

Encyclopedia of Law & Society: American and Global Perspectives

Internet Law

Contributors: Peter B. Maggs

Editors: David S. Clark

Book Title: Encyclopedia of Law & Society: American and Global Perspectives

Chapter Title: "Internet Law"

Pub. Date: 2007

Access Date: December 08, 2014

Publishing Company: Sage Publications, Inc.

City: Thousand Oaks

Print ISBN: 9780761923879

Online ISBN: 9781412952637

DOI: <http://dx.doi.org/10.4135/9781412952637.n365>

Print pages: 814-816

©2007 SAGE Publications, Inc. All Rights Reserved.

This PDF has been generated from SAGE knowledge. Please note that the pagination of the online version will vary from the pagination of the print book.

<http://dx.doi.org/10.4135/9781412952637.n365>

The Internet is a worldwide system of computer networks that use standardized, compatible communications procedures to transfer data. These procedures include physical communications protocols and data structures, such as those for pages on the World Wide Web and for electronic mail. The Internet facilitates the transfer of all kinds of data, including personal letters, photographs, sound recordings, motion pictures, and computer software. The worldwide nature of the Internet creates serious problems of conflict of national laws concerning matters such as jurisdiction, free speech, privacy, and intellectual property. Legal problems abound because most e-mail is unwanted and usually fraudulent advertising and much, perhaps most, network traffic consists of pornography distribution and copyright piracy. There is also a continuing tension between the Internet service providers (ISPs), who seek immunity from liability for the content of the information they transmit, and those harmed by these transmissions, who wish to make the ISPs police their users' conduct.

Standardization is essential to making the Internet work. Most of this standardization is voluntary, done by the World Wide Web Consortium. There has been considerable government intervention in the area of assignment of Internet domain names. The U.S. government, by contract, has given control over key aspects of this function to the Internet Corporation for Assigned Names and Numbers as the registry for the popular .com domain. Competing registrars provide technical services in registering domain names. The degree of government involvement in the management of national domains (for example, .de for Germany, .jp for Japan) varies from country to country.

The issue of jurisdiction over Internet activities presents complex problems. A Web site can be hosted on a computer anywhere in the world and be accessible to Internet users anywhere in the world. E-mail can be sent from any Internet user to any Internet users. In the course of transmission, data sent over the Internet passes through computers owned by many different organizations. When does a country (or a state in a federal system) have jurisdiction over legal issues arising from the data transfer? Most litigation over this question has occurred in the United States in cases in which a business located in one state has been sued in another state. Courts in the United States have looked to the contacts that the defendant has with the state where the suit was brought (forum). One may bring any type of action against defendants with extensive contacts with the forum state. Where contacts are more limited, three criteria must be met: (1)

the action must arise out of the contacts, (2) the defendant must have purposely availed itself of the privilege of conducting activities in the forum state, and (3) jurisdiction must be fair and just. Standards for jurisdiction will vary from country to country, but [p. 814 ↓] one may expect that a company that actively uses the Internet to sell goods or services in a particular country will be subject to the jurisdiction of that country with regard to Internet sales.

There are many differences in laws from country to country regarding freedom of speech in areas such as libel, pornography, advertising, and political campaigning. Since the Internet reaches everywhere, speech that is permissible at the source may be impermissible where viewed abroad. The most notable case involves a conflict between French and U.S. law. French law bans, but U.S. law permits, anti-Semitic and pro-Nazi speech. Yahoo, which hosted sales of Nazi paraphernalia and Nazi discussion groups, lost a case in the French courts but then pursued litigation in the United States designed to prevent enforcement of the French court ruling in the United States. A U.S. Court of Appeals found that the dispute by 2006 was moot since Yahoo had substantially complied with the French decision. Libel laws in the United States are much more tolerant of criticism of public figures than are libel laws in other English-speaking countries. As a result, the *Wall Street Journal* has found itself defending stories posted on its U.S. Web site but accessible to readers in the United Kingdom and Australia. In areas where laws are harmonized, for instance in criminalizing the Internet distribution of child pornography, international cooperation has been highly effective.

Internet commerce also presents problems because of differing regulation of commercial activity in different jurisdictions. Many countries allow Internet gambling. Others, like the United States, effectively ban Internet gambling but allow other forms of gambling. A World Trade Organization dispute resolution panel, and appellate review, found that the United States had improperly discriminated against gambling enterprises in Antigua by banning Internet gambling. The United States in 2007 was negotiating implementation of this decision. Varying consumer protection and data privacy laws also present serious problems for international sales over the Internet. Efforts are well under way in the European Union to solve these problems within the European economic space.

