Liability Issues Facing Online Businesses

David Shipley
Georgia Athletic Association Professor in Law
University of Georgia School of Law, shipley@uga.edu

Repository Citation

This Article is brought to you for free and open access by the Faculty Scholarship at Digital Commons @ Georgia Law. It has been accepted for inclusion in Scholarly Works by an authorized administrator of Digital Commons @ Georgia Law. Please share how you have benefited from this access. For more information, please contact tstriepe@uga.edu.
Liability Issues Facing Online Businesses

By David E. Shipley

Online businesses are confronted by a wide variety of liability issues covering almost the full range of the standard law school curriculum. The liability problems that face a small business in Vidalia, Georgia, which is selling Vidalia onion products at specialty stores, through print advertising, and by mail, do not go away when the business starts marketing through a Web site. In fact, there might be more exposure doing business online, and there are variations depending upon the nature of the business in question. For example, as discussed below, an Internet Service Provider ("ISP") like America Online has worries that are not shared by the online Vidalia onion business. The decision to take a business online should not be taken lightly. This article addresses only a few of the high points of this ever changing and expanding subject.

Jurisdiction

Where can an online business be sued? Courts throughout the United States are deciding cases regarding
jurisdiction over online defendants. Some courts have concluded that merely posting a Web site that can be accessed in a state is not enough for personal jurisdiction, unless the company is using its site to solicit business in the forum state.¹ For instance, in one case a South Carolina defendant's Web page, accessible by residents of all states, was not a sufficient contact to subject that defendant to personal jurisdiction in Oregon even though an Oregon resident could place orders with the defendant through the site.² Jurisdiction may depend upon showing that the Web site operator seeks contacts within the jurisdiction beyond just posting a site.³ On the other hand, some courts may be willing to find personal jurisdiction notwithstanding the passive nature of the defendant's Web site.⁴ Thus, if a company transmits information over the Internet while knowing that the information will be disseminated in a particular state, it may be subject to personal jurisdiction in that state for violations of its laws.⁵

Foreign countries might try to reach an online business with even fewer contacts to the forum. For example, German law arguably subjects any Web site accessible
from Germany to its jurisdiction, and authorities there recently arrested a CompuServe executive when the company failed to take steps to stop the transmission of child pornography accessible in Germany.\(^6\) Similarly, European consumer laws may apply when companies make sales to European consumers over the net. A recent European Community directive mandates that choice of law in disputes over consumer contracts is always the law of the domicile of the consumer.\(^7\) It seems that the hypothetical Vidalia onion products company with its Web site marketing plan may be subject to jurisdiction far outside of the Georgia counties where true Vidalia onions are grown.

### Invasions of Privacy

Concerns about invasions of privacy through new technology predate the Internet; however, its rapid expansion has increased threats against privacy. The Internet has reduced the cost of information, has made access easier than before, and has created new ways of gathering personal data. At the same time, information has become more valuable. Liability may arise by failing to implement appropriate security measures and policies for maintaining a secure system. Confidential information held by an online business without a secure system could be readily accessible to a hacker. This should be a concern to doctors and lawyers who operate online. Confidentiality of patient and client information must be protected. Conversely, liability may also arise from improperly invading the privacy of other persons. Accordingly, a Web site which collects user data must have a policy on how it utilizes and maintains user information online.\(^8\) The FTC has issued online privacy recommendations, the European Union has a Directive on the Protection of Personal Data,\(^9\) and the Children’s Online Privacy Protection Act regulates the collection, use, and distribution of information from individuals 13 years or younger. Although this latter statute is controversial and has been challenged,\(^10\) there are many other federal statutes which protect the privacy of information.\(^11\)

Having an internal policy on e-mail and computer use by employees is important. For example, the University of Georgia’s policy on the use of its computers includes the following statement:

Users shall not place confidential information in computers without protecting it appropriately. The University cannot guarantee the privacy of computer files, electronic mail, or other information stored or transmitted by computer unless special arrangements are made.\(^12\)

Any employee who reads this statement should understand that they cannot expect privacy protection for their e-mail communications and, in the event a communication is disclosed or made public, that their claim for invasion of privacy could be weak.

