/0,4164,234121,00.html>.

183. Jerry Clausing, *Foundation Gives $1 Million for Public Internet Efforts* (visited Feb. 15, 2000) <http://www.nytimes.com/library/tech/99/11/cyber/articles/03icann.html>.

184. *Id.*

> Trademarks have been an integral part of the growth of e-commerce. With the World Wide Web becoming ever so tangled, consumers, researchers, and typical Net surfers need some type of assurance that they have reached their intended destination in cyberspace. That assurance, that sign, is a trademark. From a purely technical perspective it may be the root servers and protocols that make the Internet work, but it is brand awareness . . . that has made the Internet a part of so many lives and the dispensable tool that it is today.[185]

One of Chasser's main objectives at the hearing was to forward the cause of trademark representation. She states, "[T]he trademark community must have a significant voice in domain name policy. Otherwise, a governing body weighted heavily toward the Internet technical community or registries/registrars may not fully understand or appreciate the relevance of trademark concerns to business and consumers."[186] This statement hints at culture clash and points to the need for more sensitivity and balance in the ICANN transition process. Recognizing that the technical community tends to lean toward technical agendas, Chasser crafted a well-designed list of objectives for safeguarding trademark rights in cyberspace.[187]

First, accountability starts with identity. Today, domain names may be obtained and used without verification of identifying information. The domain name registration process should require a minimum set of identifying information about domain name holders.

Second, each registry should use a centralized publicly-accessible database. The ownership of the Whois database at NSI has been an issue in the past. The database needs to be a public rather than private resource. A centralized database would avoid problems that result from registrars who may compromise on hardware maintenance and restoration services. A good start in this direction has been taken by ICANN, which has contracted with the trademark research firm Thomson & Thomson to record domain name registrations from all ICANN accredited registrars.[188] With the accelerating growth of the Internet, this information has become invaluable to organizations seeking to research or protect a trademark.

Third, a single dispute resolution policy should be consistent across all gTLD space. A global marketplace and community requires a single set of global rules. Initially, dispute resolution policy was to be limited to instances of bad faith. Now the rules will also apply to domain name disputes. Since this process bypasses the traditional court system, nothing should keep a party from using the national court systems for fact-intensive trademark infringement disputes. Then

---

185. *See supra* note 3 (testimony of Anne Chasser, President International Trademark Association, Internet Domain Names and Intellectual Property Rights). The testimony can also be found at <http://www.house.gov/judiciary/chas0728.htm>. The International Trademark Association is an organization of leading trademark owners, with 3500 members in over 120 countries.

186. *Id.*

187. *Id.*

188. *Thomson & Thomson Launches Data Quality Initiative,* INFORMATION TODAY (January 2000) <http://www.infotoday.com/it/jan00/news3.htm>.

all registrants will have to abide by a uniform universal policy or choose not to exist in cyberspace.[189]

Fourth, some type of clearing mechanism should be applied to marks which would be deemed "famous" or "well-known."[190] The solution should protect both domain name holders and trademark owners equally.

Fifth, the "go-slow" approach should be adopted with regard to adding new gTLDs. If it is deemed necessary, additions should be made one-at-a-time and with the precondition that all of the other objectives have been met. Chasser points out that many of these issues were discussed among WIPO and ICANN and within the INTA.

WIPO has also been invited to participate in the transition process at the highest levels. In defining its general framework for recommending courses of action, WIPO established three criteria: (1) the recommendation must be technology neutral; (2) it must respect the current strengths of the DNS; (3) it must not suggest regulatory activity on the Internet unless regulation would promote well-established national and international public policies.[191]

On April 30, 1999, the WIPO Report was published fulfilling its obligations as specified in the White Paper mandate. The Report only dealt with the most urgent and obvious problems.[192]

