https://doi.org/10.48009/2_iis_2007_70-75

# Internet Legal Rulings: Movement Toward A Consistent Global Legal E-Commerce Environment

**Dr. Karen Lynne-Daniels Ivy, karen.l.ivy@lmco.com**


## ABSTRACT

*The Internet has rapidly become an influential social, economic, and political force of the modern world. As the Internet and Internet legal issues have grown and developed, so too have the laws surrounding it. Countries have different approaches to Internet regulation. Most countries of the world regulate the Internet within the framework of their political, legal, moral and cultural values. Continued implementation of agreements between countries actively trading in electronic commerce is required to move toward a consistent global legal e-commerce environment. Agreements amongst all e-commerce trading countries would lead the way to a consistent global legal environment.*


**Keywords:** Internet Legal Rulings, E-Commerce Law, Global Legal E-Commerce

## INTRODUCTION

In the early days of the Internet, adhering to law was rarely addressed. The Internet community was self-regulated, supplemented by contractual agreements among owners and operators of the communications and computing infrastructure (Bagby, 2003). All of the advancements and benefits of the new Internet brought the commonly accepted notion that no one is in charge. The Wild Wild West metaphor was applied to the Internet with cyberspace depicted as a lawless frontier where anarchy and vigilantism are alive and well (Biegel, 2001). A close look at the Internet over the past ten years reveals a changing cyberworld that is, at least in part, under a significant degree of control. Today there are several E-Business regulations and legal rulings that provide "control" in the widely growing cyberworld. Legal principles governing conduct and commerce in cyberspace are still evolving (Tysver, 2000). Continued implementation of agreements between countries actively trading in electronic commerce is required to move toward a consistent global legal e-commerce environment. Agreements amongst all e-commerce trading countries would lead the way to a consistent global legal environment.

## FIVE-PART TYPOLOGY OF INTERNET REGULATIONS

After surveying patterns of Internet law and policy around the world, Eko (2001) identified a five-part typology of Internet regulation based on the multiple political, cultural, social and economic contexts, and realities around the world. This five-point typology of Internet regulation describes the differential regulation of the Internet by countries, international organizations and regional economic, cultural and political groupings. The five part Internet regulation typology consists of: 1) Internationalist, 2) Neo-Merchantilist, 3) Culturist, 4) Gateway, and 5) Developmentalist. The United States has advocated an Internet regulatory regime based on self-regulation. Since the largest proportion of Internet activity takes place in the United States, Congress and the Supreme Court are increasingly seen as the defacto regulators of the Internet for the rest of the world. The U.S. self-regulation model is rooted in the political economic and cultural realities of the United States. This includes the First Amendment guarantee of freedom of speech and of the press. Though this principle has also been endorsed by some international agencies and non-governmental organizations, many are in agreement that Internet self-regulation is neither desirable nor universally applicable (Eko, 2001). Many agree that most countries of the world still regulate the Internet within the framework of their political, legal, moral and cultural values. The result is a wide range of Internet regulation and policy that is described by Eko in terms of a five-part typology based on international, regional and national, political, economic, and cultural, moral, and social realities.

<Insert Table 1 Here>

## PROBLEMATIC INTERNET-RELATED CONDUCT

Each Internet business and individual user should understand how Internet law affects them, and understand the problematic areas of Internet-related conduct. Agreement regarding just what is harmful in cyberspace is an essential first step in the regulatory process. Strategies for addressing problems that are harmful in the Internet environment

will depend on the ability to reach a consensus on the level of harm that is wished to be prevented. There are many ways to sort out allegedly problematic Internet-related conduct. One common approach is to separate the problems out by traditional areas of the law such as contracts, tort, civil procedures, etc. A second common approach is to discuss problematic conduct under recognized sub-categories of "cyberlaw", such as freedom of expression, intellectual property, and privacy.