Online businesses must be prepared for privacy claims. Protecting credit-card numbers and other financial information of consumers is vital. Doctors, lawyers and other professionals with online operations must protect the personal information of their clients. As the amount of highly confidential information held online increases, there will be a corresponding increase in the number of complaints about invasions of privacy and violations of statutes designed to protect privacy.\(^13\)

### Tax Liability

The Internet Tax Freedom Act, passed in 1998, imposes a three-year ban on discriminatory taxes associated with Internet access and services, but it did not eliminate state taxes that were already in place.\(^14\) Many states have taxes on Internet access, telecommunications services, and other types of computer processing. At a minimum, an online business must be concerned about potential sales, use, and income taxes in those states where it is doing business, procuring and supplying goods, and making sales.\(^15\) Professor Walter Hellerstein’s summary of the law of sales taxes in a cyber economy is as follows:

First, states possess the power to enact sales and use taxes on electronic commerce subject to the limited restraints now temporarily imposed by the Internet Tax Freedom Act. Second, states generally have exercised that power under their sales and use taxes only with respect to tangible (as distinguished from digital) products. Third, states lack the constitutional power to require a non-physically-present seller who sells tangible or digital products over the Internet to collect any use tax that a state may seek to impose with respect to such products, even though the
consumer has a legal obligation to pay such use tax. Finally, Congress possesses broad constitutional authority to expand, restrain, or otherwise prescribe the rules governing state taxation of electronic commerce.\textsuperscript{16}

In short, tax liability issues are not settled. Online businesses should not expect to receive clear answers to all of their questions about these potential tax issues.

**Contractual Liability Issues**

Purchasers of personal computers and software are now familiar with the warning that flashes on the screen when the machine is turned on for the first time or when new software is loaded: “By turning on this XYZ computer and loading the XYZ software package, the purchaser/operator hereby agrees to the terms of the following license.” The terms and conditions of most of these licenses, often called click-on licenses, are likely enforceable in view of the decision in \textit{ProCD, Inc. v. Zeidenberg}.\textsuperscript{17} An online business may need to adhere to another company’s license, and it may need to enforce its own click-on, click-off license. The holding of \textit{ProCD} also raises a number of issues such as what type of notice, if any, is sufficient to inform a buyer that certain contract terms will apply. A pay-now-terms-later license was held enforceable in \textit{M. A. Mortenson Co. v. Timberline Software Corp.}\textsuperscript{18} These types of licenses appear to be enforceable even if notice of the terms seems minimal, and, according to several courts, the Gateway 2000 “Accept or Return” policy does not constitute a contract of adhesion.\textsuperscript{19} Moreover, recent decisions portend regular enforcement of bundled or linked terms, at least insofar as is necessary to reasonably protect intellectual property rights. However, it is too early to tell how these results will be balanced against the willingness of some courts to find such agreements unenforceable when necessary to protect the rights of injured consumers.\textsuperscript{20}

The doctrine of copyright misuse is gaining acceptance, and courts might apply it more often in licensing litigation. This doctrine is defined as the use of a copyright to secure an exclusive license or limited monopoly beyond that granted by copyright law and which is contrary to public policy.\textsuperscript{21} For instance, the Fourth Circuit held that a company had misused its copyright by including in its standard license a non-competition clause which prohibited licensees from creating competing software programs during the ninety-nine year term of the license. The court stated this agreement “essentially attempts to suppress any attempt by the licensee to independently implement the idea which [the copyrighted program] expresses.”\textsuperscript{22} The length of the restraint also was a problem for the court.\textsuperscript{23} However, it is important to note that the concept of copyright misuse is not settled. Drafters of software licensing agreements must weigh carefully the impact of this potential defense. Poor drafting may deprive copyright owners of the ability to enforce their copyrights and license agreements.\textsuperscript{24}

**Criminal liability**

The Internet can be misused in a variety of ways that may result in criminal liability for the user. For instance, in the spring of 1999 the FBI arrested a Raleigh, North Carolina, man on federal charges of fabricating news of a corporate takeover and posting a false report on an Internet site said to belong to the Bloomberg News Service. This is believed to be the first stock manipulation scheme done with a fraudulent site. Due to the hoax, the publicly traded stock of the company in question, PairGain, went up over 30 percent and trading volume increased dramatically.\textsuperscript{25}

In another federal case, a Utah citizen was indicted for making a threatening communication in violation of a federal statute when he knowingly transmitted in interstate commerce a communication stating that he intended to injure another person with a bomb. The fact that the threatening message was sent to someone in Utah did not block the prosecution because the message first went to America Online’s facility in Virginia before reaching the Utah recipient. The federal magistrate held that the defendant had used interstate commerce and this was upheld by the district court.\textsuperscript{26}

In another case, a former network administrator was indicted for launching a LAN-based logic bomb which was timed to explode three weeks after he had been fired. This act of sabotage destroyed his former company’s software and caused over $10 million in damage. He was charged with violating federal statutes outlawing fraud and other activities with computers.\textsuperscript{27}