At the top of the list was "a significant problem" between the privately-administered globally-accessible domain name system and the publicly-administered territorial-based intellectual property rights system.[193] The practice of cybersquatting was universally condemned. It was recommended that "a simple, quick and uniform administrative dispute resolution procedure be introduced in the gTLDs to deal with complaints of the deliberate, bad faith registration and use of domain names in abuse of trademark rights."[194] Domain name applicants would be required to agree, in the registration agreement, to submit to the procedure. If one chose to disagree with the registration agreement, the domain name would not be granted.[195]

The WIPO Report listed the unreliability of contact details of domain name registrants as a "major impediment" to intellectual property owners in defending their rights against abusive registrations.[196] Several methods of deterrence were recommended. It was decided that domain name applicants must provide "representations" that the information they supply them is true and accurate.[197] The basis for the cancellation of an agreement would be the supplying of inaccurate and unreliable information, as well as the failure to update domain name contact

189. Courtney Macavinta, *Domain Policy Aims To Keep Fights Out Of Courts*, CNET NEWS (October 4, 1999) <http://news.cnet.com/news/0-1005-200-805704.html>.

190. These types of marks are usually the most inviting to domain name pirates and cybersquatters.

191. *See infra* note 192.

192. World Intellectual Property Organization, Final Report of the WIPO Internet Domain Name Process (visited April 4, 200) <http://ecommerce.wipo.int/domains/process/eng/final_report.html>.

193. *Id.*

194. *Id.*

195. *Id.*

196. *Id.*

197. *Id.*

information. If the contact information is so unreliable that notification of the registrant is not possible, the registrar would have the authority to "take down" the domain name or cancel the registration.[198] In summary, a take down model would be used to ensure the availability of reliable and accurate contact details as a "fundamental" requirement.[199]

Implementing the WIPO recommendations would serve the interests of a number of trademark and public copyright protection policies. And it would also prevent fraud and dishonest commercial practices to some degree. But what would happen to the protection of free political speech or free religious expression? WIPO has suggested "exploring" the possibility of expanding the gTLDs in the future to segregate commercial use from non-commercial use.[200] If one wanted to establish a political parody site, it would fall within the use-restricted area designated for non-commercial speech.

The WIPO Report also recommended applying uniformity to all pronouncements on dispute resolution policy in the gTLDs.[201] If registrants knew there were more lenient registration policies in another location, these locations would become a haven for those who intend to register in bad faith. Uniformity would prevent varying degrees of respect for intellectual property in different geographic areas. There would be no forum shopping. One problem with this policy is the potential for a decision between two parties to be tied to a particular court's jurisdiction when a dispute panel cannot resolve the issues satisfactorily. In many cases, the registrar's domicile would determine jurisdiction. Since there are more registrars in the U.S., the odds favor U.S. netizens.

Another of ICANN's partners is the Global Internet Project (GIP).[202] GIP is an international group of thirteen leading Internet executives committed to the growth of the Internet worldwide. They are working to ensure a transparent, participatory process at ICANN for the purpose of creating universal standards, including policies that will ensure the convergence of the telephone, television, and the Internet without restrictive government intervention. With the help of partners like the INTA, WIPO, and GIP, ICANN's experiment in privatized international governance is sounding better all the time.

VIII. THE SAFE HARBOR MODEL

It has been said there are two things in life that are certain. And at least one of these things is headed straight to a nearby browser. Yes, the Internet has become such a lucrative venture that the world's governments are rubbing their hands and salivating in anticipation of taxing their piece of the Internet pie. The United States has been against Internet taxation from the beginning. But it is becoming increasingly difficult to keep everyone's hands out of the proverbial cookie jar.

198. *Id.*
199. *Id.*
200. *See supra* note 192.
201. *Id.*
202. *ICANN Endorsed by GIP* (Sept. 16, 1999) (ITAA, Sheila O'Neill, +1 703/284-5329) <soneill@itaa.org, http://www.gip.org/> .

