Winter 1996


Diana J. P. McKenzie

Follow this and additional works at: http://repository.jmls.edu/jitpl

Part of the Computer Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation


http://repository.jmls.edu/jitpl/vol14/iss2/3

This Article is brought to you for free and open access by The John Marshall Institutional Repository. It has been accepted for inclusion in The John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of The John Marshall Institutional Repository.
Without Getting Wet

DIANA J.P. McKENZIE†

I. INTRODUCTION

Not too long ago, transacting business involved nothing more than paper, pen, and face-to-face contact. Whether you were building a house or publishing a book, the dealings relied on physical space: A meeting, a written contract, a finalizing handshake. But even then, when intentions could be expressed clearly by all parties, countless legal problems arose. With the arrival of telephones, televisions, telexes, and fax machines, the landscape of business liability changed considerably. Legislatures and the courts struggled to keep law abreast of technology.

None of the legal developments of the past could have prepared us for the transformations in business law happening right now—with the recent predominance of computers in the marketplace. What promises to be the most exciting and most complex area of future legal development is that of "cyberspace," a word that encapsulates numerous terms-of-art: The Information Superhighway, the Internet, and the World Wide Web, among others. The law in cyberspace poses many challenges precisely because of the radical departure from most of our preconceived notions about business transactions. Cyberspace allows its users to obliterate, and declare obsolete, physical space and time. Business dealings can occur across the globe, in an instant, without paper, pen, or face-to-face contact. But this remarkable technology does not come without risks. Like any new business terrain, cyberspace can be a legal minefield for the unprepared. What follows is an attempt to signal various areas of potential liability for persons conducting business in cyberspace, with an emphasis on practical suggestions to reduce exposure by anticipating trouble spots.

† Gordon & Glickson P.C., 444 North Michigan Avenue, Suite 3600, Chicago, Illinois 60611-3903. Brian Fagel, a recent graduate of The University of Chicago Law School, assisted in the preparation of this article.
II. TRANSACTING BUSINESS IN CYBERSPACE

A. MARKETING

1. Advertising

Cyberspace provides a vast array of marketing possibilities, many of which are being explored for the first time. Many companies are using the Internet as another medium for traditional forms of advertising; but the Internet is unique because there are virtually no restrictions on the amount of information transmitted and the feedback that can be received.¹ A company can provide a potential buyer with an overwhelming amount of product information, in the form of text, pictures, interactive activities, and video clips. The company can also track the frequency and manner in which different consumers navigate through the information, and thus gather data for future marketing efforts.

The fact that no centralized authority controls the Internet increases the advertiser's legal exposure. When there is no one entity responsible for everything, there is no one other than the advertiser who could be held responsible for a transmission. If an injured party wants to explore the possibility of legal relief (on the Internet, as opposed to on a paid online service, like Prodigy), there is no large corporate co-defendant with deep pockets to satisfy a judgment or to make a settlement payment. As is the case with the Internet in general, a company can very easily find itself on its own.

As such, advertisers on the Internet should be particularly careful about the information they are disseminating. The traditional legal risks of advertising remain in effect in cyberspace—copyright and trademark infringement, unfair trade or deceptive practices, consumer protection, defamation, privacy, publicity, and trade or product disparagement. Advertising on the Internet also introduces new legal risks. First, because online advertisements can be accessed worldwide, the question of international liability arises. For example, French law prohibits the use of comparison advertising,² and Iranian law prohibits the display, in advertisements, of women alone, or not fully covered. While it is unlikely that another country's jurisdictional reach will allow criminal liability to attach for the actions of a wholly national U.S. company, the possibility remains that U.S. companies doing international business may encounter new legal tangles when advertising online. Second, if online advertising contains "hyperlinks," which allow the user to jump from one page to a totally independent page, the advertiser providing the hyperlink could

². Carla Michelotti, Address at the Chicago Bar Association Luncheon (June 21, 1995) (Ms. Michelotti is the Senior Vice President and Associate General Counsel of the Leo Burnett Company).
be liable for actionable (e.g., false, defamatory, deceptive) content on the jumped-to page.