Internet content providers need to be aware that their material can be examined for obscenity not only under the community standards of the place they are located, but also in any community in which the material is available. A pornographic site based in Atlanta could be charged under federal obscenity laws in Arkansas and judged under the community standards in Little Rock.\textsuperscript{28}

Computer crime is a growing concern for network operators and online businesses. They must devote more and more resources to avoid system crackers, unauthorized access to their information, damage to data, the spread of viruses, and other kinds of hacking.\textsuperscript{29}
Liability for Unauthorized Practice

Lawyers, doctors and other professionals are using the Internet, and Web sites devoted to medical, legal and financial issues are common. These sites help with marketing and attracting new clients and customers. However, regulation of professional advertising varies from state to state. Some jurisdictions have begun to monitor lawyers’ Web sites, and the medical press is warning doctors about liability issues which may arise from their sites. Moreover, cyberlawyers and cyberdoctors must be concerned about engaging in unauthorized practice in those jurisdictions where their sites can be accessed. In January 1998 the California Supreme Court opined that a lawyer may be engaging in the “unauthorized practice of law” in violation of state statutes, by advising a California client on California law through “telephone, fax, computer, or other modern technological means.”

Liability for Fraud and Unfair Trade Practices

Statutes and common law proscribing fraud are being extended to deal with online activities. The FTC has sued to halt a pyramid scheme operated on a company’s Web site, and the SEC has pursued a number of fraudulent online marketing schemes. More and more companies are selling securities on the Web, and the Internet contains a great deal of information about publicly traded companies. Hence, misleading or deceptive information on a site may result in violations of unfair trade practice and consumer protection statutes. The Computer Fraud and Abuse Act, with civil and criminal provisions, is a powerful weapon against hackers. For instance, in North Texas Preventative Imaging, L.L.C. v. Eisenberg, a time bomb inserted into a software update to ensure payment was seen as a possible violation of the Act’s civil provisions.

It is reasonable to conclude that a marketing scheme, trade practice, sales program, or method of doing business which is regarded as fraudulent or unfair in the “offline” world, also will be treated as fraudulent or unfair when it is perpetrated online.

Liability for Defamation and Libel

Managing libelous speech on the Internet is another area of concern. Online businesses can be liable for slander, defamation and libel through a wide variety of online activities. For instance, Wade Cook Financial and Wade Cook Seminars filed suit in federal court for defamation against several “John Doe” defendants — unnamed users of Yahoo! Inc. — alleging that they published false and defamatory statements about the company on the Yahoo! Business & Finance Message Board. Defamation can occur in a posting on a bulletin board or on a file server, databases can contain defamatory material, and there can be defamatory statements in e-mail. A scanned photograph can be defamatory. Here also, an entity responsible for posting a defamatory message online can be just as liable for its actions as if it had made the defamatory statement in the offline world.

For ISPs like America Online and CompuServe, a much debated issue is whether they should be liable for the defamatory speech of their members. Permitting widespread distribution of libel on the Internet can damage the community of users, but mandating liability for ISPs or those in a position to be moderators of postings can be just as damaging and possibly result in regulation of speech and its content. Section 230 of the Communications Decency Act of 1996 granted ISPs broad immunity from liability if they merely carry content generated by others. In Doe v. America Online, Inc. a tort action for distribution of child pornography was dismissed in reliance on section 230. Similarly, in Zeran v. America Online, Inc. the court upheld an ISP’s immunity and explained that Congress’s rationale for this protection was “to maintain the robust nature of Internet communication” and to keep ISPs from “severely restrict[ing] the number and type of messages posted” out of fear of being liable. The court in Blumenthal v. Drudge took an extra step and held that even an ISP which pays a member for certain postings is immune from liability for the poster’s libel absent a showing of ISP control.

The debate over whether an ISP should be immune from liability for the libelous postings of its members will likely continue as use of the Internet grows. Blanket immunity might go too far, but it is difficult to predict the chilling impact of holding ISPs liable for members’ postings.
Liability for Sexual Harassment and Other Employment Issues

The use of Web sites and e-mail can expose companies to claims of sexual harassment, creating a hostile work environment and employment discrimination. A company-wide policy defining appropriate uses may be necessary. Moreover, it is important to remember that employee use of e-mail can be evidence obtained through discovery in litigation, yet employer monitoring of company/employee e-mail and Web page use can expose the employer to liability for violating the Electronic Communications Privacy Act.44