European nations have been among the most vocal and antagonistic towards an untaxed Internet. During the final phases of WorldCom's $40 billion acquisition of MCI, the Europeans held up the deal. I remember a meeting in Jackson, Mississippi. There were about forty people crammed into a room to discuss the current status of the merger. It had passed U.S. regulatory hurdles to qualify as the largest corporate merger in America, but there was an unexpected bump in the road. It was revealed that the fate of the merger was in the hands of the Europeans. WorldCom and MCI would not know anything definitive until the Europeans decided what could be done to satisfy their markets. I remember thinking that seemed a little odd. Here were two American companies sitting around waiting for the Europeans to say they could or could not move forward. Finally, in September 1998, the acquisition was approved. But the mega-merger was conditioned upon complying with a European directive. MCI had to sell its Internet backbone business before the European Commission would bless the deal. The business was sold to Cable & Wireless PLC and WorldCom took on its new e-dentity—MCI WorldCom.[203]

European intervention and involvement in the shaping of MCI WorldCom's e-dentity was just the beginning of a more intrusive campaign to ensure Europe's share of control over the future of e-commerce. On October 25, 1998, while expressing concern for the privacy rights of its citizens, the EU announced a new Directive on Data Privacy.[204] The announcement threw a big wrench into the transatlantic economic partnership and sent shock waves throughout the U.S. business community. The directive seemed to catch many by surprise. It was presented as an internal EU policy that would ensure the free flow of data between the fifteen EU member states. Besides giving individuals the right to review, correct, and limit the use of their personal information online, the directive also required member states to block the transmission of data to the United States in cases where privacy protections were found to be inadequate. Ironically, the policy designed to improve the free flow of information within the EU threatened the flow of data to the United States.

In April 1999, the U.S. Department of Commerce developed documents to help U.S. companies comply with EU directives and avoid data flow disruptions, known as "safe harbors."[205] The documents also specified how U.S. telecommunications, financial services, and cable industries could comply.

The concept was simple. Europe wanted better privacy protection for its citizens. So it made a decision to legislate an internal solution. And whether intentional or not, the policy was seen as a shot across the bow of mother ship e-America. Apparently, the message of an industry-led self-regulation model for ensuring consumer confidence didn't sell well in the EU camp. The incident certainly raised suspicions and shed new light on the transatlantic partnership. The

---

203. *See supra* note 159.

204. *The European Union Directive on Data Privacy and Its Impact on Global Information Systems in US Corporations* (visited February 13, 2000) <http://www.hunter-group.com/thg/ART/white_data.htm>.

205. *See* John B. Reynolds and John F. Papandrea, *Department of Commerce Publishes New EU Privacy Directive "Safe Harbors" Principles*, WILEY, REIN & FIELDING (May 1999) <http://www.wrf.com/publications/cyberspace/view_update.html>.

Europeans were beginning to act like protectionists and were willing to risk isolating themselves from U.S. trade interests in order to lock down safe harbor practices on the Internet. But by doing so, the Europeans were also making a deliberate choice to counter U.S.-preferred economic and security interests.

The new policy resulted in the creation of a unique EU-regulated commercial zone through which all transatlantic data would flow. Even though the fifteen EU member states would be bound by a U.S./European Commission understanding, only the European Commission acting with a committee of member state representatives would be able to interrupt personal data flows from an EU country to a U.S. organization. As overseers of the terms and conditions upon which all Internet traffic is subject, the EU would now be in a position to dictate terms to the United States and others who agreed to abide by the safe harbor rules. The closest thing the United States has to this kind of virtual headlock on e-commerce is the Internet root servers.

For the moment, participation by U.S. organizations in the safe harbor program is considered voluntary. But one should be wary of an initial strategy that relies upon voluntariness coupled with an attempt to overlay EU law by extension. In a sense, the strategy can be equated to falling hook, line, and sinker for an excellent introductory rate on a credit card. After much volunteer use, dependencies form and the costs go up shortly thereafter. Safe harbor is intended to affect only those organizations that receive personal data from the EU. This limitation means that safe harbor will "only" control the single most highly interdependent commercial relationship between the two largest economic trading partners in the world. It will touch close to $326 billion in trade and will affect the e-dentities of every consumer who lives and works in the EU or the United States.