Biegel (2001) suggested a viable approach that divides current Internet regulation problem areas into four categories: 1) dangerous conduct, 2) fraudulent conduct, 3) unlawful anarchic conduct, and 4) inappropriate conduct. Under this framework, a roadmap for prospective Internet regulation can be identified based on representative characteristics that would be established for each broad category. The dangerous conduct category is composed of acts and behaviors that may impact physical or national safety. Such conduct includes threatening behavior, creating and trafficking in child pornography, unlicensed online health care, and certain types of hacking activity that may be considered "cyberterrorism" or "acts of cyber war" (Biegel, 2001). Threatening behavior can be loosely defined as any activity that, if unchecked, may lead to physical injury. This category would include threats communicated via email or the World Wide Web, as well as activity that some have labeled "cyberstalking". The second category of problematic acts in the online world -- fraudulent conduct -- is comprised of behavior that may impact the economic safety of person, businesses, institutions, and governments. Fraudulent actions in this category, referring to a wide-range of generally dishonest activity and conduct, might include hacking that poses the threat of financial loss, deceitful business practices including privacy invasions, and online fraud in general. The third category, unlawful anarchic conduct, includes problems that are typically viewed as the direct result of an inconsistent, overbearing, or anachronistic legal system. The areas of conduct that fit under this category include digital copying, pornographic expression, and online defamation. Behavior in this category is not generally fraudulent or dishonest, there is no danger to physical safety or national security, and the potential impact on the economic well-being of other persons and groups may not be very clear. The last category of problematic conduct in cyberspace is comprised of behavior that most would label "inappropriate". This category includes four specific types of activity: 1) discriminatory "hostile environment" harassment of individual persons, 2) extremist and hate-related websites, 3) inappropriate online activity in an education setting, and 4) offensive or overly aggressive business practices (Biegel, 2001).

## CRITICAL E-COMMERCE LEGAL ISSUES

Several Internet legal issues exist today within the four problematic Internet-related conduct categories identified by Biegel (2001). Various e-commerce legal issues have caused a focus on Internet law: 1) E-filing in courts: Electronic filing of litigation documents is allowed in some courts; 2) Evidence: Some electronic documents can be used as evidence in court; 3) Jurisdiction: Which state or country jurisdiction prevails when litigants are in different statues or countries? Who can sue for Internet postings done in other countries? ; 4) Liability: The use of multiple networks and trading partners makes the documentation of responsibility difficult. How can liability for errors, malfunctions, or fraudulent use of data be determined?; 5) Defamation ; 6) Identity fraud; 7) Computer crime; 8) Digital signature: Digital signatures are now recognized as legal in the United States and some other countries, but not in all countries; 9) Regulation of consumer databases: The United States allows compilation and selling of customer databases; 10) Encryption technology: Export of U.S. encryption technology was made legal in 1999; 11) Time and place: An electronic document signed in Japan on January 5 may have the date January 4 in Los Angeles. Which date is considered legal if disputes arise? ; 12) Location of files and data: Much of the law hinges on the physical location of files and data. With distributed and replicated databases, it is difficult to say exactly where data are stored at any given time; 13) Electronic contracts; 14) E-communications privacy: Electronic Communications Privacy Act (ECPA) protects individuals' electronic communications and stored messages against government surveillance conducted without a court order, from third parties with no legitimate access to the messages, and from the carriers of the messages, such as Internet service providers; 15) IPOs online: Websites posted with the necessary information about the securities offerings are considered a legal channel for selling stock in a corporation; 16) Antitrust; 17) Taxation: Taxation of sales transactions by states is on hold in the United States and some countries, but the issue will be revived. An additional issue is whether, and how, taxes can be collected from online gamblers' winnings; 18) Money laundering: How can money laundering be prevented when the value of the money is in the form of a smart card?; and 19) Corporate reporting: Online

corporate reports are difficult to audit because they can be changed frequently, and auditors may not have time to perform with due diligence. How should auditing of online reports be conducted? What legal value does it have? (Turban et al., 2004) Doing business electronically requires having a supportive legal environment that imposes direction in dealing with the critical e-commerce legal rulings.

## INTERNET LAW

As the Internet and Internet legal issues have grown and developed, so too have the laws surrounding it. Laws are strict legal rules governing the acts of all citizens within their jurisdictions. There are seven major parts of Internet law: 1) Copyright law, 2) Domain Names and Trademarks, 3) Patent Law, 4) Privacy, 5) Free Speech and the First Amendment, 6) Contract Law and High Technology, and 7) Employment law (Isenberg, 2002).