Liability for Termination of Users

The issue of potential liability for terminating members has not been heavily litigated, but ISPs are being advised to establish use policies with members in order to make their authority to terminate clear. So long as providers are regarded as private actors rather than public forums or utilities, such membership contracts and policies should be upheld. For instance, in Cyber Promotions, Inc. v. Apex Global Information Services, Inc.,45 an ISP’s summary termination of a member was enjoined because the contract between the ISP and the member provided for notice prior to termination. The court said that even though the member, Cyber Promotions, was not liked on the Internet, it was entitled to have its contract enforced.46

Liability for Infringement of Intellectual Property Rights

Any online business needs to be aware of copyright and trademark infringement issues because “[i]n general, unauthorized use on the Internet of another's written words, trademarks, trade names, service marks, literary characters, images, music or sound is a violation of that party’s intellectual property rights, just as it would be in a non-Internet medium under traditional principles of intellectual property law.”47 Infringement can result from the selection of a domain name that is used to identify and locate the site on the Internet. Many companies use their trademark as the domain name for their site (such as “www.ford.com” for Ford Motor Company), but it is not uncommon for companies to encounter another site operating under an identical or confusingly similar domain name. Counsel needs to be familiar with the policies and procedures of Network Solutions, Inc., which is responsible for the registration of domain names, the case law on domain name disputes, and the law on trademark infringement and dilution.48

Copyright infringement is very easy with the Internet. Once online, digital versions of works can be uploaded, downloaded and duplicated with ease, modified, and transmitted to thousands of other users almost instantaneously. Virtually every activity on the Internet—browsing, caching, linking, downloading, accessing information, and operating an online service—involves making copies. Copying is inherent to the medium, but there is still uncertainty about the scope of copyright owners’ rights. They may have potentially unprecedented rights over the use of their materials on the Internet, and balancing their rights with user interests will have to be struck by application of the fair use doctrine and recognition of implied licenses.49

Discovering, tracking and stopping trademark and copyright infringement on the Internet is daunting, but techniques and technology are being developed to monitor the Web for illegal use of trademarks, copyrighted materials, and other works.50

Franchise Liability

Franchise law violations can occur in cyberspace in any jurisdiction from which someone can access a supplier’s Web site. The FTC has proposals to deal with the application of franchise regulations in cyberspace, but these proposals will not help suppliers of computer hardware and software determine whether their distribution agreements are subject to franchise regulation in the first place. If a supplier does not want to deal with the laws and regulations associated with being a franchise, it may need to change its relationship with distributors to avoid having contracts satisfy the definition of a franchise.51

Liability for Advertising

The Internet works well for advertising but this easy and relatively inexpensive access to the global market also gives everyone relatively easy access to the site owner. Every site owner needs to remember that the site could be subject to regulation or result in liability outside those specific areas being targeted by the advertising. Some countries prohibit comparative advertising, and others may deem sexual, religious or political content illegal.52 For instance, as noted above, a prosecutor in Munich arrested the local managing director of CompuServe on charges that Internet content distributed by CompuServe’s main computers in Dayton, Ohio, violated German anti-obscenity laws. The local managing director had nothing to do with the content made available to CompuServe subscribers.53
Liability Issues Facing Service Providers

ISPs are confronted by a variety of legal issues. If the system is used as an outlet for defamation, should the user who posted the defamatory statement or the ISP providing the forum be held liable? If pornographic or obscene material is posted, who is liable? If copyrighted material is reproduced and transmitted without the permission of the copyright owner, who is liable? Can the provider be liable for the spread of a virus? Can the provider be liable for invasions of privacy? What risks are being faced by system operators?54 What if the general service provided by the ISP is deficient?55 There are several theories for either holding ISPs liable or arguing that they should be exempt including analogies between ISPs and the print media; asserting that the ISP is a common carrier or broadcaster; or saying that the system is like routine mail delivery, a public forum, or a traditional bulletin board. In any event, how realistic is it for an ISP to be able to control or monitor the thousands of messages which are transmitted on its system?56 Fortunately, many of the issues surrounding potential ISP liability for copyright infringement are now addressed by amendments to the Copyright Act that were enacted in 1998,57 and the Communications Decency Act of 199658 addresses ISP liability for libelous postings.59

Conclusion

Taking a business online through the utilization of new information technologies and use of the Internet is exciting. There is no doubt that the potential rewards are tremendous. There are, however, many risks involved. Business practices, employee conduct, and other activities which can lead to liability in the "offline" world, will also result in liability for the online business.60 Nevertheless, it is clear that these risks have not stopped entrepreneurs from establishing successful offline businesses, and the online liability risks do not appear to be holding back many cyberspace entrepreneurs. Log On! 