By pledging to inform individuals about the online collection of their personal information, businesses will also be committing to procure the necessary systems and processes to make it happen. This commitment will require a significant investment of time and human resources, the likes of which many companies would be unwilling to make. The United States had hoped to convince the EU of the error of its ways by reaching an agreement at the June 1999 EU-U.S. Summit in Bonn, Germany, but no agreement materialized.[206]

The Europeans have watched U.S. businesses hang onto the idea of self-regulation for all of the wrong reasons. While agreeing in principle to self-regulate, many businesses have failed to self-regulate in practice. Knowing a consumer's buying habits offers a competitive advantage in the market.[207] In this sense, the idea of operating in a safe harbor is at odds with the economic interests of most businesses. But public outcry about electronic profiling and the collection and misuse of personal information has reached a fever pitch in the United States. Meanwhile, the Europeans are growing weary as the United States conducts

206. Robert MacMillian, *Privacy Talks Didn't Surface at EU Summit*, NEWSBYTES (June 25, 1999).

207. Ted Bridis, *Government gives Internet until year's end on privacy rules* (visited Feb. 14, 2000) <http://detnews.com/1998/cyberia/9807/213/07230060.htm>.

study after study, only to reconfirm that the self-regulation model is best for protecting consumer rights in cyberspace.

In July 1999, Federal Trade Commission Chairman Robert Pitofsky testified before Congress on the status of consumers' online privacy protection.[208] A report entitled *Self-Regulation and Privacy Online* was presented to the Subcommittee on Telecommunications, Trade, and Consumer Protection of the House Commerce Committee.[209] Reading from the report, Pitofsky stated, "[T]he Commission believes that legislation to address online privacy is not appropriate at this time."[210] Pitofsky pointed out that his recommendation was confirmed by two studies done by Georgetown University Professor Mary Culnan, the Online Privacy Alliance, TRUSTe, BBBOnline, and others.[211] The self-regulation model, as opposed to legislative action, was declared the most efficient and least intrusive means for protecting the privacy rights of online users.

Not everyone at the hearing shared the same level of confidence in this conclusion. Referring to business' track record with the self-regulation model, FTC Commissioner Mozelle W. Thompson painted a gloomier picture. He stated, "I believe that we will not progress further . . . Congress and the Administration should not foreclose the possibility of legislative and regulatory action . . . ."[212] One can almost hear a conservative hint of dissension in Commissioner Thompson's statements. Commissioner Sheila F. Anthony was clearer, stating, "I believe that the time may be right for federal legislation to establish at least baseline minimum standards. I am concerned that the absence of effective privacy protections will undermine consumer confidence and hinder the advancement of electronic commerce and trade."[213]

One cannot help but see the differences of opinion expressed by Chairman Pitofsky and his commissioners. Commissioner Anthony's statements even contradict the findings of the report. It is as though Chairman Pitofsky, obligated to give a politically correct answer, left it up to his commissioners to reveal the need for guarded skepticism in light of Europe's growing protectionism.

In September 1999, Commerce Secretary Daley was blindsided by another unilateral European action.[214] What made this event so disturbing was that the United States and the EU had agreed in June of the same year on early warning

---

208. *"Self-Regulation and Privacy Online"*, FTC News Release (July 13, 1999) <http://www.ftc.gov/opa/1999/9907/report1999.htm>.

209. *"Self-Regulation and Privacy Online" before the Subcommittee on Communications of the Committee on Commerce, Science, and Transporation* (July 27, 1999) 106th Cong. (prepared statement of the Federal Trade Commission). Copies of the report are available at <http://www.ftc.gov>. Information can also be obtained from the FTC's Consumer Response Center, Room 130, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580; 202-FTC-HELP (202-382-4357); TDD for the hearing impaired 202-326-2502. To find out the latest news as it is announced, call the FTC NewsPhone recording at 202-326-2710.