### Copyright Law

Copyright provides an author with a tool to protect a work from being taken, used, and exploited by others without permission. Copyright law grants several different rights to the author, creator, or owner of the work. These rights essentially define what the copyright owner can do with the copyrighted work and what rights the owner can license or assign to others. These rights are actually a bundle of exclusive rights, called statutory rights (Bagby, 2003). The owner of the copyrighted work has the exclusive right to reproduce it, prepare derivative works based upon it, distribute copies by sale or other transfer of ownership, to perform and display it publicly, and to authorize others to do so (Rosenoer, 1997). One does not need to have a registered copyright to use the copyright symbol, ©.

E-Business leaders must understand their right of ownership as well as the possible infringement directions. Online systems are vulnerable to infringement liability from at least four different sources: 1) The person creating the system may incorporate unauthorized copies of other peoples' works; 2) Those operating and maintaining the system may add unauthorized copies; 3) Subscribers may also upload infringing copies of works to a system; and 4) Infringing copies may be transmitted throughout the system (Rosenoer, 1997). Copyright infringement can be very expensive. The U.S. Copyright Act says that an infringer of copyright is liable for 1) the copyright owner's actual damages and any additional profits of the infringer, or 2) "statutory damages" in an amount ranging anywhere from $750 to $30,000 (or $150,000 if the infringement was "willful") (Isenberg, 2002).

### Domain Names and Trademarks

A domain name uniquely identifies an organization's IP address on the Internet. Consumers expect to find companies they are seeking by using a specific domain name. For this reason, most companies request a domain name identical to their actual name. "Trademarks protect words, symbols, slogans, designs, characters, packaging, sounds, smells, and colors, as well as product configurations, as used in commerce" (Rosenoer, 1997, p. 95). Primary trademark and service mark protection is found under the Lanham Act (Rosenoer, 1997). The Lanham Act defines the scope of a trademark, the process by which a federal registration can be obtained from the Patent and Trademark Office for a trademark, and penalties for trademark infringement. The full implication of the Internet on trademarks is uncertain but already emerging in several key areas. Legal issues regarding trademarks and domains include trademark infringement, trademark dilution, and cybersquatting.

### Patent Law

A U.S. patent is a contract between an inventor and the government. The high technology economy has given new significance to patent law. Software and "business methods" are protectable by patents in the United States. Patents are being granted to protect business methods primarily because of the new application of the method on the Internet. One of the most notable software copyright cases in the mid 1980's was Whelan Associates, Inc. v. Jaslow Dental Laboratory, Inc. The court ruled that "copyright protection of computer programs may extend beyond the programs' literal code to their structure, sequence, and organization" (Becker, 1986, p. 18). Today, many high technology and Internet companies have begun to use patents for legally protecting their computer software and other innovative techniques from misappropriation by others. Internet companies apply for legal patents to: 1) prevent others from making, using, or selling verbatim copies of the software, and 2) prevent others from utilizing the functionality by which the software operates.

**Privacy**

The Internet has created a whole new set of legal issues relating to privacy. The main issues center around: What type of information may a company collect about individuals online, and what may the company do with that information? Many E-commerce consumers complained that website privacy policies are difficult to understand, sometimes because they are vague and other times because they are full of legalese. Partially as a result of this complaint, the World Wide Web Consortium (W3C) developed the Platform for Privacy Preference, commonly known as P3P, a technological approach to interpreting and applying privacy policies. Any website may choose to implement P3P, but no law requires any site to do so. In 1998, the U.S. Congress passed a law that controls how website operators can collect or maintain personal information about children. Any website collecting information from children should be aware of the Children's Online Privacy Protection Act (COPPA). This law is the only Internet-specific federal privacy law in the United States.

**Free Speech and the First Amendment**

As stated by Lessig (1999), in the United States, the right to free speech means the right to be free from punishment by the government in retaliation for at least some (probably most) speech. The First Amendment provides that U.S. Congress shall make no law abridging the freedom of speech or of the press. The USA is not the only country where citizens have a right to freedom of expression. In contrast to Australia, governments in comparable countries including Canada, New Zealand, the United Kingdom and various European countries have chosen to legislate to give citizens a right in domestic law to freedom of expression similar to that contained in the International Convention on Civil and Political Rights (ICCPR). One of the greatest free-speech advantages the Internet provides is the ability to broadcast material from all over the world to all over the world.