It is possible that an advertiser's potential legal exposure for international transmissions and hyperlinks may be decreased through the careful use of appropriate disclaimers—although the legal viability of such disclaimers has not yet been tested. To minimize liability, an advertiser should include a disclaimer on the same screen that actionable images or words appear. This disclaimer should warn the cyberspace surfer of the nature of the material contained on the underlying web pages. (Likewise, to avoid liability for material contained in hyperlinked pages, the disclaimer should appear adjacent to the hyperlink, cautioning the user against clicking on the highlighted words.) An example of one type of disclaimer (albeit not in a pure advertising context) appears on Penthouse Magazine's "Penthouse Internet" World Wide Web home page. The disclaimer, prominently displayed atop the page (yet below a digitized photograph of the current issue of Penthouse magazine), alerts the viewer that "Penthouse Internet contains sexually oriented adult material intended for individuals 21 years of age or older," and that "if you are accessing Penthouse Internet from any country or locale where adult material is specifically prohibited by law, go no further." The italicized words represent a hyperlink, leading the viewer to a page listing several countries which prohibit adult material.

The Penthouse example should provide the online advertiser with nothing more than a model for drafting a legally sound disclaimer; one major problem with Penthouse's disclaimer, from a legal standpoint, is the existence of numerous other access points to the prohibited material. That is, if a viewer enters the Penthouse site at an embedded page instead of the home page (which is not unlikely, if the viewer learns of the site via an online search engine), the viewer never sees the disclaimer. While the disclaimer may not actually halt the viewer from proceeding, the ease of entering the site without ever encountering the disclaimer could make the disclaimer legally worthless. This problem can be avoided by posting the disclaimer atop every page that provides, or provides links to, potentially actionable material.

Advertising about cyberspace—for example, print advertising for an online service provider—is subject to the same rules as traditional advertising. The recent "Howard Stern Case" is a prime example. Delphi Internet, an online service provider, used a photograph of radio talk show host Howard Stern in a print advertisement for a subscriber-participant debate on a bulletin board. The ad was placed soon after Stern declared

---

his candidacy for governor of New York. Stern sued Delphi under New York state law, claiming commercial misappropriation of his name and likeness. The court dismissed the action. The decision turned on the "incidental use exception" to the law, which allows a publisher of newsworthy events or matters of public interest to use a private person's name or photograph. The court easily adapted the law to cyberspace: "[T]he incidental use exception applies to all 'news disseminators,' not just newspapers and magazines." Online service providers, when engaged in public forum discussions, are no different than any other source of news:

Because Stern's name was used by Delphi to elicit public debate on Stern's candidacy, logically the subsequent use of Stern's name and likeness in the advertisement is afforded the same protection as would be afforded a more traditional news disseminator engaged in the advertisement of a newsworthy product.

This case represents the willingness of some courts to view cyberspace in realistic terms—as just another extension of the business tools with which we are all familiar. Many seemingly troublesome legal issues may be easily resolved when cyberspace is viewed as merely a complement to "real" space.

As companies now turn to the Internet and, specifically, the World Wide Web, to advertise, they are hurrying to be among the first to avail themselves of cyberspace's expansive and growing consumer pool. But eagerness could invite serious legal exposure if caution is not used. The following suggestions should help guide those interested in cyberspace advertising:

- Review existing advertising policies to determine whether they are adequate to cover cyberspace advertising.
- Require appropriate legal and other screening of all materials made available in cyberspace—and be aware of potential international legal exposure.
- Examine agreements with all cyberspace consultants and outsourcers to ensure that they are not authorized to modify or publish corporate materials which have not been screened.
- Educate all personnel involved in cyberspace advertising about the risks of liability and the requirements for screening.
- Include trademark, copyright notation, and other disclaimers.
- Establish a policy regarding hyperlinking, cross-linking, and referral agreements.
- Post disclaimers warning of potentially prohibited material prior to giving users access to such material.
- Review "advertising injury" insurance coverage.