210. *Id.*

211. *Id.*

212. *Id.*

213. *Id.*

214. *US: EU law could chill e-commerce*, REUTERS (September 15, 1999) (from ZDNet) <http://zdnet.co.uk/news/1999/36/ns-9992.html>.

mechanisms to prevent this type of surprise, and to identify and solve bilateral trade problems before they could become full-blown disputes. The EU began considering a draft law that would allow disgruntled Internet shoppers to sue foreign companies in the shoppers' own national courts. The law states that if an offending company's web site can be seen in the EU, it could find itself facing lawsuits in any one of the EU member countries.[215] Daley called the law "chilling" and pointed out, "There is . . . a serious question of whose laws prevail."[216] Speaking at WIPO, Secretary Daley's comments concerning the draft law sounded as if he had come to expect this type of action from the EU. He characterized the relationship by saying, "[D]ispute . . . is positive to our economies."[217]

Testifying before Congress on the role of standards in the growth of global electronic commerce, Andrew Pincus, General Counsel of the Commerce Department, stated, "Many of the most important nations and regions of the world articulate a view of global electronic commerce that has government intervening more aggressively in setting standards."[218] He went on to acknowledge that the United States and Europe could provide a model of regulatory harmonization for the entire world, but not without exercising "unselfish economic leadership."[219] Pincus' vision for harmony includes a small caveat: "The U.S. Government is determined to prevent other governments from using the standardization process to impose technical barriers to trade or to interfere with the web as a global enterprise."[220]

As the WTO meetings in Seattle drew closer, Europe's position on Internet taxation became evident. Trade relations between Europe and the United States became increasingly regulatory.[221] An important issue was the expiration of a WTO Internet tax moratorium, a concern that acted as a catalyst to raise the level of intensity and to disgruntle the international politicians as they descended upon the city of Seattle. Most countries wanted the Internet tax moratorium extended. But Europe began playing hard ball.[222]

Michel Servoz explained the official EU stance by placing a condition on extending the moratorium. He stated, "The moratorium is intrinsically linked with the question of classification."[223] Europe wants e-commerce to be classified as services. The United States prefers to categorize e-commerce as goods. There are varying degrees of control tied to each classification. WTO rules for services

---

215. *Id.*
216. *Id.*
217. *Id.*
218. *Role of Standards in Growth of the Global Electronic Commerce: Before the Department of Commerce Committee on Commerce, Science and Technology Subcommittee on Science, Technology, and Space,* 106th Cong. (Oct. 28, 1999) (testimony of Andrew Pincus, General Counsel of the U.S. Department of Commerce).
219. *Id.*
220. *Id.*
221. David Aaron, *Friction in EU, U.S. Trade Relations Increasingly Regulatory,* Remarks at the Conference on Transatlantic Regulatory Harmonization and Global Standards, George Washington University Washington, D.C. (Oct. 8, 1999). (Mr. Aaron is the Ambassador Undersecretary of Commerce for International Trade).
222. David McGuire, *EU-US Sparring Could KO Net Tariff Moratorium,* NEWSBYTES (Nov. 29, 1999).
223. *Id.*

are stricter than its rules for goods. And member countries have greater control over goods than they do over services. So by linking the classification issue to the extension of the e-commerce moratorium, the EU has successfully stifled much of the progress on the matter. Erika Mann, a European Parliamentarian, suggested the EU might agree to a short-term extension of the moratorium on the condition that the United States would agree to resolve the classification issue.[224]

The talks ended with the EU proposing regulation of the Internet worldwide through international agreements and organizations, such as the Organization for Economic Cooperation and Development (OECD) and WIPO, and through self-regulatory mechanisms such as the Global Business Dialogue on Electronic Commerce (GBDe).[225] The United States agreed to continue working, as part of the New Transatlantic Agenda (NTA),[226] on consolidating the WTO, working on new international rules for intellectual property rights, and ensuring interconnectivity and interoperability in information systems.[227]

Since July 1997, Europe's intentions have been to "work towards global consensus through active involvement in current international cooperation and negotiations, within WTO and OECD to establish a stable, rule-based environment for electronic commerce as soon as possible."[228] Since that time, there seems to be willingness on the part of the Europeans to take steps outside of the normal parameters. Safe harbors are good examples of EU directives that extend the reach of EU law into the world of cyberspace and all over the globe. With the e-dentities of so many at stake, the world's new e-conomy may soon face one of two realities in the very near future. My guess is that e-commerce will not see death, but it will see taxes sooner than we think.