**Contract Law and High Technology**

The growth in online communications soon led to the acceptance of electronic contracts and electronic signatures. In 1999, the National Conference of Commissioners on Uniform State Laws (NCCLUSL) approved the Uniform Electronic Transaction act (UETA) (Isenberg, 2002). The heart of UETA states that a "record or signature may not be denied legal effect or enforceability solely because it is in electronic form" (Isenberg, 2002, p. 275). June of 2000, U.S. Congress passed the Electronic Signatures in Global and National Commerce Act, known as the E-Sign Act. Similar to UETA, the purpose of the E-Sign Act is to provide legal validity to contracts entered electronically (Isenberg, 2002). Effective as of October 1, 2000, the E-Sign Act provides that "a signature, contract, or other record relating to a transaction may not be denied legal effect, validity or enforceability solely because it is in electronic form" (Isenberg, 2002, p. 275). Under the E-Sign Act, assuming a contract meets other legal requirements, the electronic signature is valid even if the parties negotiated and agreed to it via e-mail or on the Web. The E-Sign act does not apply to all transactions. It does not apply to wills; family law transactions such as adoption and divorce; notice of cancellation of utility services; cancellation of health insurance; or product recalls.

**Employment Law**

The increased use of technology has created legal challenges for employers. Several companies have implemented Internet use policies and implemented employee Internet monitoring practices. Labor and workers' rights groups such as the Communications Workers of America and the Privacy Rights Clearinghouse are increasingly concerned about this brand of electronic spying. Legally, there's a difference between phone calls at work and e-mail at work. Under the Electronic Communications Privacy Act of 1986, an amendment to the federal wiretap law, companies cannot monitor personal phone calls; however, e-mail remains fair game.

## GLOBAL IMPACTS

Electronic commerce will continue to grow, but its full potential will not be achieved without international co-operation between businesses, individuals, and governments. This co-operation is required in order to bring a balanced solution to the requirements to provide secure and authenticated electronic commerce transmissions whilst preserving the rights of government to monitor such transmissions for the purposes of public policy, preservation of data protection, and prevention of illegal acts and terrorism (Bond & Whiteley, 1998). New Internet laws are required, without becoming overly burdensome to e-commerce businesses and users (Krishnan, & Jane, 2004, p. 9). Existing laws are not capable of being adapted to this truly new sphere of business. The current laws suffer from two fundamental problems: 1) the changing nature of the technology had the potential to render any legislation

redundant within a short period of time, and 2) national laws are inadequate to govern what is truly a global issue (Krishnan & Jane, 2004). Due to the global reach of e-commerce, the vast span of electronic commerce creates difficulty in reaching a consensus on suitable laws.

**Practical Examples of Internet Legal Rulings with Global Implications – And Recommendation**

In 2000, one of the most popular online auction houses and Internet portal Yahoo!, started to offer Web surfers hundreds of Nazi artifacts to the highest bidder. The Lique Internationale Contre le Racism et l'Antisemitisme (LICRA) was joined by the Union of French Jewish Students (UEJF) and initiated legal action against Yahoo!. The two groups maintained that Yahoo!'s public auctions of Nazi memorabilia constituted a direct affront to French laws that prohibit any public material that incites or promotes Nazism or hate (Sammut, 2007, p.1). The Yahoo! lawsuit is significant because it establishes legal precedent in the attempt by a national court to exercise and impose its jurisdiction over another country's by demanding the removal of contentious Web site contents (Sammut, 2007, p.1). Major implication for Internet freedom and civil liberties are also incorporated in the Yahoo! legal action.

A 2002 ruling by Australia's highest court could have far-reaching implications for U.S. –based Internet publishers who may find themselves facing libel suits in countries where freedom of speech is not as vigorously upheld as in the U.S. (Goodenough, 2002). The Australian High Court ruled that Australian-based mining entrepreneur Joe Gutnick could sue American multimedia giant Dow Jones in the state of Victoria over material published on its WSJ.com website (Head, 2002). Gutnick claimed a WSJ.com article was defamatory. The WSJ.com website is posted in New Jersey, U.S.

In addition to defamation laws, media lawyers predict Internet publishers could be exposed to contempt of court charges in every country under the same principle (Head, 2002). Countries operating in the English common law tradition are likely to follow the Australian High Court precedent, including Britain, Canada, New Zealand, Malaysia, India, Sri Lanka, Fiji, Singapore, Zimbabwe and South Africa (Head, 2002, p.1). Similar rulings have been made by the Japanese and Canadian courts having major implications for how we think of jurisdiction over Internet activity.