Endnotes

6. Masters, supra note 5, at 5.
7. Ron N. Dreben & Johanna L. Werbach, Top 10 Things to Consider in Developing an Electronic Commerce Web Site, COMPUTER LAW., May 1999, at 17, 19; see also Cendali, supra note 5, at 58-74; Masters, supra note 5, at 5.
12. The University of Georgia Computer Security and Ethical Use Committee (visited Jan. 6, 2000) <http://www.uga.edu/compssec/use/html/>. The computer policy includes the following comments to provide further guidance: Ordinary electronic mail is not private. Do not use it to transmit computer passwords, credit card numbers, or information that would be damaging if made public. Bear in mind that students’ educational records are required by law, and by U.S.C.A. policy, to be kept confidential. It is also necessary to protect confidential information about employees, such as performance evaluations. This applies not only to networked computers, but also to computers, tapes, or disks that could be stolen; an increasing number of computer thieves are after data rather than equipment. The University will normally respect your privacy but cannot guarantee it absolutely. There are many ways a normally private file can end up being read by others. If a disk is damaged, a system administrator may have to read all the damaged files and try to reconstruct them. If email is mis-addressed, it may go to one or more “postmasters” who will read it and try to correct the address. For your own protection, system administrators will often look at unusual activity to make sure your account hasn’t fallen victim to a “cracker.”

David E. Shipley has been dean and professor of law at the University of Georgia School of Law since July 1, 1998. He has experience teaching courses on copyright, administrative law, civil procedure, intellectual property, legal and equitable remedies, and domestic relations. He is a graduate of Oberlin College (Ohio) with highest honors in American History, and the University of Chicago Law School where he was executive editor of the Chicago Law Review.
The Georgia Open Records Act applies to information stored in computers. This act gives citizens the right to obtain copies of public records, including any record prepared, received, or maintained by the University in the course of its operations. Some kinds of records are exempt; among these are student records (including tests and homework), medical records, confidential hiring evaluations, trade secrets (which probably includes unpublished research), and material whose disclosure would violate copyright. Moreover, the Open Records Act is not a license to snoop; requests for information must be made through proper administrative channels.

15. Dreben & Werbach, supra note 7, at 18.
17. 86 F.3d 1447 (7th Cir. 1996).
20. Stephen J. Davidson & Scott J. Bergs, Open, Click or Download: What Have You Agreed To? The Possibilities Seem Endless, COMPUTER LAW., Apr. 1999, at 1, 6, 8.
22. Id. at 978.
23. Id.
28. See United States v. Thomas, 74 F.3d 701 (6th Cir. 1996); see generally George B. Delia & Jeffrey H. Matsuo, LAW OF THE INTERNET Ch. 8 (2000) (Chapter 8 is entitled “Obscene and Indecent Materials”); Casenover supra note 5, at 549.
31. Masters, supra note 5, at 6.
32. SEC Continues Internet Fraud Crackdown, COMPUTER LAW., Apr. 1999, at 27 (summarizing four enforcement actions filed by the SEC on February 25, 1999, against 13 individuals and companies across the country for committing fraud over the Internet and deceiving investors).
33. See also Jonathan Wilson, What’s In a Web Site?, GA. B.J., Apr. 1999, at 14-18.
36. See also supra note 28, at 1116.
37. Company Files Defamation Action Against “John Doe” Internet User, COMPUTER LAW., Apr. 1999, at 27; see also Masters, supra note 5, at 6.
38. Lounbry, supra note 28, at 1106, 1115.
41. No. 129 F.3d 327 (4th Cir. 1997).
42. Id. at 330-31.
47. Id. (Cyber Promotions was a spammer — a company which, without solicitiation, e-mailed its message to thousands of addresses simultaneously); see also Developments in the Law, supra note 42, at 1604. No court has yet imposed on an ISP a duty to provide notice and a hearing to terminated members, but if the public access model of the Internet grows, public providers may be classified as state actors who should be held to certain procedural requirements before member termination. Developments in the Law, supra note 42, at 1605.
48. Cendali, supra note 5, at 485.
49. Scott A. Zebrik, A Step-by-Step Guide to Handling Domain Name Disputes, COMPUTER LAW., Apr. 1999, at 21, 23; see also Cendali, supra note 5, at 492-523 (summaries of numerous cases involving domain name disputes).
51. Cendali, supra note 5, at 486-87.
54. Masters, supra note 5, at 6; Ezor, supra note 51, at 8; see generally Mary M. Luria, Controlling Web Advertising: Spamming, Linking, Framing, and Privacy, COMPUTER LAW., Nov. 1997, at 10.
55. Loundy, supra note 28, at 1081-82.
57. Loundy, supra note 28, at 1082-1105.
60. See also supra note 29 to 35.
61. Wright & Winn, supra note 54, at 1-1.