IX. UNIVERSAL SERVICE AND THE DIGITAL DIVIDE

The National Telecommunications and Information Administration issued a report in July 1999 entitled *Falling Through the Net: Defining the Digital Divide.*[229] The report found a growing gap between those with access to computers and the Internet and those without. The prospect that some will be left behind in the information age can have serious repercussions on U.S. society. The digital divide threatens to impair the health of communities, impede the

224. *Id.*

225. *Id.*

226. NTA was started in Madrid, Spain in December 1995. It calls on businesses to play an "enhanced role" and to provide critical input through a forum known as the Transatlantic Business Dialogue (TABD). The TABD was started in Seville, Spain in 1995. Some say it was created by the Clinton Administration to deal with common regulatory problems. It is made up of corporate heads from both sides of the Atlantic, who come together to make recommendations to senior U.S. and EU officials. TABD has been unusually effective on the U.S.-EU Mutual Recognition Agreement, encryption, and data privacy. It was designed as a way to discuss ways for the United States to iron out regulatory differences and find common ground on e-commerce with the Europeans through reducing trade and investment barriers that may pose a threat to the Transatlantic Economic Partnership (TEP), which is a high level, heads of government mechanism committed to resolving problems and finding areas of common interests on technical standards and regulatory processes by tackling economic issues systematically, minimizing the impact of disputes and opening up trade.

227. *See supra* note 222.

228. *Global Information Networks Ministerial Conference*, Bonn, Germany, July 6-8, 1997.

229. *Falling Through the Net: Defining the Digital Divide* (visited Feb. 15, 2000) <http://www.ntia.doc.gov/ntiahome/fttn99/contents.html>.

development of a skilled workforce, and compromise the economic welfare of the nation. The relevance of this issue is getting more and more attention.

FCC Chairman William Kennard has made it a personal priority to bring new technologies like the World Wide Web to some of the country's poorest communities.[230] His efforts are motivated by the fact that sixty percent of American jobs now require the use of computers.[231] Those who live in rural areas are at risk if they too are not exposed to the technology that is helping millions become more competitive and informed in the workplace. Kennard's wish is to see that every American has equal access to technology regardless of socio-economic status. He expressed his fear by saying, "We can't afford to have in this country a digital Dark Ages where some people are just cut off from all this technology."[232]

The President shares the same view. In his Year 2000 State of the Union Address, President Clinton called for the promotion of policies to help bridge the country's digital divide.[233] Singling out the Mississippi Delta as one area where "our nation's prosperity hasn't yet reached," he announced a new $100,000,000 New Markets initiative to promote economic development.[234] He emphasized the need to connect "all" Americans to the Internet, leaving no one behind.[235]

The Telecommunications Act of 1996[236] was one of the first significant steps taken by Congress and the FCC to help close the gap between the "haves" and the "have nots." As part of this effort, low-income areas were targeted to receive support for basic phone service. E-rate funds were also set aside to offset the cost of Internet access in schools and libraries.