In 2005, the World Trade Organization (WTO) ruled that the U.S. can set certain limits on Web gambling sites located in offshore locations. Under the WTO ruling, the U.S. could restrict online gambling on sporting events, but could not prohibit offshore companies from offering online betting on horse racing, since some states already allow that form of gaming over the Internet.

**Recommendation:** Web publishers in all countries should be aware of legal rulings practiced in various countries and lawsuits which have established legal precedent as we move toward a consistent global legal e-Commerce environment.

## CONCLUSION

There are several regulations and legal rulings that provide structure in the E-Business environment. Countries have different approaches to Internet regulation. Most countries of the world regulate the Internet within the framework of their political, legal, moral and cultural values. The key forum for promoting and negotiating a liberal trade environment for electronic commerce internationally at this time is the World Trade Organization (WTO). Continued implementation of agreements between countries actively trading in electronic commerce is required to move toward a consistent global legal e-commerce environment. Agreements amongst all e-commerce trading countries would lead the way to a consistent global legal environment.

## REFERENCES

1. Baby, J. (2003). E-Commerce law issues for business. Mason: West Legal Studies in Business.
2. Becker. (1986). Whelan Associates Inc. v. Jaslow Dental Laboratory, Inc., et al. Retrieved March 10, 2007 from http://digital -law-online.info/cases/230PQ481.htm.
3. Biegel, S. (2001). Beyond our control: confronting the limits of our legal system in the age of cyberspace. Cambridge: MIT Press.
4. Bond, R., & Whiteley, C. (1998). Untangling the web: A review of certain secure e-commerce legal issues. International Review of Law Computers & Technology, 12(2), 349-370.
5. Eko, L. (2001). Many spiders, one worldwide web: Towards a typology of internet regulation. Retrieved June 05, 2003 from www.capella.edu online library.
6. Goodenough, P. (200). Court ruling may have global implications for online media. Retrieved on May 4, 2007 from http://www.cnsnews.com.

7. Head, M. (2002). Australian high court libel ruling threatens Internet free speech. Retrieved on May 4, 2007 from http://www.wsws.org/articles/2002/dec2002/defa-d13.shtml.
8. Isenberg, D. (2002). Gigalaw guide to internet law. New York: Random House Trade Paperbacks.
9. Krishnan, V., & Jane, J. (2004). Legal and transaction issues in e-commerce. Retrieved December 4, 2004 from http://www.indiainfoline.com/bisc/ietx.html.
10. Lessig, L. (2000). Code and other laws of cyberspace. New York: Basic Books.
11. Rosenoer, J. (1997). Cyberlaw: the law of the Internet. Germany: Springer Verlag.
12. Sammut, H. (2007). J'Accuse encore. Retrieved on May 4, 2007 from http://www.maltacolocation.com/page.asp?p=197&l=1&i=144.
13. Turban, E., King, D., Lee, J., & Viehland, D. (2004). Electronic commerce 2004 a managerial perspective. Upper Saddle River: Pearson Prentice Hall.
14. Tysver, D. A. (2000). Trademark on the Internet. Retrieved June 06, 2003 from http://www.bitlaw.com/internet/trademarks.html.

Table 1. Five-Part Typology of Internet Regulation

| Model | Model Description |
|---|---|
| Multilateralist or International Model | The Multilateralist model is anchored in international agreements, conventions, policies, regulations and treaties to which most of the countries of the world agree, either as individual nations or within the framework of regional economic or political groupings (Eko, 2001). |
| Neo-Merchantilist or E-Commerce Model | The Neo-Merchantilist model is a regulatory model that combines several libertarian principles and applies them to the Internet; thereby, making them global concepts. This includes the marketplace of ideas, laissez-faire economics, free trade, and the free flow of information, goods and services (Eko, 2001). |
| Culturist Model | In the Culturist model, culture and cultural protection are the overriding goals of Internet regulation (Eko, 2001). |
| Gateway Model | Under the Gateway model, a government or a government agency serves as the de facto or de jure gateway to the Internet for whole countries or regions (Eko, 2001). |
| Developmentalist Model | The Developmentalist model is rooted in an understanding of the role of mass communication in social and economic development that was first applied to "non-self-governing territories" during the colonial era (Eko, 2001). |