Most Internet-related litigation has been about intellectual property issues. Trademark litigation has centered on domain names. Copyright owners have brought numerous suits against organizations that have facilitated illicit file sharing and against the file sharers themselves. Patent owners have taken advantage of the broad protection of business methods in U.S. patent law to claim exclusive rights in basic methods of Internet commerce.

The issue of trademark rights in domain names is complicated by the nature of the domain name system. International treaties have led to a high level of standardization of trademark law from country to country. Two basic principles are (1) that trademark rights are limited by national boundaries and (2) that trademark rights are limited to particular categories of goods or services. However, businesses strongly prefer to register domain names in the .com domain. Under trademark law, different companies could register, for instance, Acme as a trademark in different countries, and different companies could even register Acme as a trademark for different products in the same country. However, there can be only one <http://acme.com> domain name.

The situation has been further complicated by cybersquatters, who rush to register famous trademarks as domain names, hoping to sell the domain names to the trademark owners. The law has dealt harshly with cybersquatters. Domain registries have implemented compulsory dispute resolution procedures heavily weighted against cybersquatters. Courts have stretched traditional trademark laws and newer antidilution laws to cover cybersquatting. The United States and other countries have passed legislation specifically aimed against cybersquatting. There is less uniformity on the issue of the rights of a person who registers a domain name incorporating a trademark so as to exercise free speech rights to criticize the trademarked goods or services.

Copyright owners see the Internet as a huge and rapidly expanding threat to their rights. The rapid spread of broadband Internet access and peer-to-peer software has led to an ever-increasing volume of the distribution of music files and to a rapidly emerging practice of the distribution of motion pictures. Because the United States is the world center of both the entertainment industry and the computer industry, it has been the site of path-breaking litigation. Domestic

Web sites openly distributing copyrighted material are not part of the problem, because criminal and civil copyright laws make it easy to shut them down. Rather the problem is centered on peer-to-peer distribution, whereby music or movies are transmitted from one personal computer to another directly over the Internet without going through a central server. Initial lawsuits were successful against systems like Napster and Aimster, which provided indexes to aid users in locating (usually illicit) files. In the *Grokster* case, *MGM Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005), the U.S. Supreme Court held that the defendant, which had created a pure peer-to-peer system with no central indexing, could be sued for copyright infringement. The company then closed down its peer-to-peer file sharing service.

The United States has gone further than other countries in allowing patents for business methods, including business methods implemented with computer software. During the 1990s, the U.S. Patent and Trademark Office was flooded with applications for business method software implementations but lacked a good method of searching for prior art. As a result, many unwarranted patents were issued, leading to extensive subsequent litigation. The European Union is currently debating the proper role of software patents.

Unsolicited, unwanted e-mail advertising has become a huge problem worldwide. In 2003, the U.S. Congress passed the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM) Act, 15 U.S.C. § 1701 (Supp. III 2003), which purported to regulate such e-mail but in fact preempted stronger state statutes. The act has been a total failure. Unsolicited e-mail has substantially increased since 2003; no more than 1 percent of e-mail advertising complies with the act. The act took an opt-out approach to e-mail advertising, in contrast to the European Union's opt-in approach. However, the difference in approaches has made no difference in results, since the senders of unsolicited e-mail completely ignore the applicable laws everywhere. Only a handful of enforcement proceedings have taken place under CAN SPAM. The reasons for the failure of the act to curb unsolicited e-mail lie not in the flawed provisions introduced through industry lobbying, but in the structure of the Internet itself. What is needed for a solution is not corrective legislation and not more enforcement action but rather a key change in the Internet mail system to allow tracing of rogue mail sources.

Peter B. Maggs

<http://dx.doi.org/10.4135/9781412952637.n365>

See also

- [Civil Court Procedures, Doctrinal Issues in](#)
- [Communications Revolution](#)
- [Communications Systems](#)
- [Expression, Freedom of](#)
- [Gambling](#)
- [Intellectual Property, Doctrinal Issues in](#)
- [Sovereignty and Jurisdiction](#)
- [Technology, Legal Practice and New](#)

Further Readings

Bellia, Patricia L., Paul SchiffBerman, and David G.Post. (2007). *Cyberlaw: Problems of Policy and Jurisprudence in the Information Age* , 3d ed. St. Paul, MN: Thomson-West.

Bowrey, Kathy. (2005). *Law and Internet Cultures* . Cambridge, UK: Cambridge University Press.

Geist, Michael A. (2002). *Internet Law in Canada* , 3d ed. Concord, Ontario: Captus Press.

Radin, Margaret Jane, John A.Rothchild, and Gregory M.Silverman. (2002). *Internet Commerce: The Emerging Legal Framework* . New York: Foundation Press.

Wright, Claire, WillMcAuliffe, and AnnaGamvros. (2003). *Internet Law in Hong Kong* . Hong Kong: Sweet & Maxwell Asia.