But low-income subsidy funds have gone up every year, while the number of people assisted has remained relatively flat.[237] In some cases, political problems have gotten in the way of the money. Jeff Chester, executive director of the Center for Media Education, said, "[t]he [Federal Communications Commission] has not done enough urging the states to take advantage of this funding. We need to focus on this problem. If we're ever going to have an equitable society, we have to ensure that the folks on the bottom get in right away."[238] In Mississippi, Senator Willie Simmons has alleged that the funding has gotten caught up in partisan battles between legislators and the governor.[239] As a result, Senator Simmons intends to tap into the state's tobacco settlement coffers as a funding source for the poor.[240]

---

230. Sharon Collins, *FCC Chairman Kennard on High-Tech Crusade* (visited February 15, 2000) <http://cnn.com/1999/TECH/computing/12/07/fcc.chief.profile/index.html>.
231. *Id.*
232. *Id.*
233. President Clinton, *State of the Union Address* (Jan. 27, 2000) <http://www.whitehouse.gov/WH/SOTU00/sotu-text.html>.
234. *Id.*
235. *Id.*
236. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996).
237. John Borland, *States slow to grab subsidies for telecom service* (visited February 15, 2000) <http://dailynews.yahoo.com/h/cn/19991021/tc/19991021006.html>.
238. *Id.*
239. *Id.*
240. *Id.*

Since most agree that universal Internet access and e-commerce will bring "enormous potential for growth anywhere,"[241] one might ask who should be driving the process. With big business driving the process, people would be susceptible to the effects of self-regulation and market "spin." In a safe harbor model, personal data could be filtered and stopped at the transatlantic border. If government is to move the process forward, it should be willing to provide access for all people. In this scenario, it would be impossible to maintain the balance that spurs on competition while guaranteeing the rights of access to the underprivileged.

These facts may be the reason the process has ended up being driven by the United Nations World Intellectual Property Organization. WIPO is working closely with ICANN to make universal service a reality. Bringing competition into management of domain name space was a high priority. Congress is also working to coordinate American law with WIPO recommendations. TABD is bringing business and government together to promote best practices. And ISPs are finding many of their policies driven by WIPO.

Speaking of the unique international challenge to help privatize control of DNS, WIPO's Legal Counsel Frank Gurry acknowledged, "[I]t is an unusual process for WIPO insofar as it is a process that is carried out direct with the private sector or the interested parties, and not direct with our Member States . . . ."[242] Gurry also said,

> So, in some respects we see this process as something of a prototype, or with the potential of being a prototype for the sort of questions that are increasingly going to arise as a result of the intersection of the real world and the institutions that have been developed on the basis of the past experience of the real world and what is rapidly becoming the very intensely active space of cyber-space.[243]

In 1997, Bruce Lehman, U.S. Commissioner of Patents and Trademarks, began recommending WIPO as the vehicle for establishing a global patent office to take advantage of technical advances and to allow multiple filings of patent applications through a single filing.[244] Just as with trademarks, inventors are required to file patent applications in every country of the world. A single global database would streamline the process for filing applications. But by merging these global issues under WIPO, new "supranational" procedures for registering intellectual property would be governed by a relatively unknown system called the "Madrid System of International Registration of Marks." The Madrid Protocol is a treaty, largely adopted in Europe, that seeks to streamline the

241. President Clinton, Remarks at World Economic Forum in Davos, Switzerland (Jan. 29, 2000). The text of the President's remarks can be found at <http://www2.whitehouse.gov/WH/SOTU00/Sotu-text.html>.

242. World Intellectual Property Organization consultation meeting at Georgetown University, Washington, D.C. (October 1, 1998) <http://wipo2.wipo.int/process/eng/dc-transcript1.html>.

243. *Id.*

244. John Gehl and Suzanne Douglas, *Lehman Calls For Global Patent Protection*, BNA DAILY REPORT FOR EXECUTIVES (Feb. 4, 1997).

process of registering trademarks for protection in member countries. It enables trademark owners to obtain registration of their trademarks, based on the filing of a single application, versus one application per country.

The Madrid Protocol has been designed to handle many of the issues inherent in patent, domain name, and trademark systems, as well as the dynamics for future registrations that include graphics. One perceived problem with the current system of domain names is that there is no universal directory service that would allow a user to determine the domain name of a trademark holder. To resolve this problem, WIPO calls for a trademark directory in the context of Internet domain names that would relate a trademark to the Internet home page of the trademark owner. Such a directory would be searchable by trademark and would include information on the owner of the trademark and the countries in which the trademark is registered. It could also include any special typeface, graphical design, or other representation associated with the trademark.

The Madrid Protocol would include the use of a central directory. But at this point its implementation would be "supranational" and euro-centric. Unlike in the safe harbor regime, businesses may not volunteer to become members of the Madrid Protocol. The U.S. Congress will have to determine American participation.

The United States will have to become a member to the protocol, but many questions are yet to be answered about what happens to individual rights in this scenario. Protection could be watered down under an international community consensus that is not based on United States law.

Realizing that the application of the Madrid Protocol could be unfair for American interests, I submitted the following comments to the Department of Commerce during their call for public comments in January 1998:

> I am concerned that the European Union (EU) will have an unfair advantage over the United States as the TLDs and international trademark laws are merged. As the world's economies become more and more dependent upon the proper functioning of the Internet's TLDs, the synergies of a united Europe and WIPO's enforcement of 'the Madrid Protocol' would put US companies and US-based Internet users at a clear disadvantage.[245]

As privatization of the domain name system ran aground, I became convinced that the United States would inevitably succumb to the pressure of WIPO and adopt the Madrid Protocol. In July 1998, I made a personal bet with the Father of the Internet that WIPO, the Madrid Protocol, and Europe would end up running the whole show. It was a hunch that intrigued Mr. Cerf. He ended up e-mailing me for more information about the Madrid Protocol.

In March 1999, I wrote the office of those who were instrumental in establishing WIPO's "Notice and Take Down" model, known in the United States as the

---

245. *See* <http://www.ntia.doc.gov/ntiahome/domainname/130dftmail/01_30_98.htm>.

Digital Millennium Act of 1998.[246] Their answer to one of my concerns was, "We had never considered the possible DNS implications with respect to this treaty and your note prompted us to do some research on the subject." As the e-mails continued back and forth, it became apparent that the economics of the treaty would far outweigh any possible technical difficulties that might result.

The cultural differences between those crafting policy and those working in the real world of managing networks on a day-to-day basis are pronounced. I contacted the person in charge of answering the technical questions about how the Madrid Protocol would affect DNS. When I asked how it would affect network managers in the United States who are using directory-enabled networking (LDAP) to dictate authentication policies on their local area networks, no answer could be given. When I asked further about using user-to-address mapping services, such as those provided by CheckPoint Software, there was no answer. The reality is that the Madrid Protocol, if adopted, could potentially have an effect on every network in the United States and the daily operations that support them.

If the public remains silent, big business will continue to push Congress for U.S. adoption of the Madrid Protocol. In fact, the Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks (Protocol) or Madrid Protocol Implementation Act is pending action in the Senate.[247] It intends to amend the U.S. Trademark Act of 1946.[248] Senator Patrick Leahy introduced the bill, stating, "[T]his legislation will conform American trademark application procedures to the terms of the Protocol in anticipation of the U.S.' eventual ratification of the treaty, thereby helping American businesses to create a 'one stop' international trademark registration process."[249]

If this ratification happens, the little guys will have to go about reconfiguring their networks after the fact. There is a legitimate need to find a solution for combining the registration processes of trademarks and domain names under a globally unique registry. But going along with the rest of the world, even if it can be cost-justified, may not be the most honorable thing to do. If the international approach to the development of a legal framework for cyberspace is not based on protecting individuals, it will be based on protecting the economic interests of the "system" itself.

---

246. Pub. L. No. 105-304 (1998). The "Take Down" model focuses on ISPs controlling or "legislating" web content. Web content is not considered freedom of speech by some. The same model limits the liabilities of ISPs.

247. S. 671, 106th Cong. (1999) (this bill did not pass Congress); S. 2191, 106th Cong. (2000) (this bill is pending).

248. 15 U.S.C. § 1051 *et seq.* (1994) (also known as the Lanham Trademark Act).

249. 145 Cong. Rec. S 8,252-01 (July 12, 1994).