5. Id. at 697 (citations omitted).

6. Id. at 698.
2. Selling: Money and Goods In Cyberspace

Countless goods and services are sold over the Internet, and the numbers continue to escalate. Aside from the standard warranty and misrepresentation claims that accompany physical sales transactions, Internet sales also raise the increasingly important issue of transmission security. The lack of a secure means of paying for a product over the Internet has been a major impediment to direct sales online.\(^7\) Shopping service networks, much like television's Home Shopping Club or QVC, have thus far relied on membership programs, where shoppers send in credit card data off-line and thereafter use passwords to purchase items.\(^8\) Alternatively, some Internet marketers simply provide an 800 number, forcing the consumer to close the deal offline. But numerous security services are cropping up, utilizing encryption systems to allow safe transmittal of credit card numbers.

The potential failure of an encryption system or a shopper's ignorance of the danger of transmitting a credit card number through unsecured cyberspace, makes the Internet user an easy target for fraud. Banks are most at risk from online credit card fraud. Under the Federal Reserve Board's Regulation E, a cardholder is only liable for the first fifty dollars in unauthorized charges, while the bank is liable for the rest.\(^9\) This may somewhat relieve the online shoppers' anxiety, but it has caused a flurry of activity by banks, who are attempting to create a secure encryption system. While efforts are underway by many companies to allow anonymous, safe monetary transactions over the Internet, until secure digital cash is commercially available, the best advice is to enter any online business transaction with caution.

On a similar note, corporate financial transactions—transactions involving businesses and/or financial institutions—have been occurring online for years. Wire transfers and electronic funds transfers are now commonplace, and major banks are changing their policies to promote even greater use of online processing.\(^10\) The ability to move digital money worldwide instantly raises numerous technical and security issues. The legal issues arising from corporate electronic financial transactions include potential liability for unauthorized payments, employee theft, consumer fraud, and tax consequences. The fraud and theft issues have been around for many years, with theft via computer being a vigor-

---

8. Id.
ously enforced criminal act.11 As electronic transactions become more prevalent, businesses, financial institutions, and individuals should be particularly cognizant of the potential legal and financial pitfalls.

Security issues aside, selling products over the Internet raises legal questions unique to cyberspace. As with online advertising, online selling has the potential to reach across the country, and even across the world. As Robert and Carleen Thomas, operators of a private adult bulletin board in California, recently learned, it is crucial to anticipate one’s audience prior to setting up shop. The Thomases, although operating in California, were convicted under the obscenity laws of Tennessee because their pornographic material was available in Tennessee, and was found to be obscene under the conservative local “community standards” of Tennessee.12 It is likely that other laws, in particular the laws regulating sales, could create differing results from jurisdiction to jurisdiction, thus creating a legal minefield for the uninformed online seller.

The following suggestions should help prevent problems when buying, selling, or sending money through cyberspace:

- Businesses or individuals intent on buying or selling products through cyberspace should avail themselves of the safest available means of transaction, using secure methods of encryption.
- Businesses selling products through cyberspace should be aware of laws regulating sales in all potential markets—nationally and abroad.
- Technical security policies should be updated to keep pace with current technology and practices.
- Consider the adequacy of financial reporting controls and compliance with accounting and auditing procedures and standards.
- Examine the potential need for special international security measures.
- Review insurance and bond coverage.

3. Direct Distribution: Digitizable Products

Additionally, businesses whose products and services can be digitized are distributing directly to their customers. Many software companies distribute demo versions, updates, patches, and sometimes full product over the Internet. The legal issues raised by electronic distribution include potential antitrust and unfair competition claims, franchise questions, agency issues, and virtually every other distribution law issue (as well as copyright, patent, and trademark issues, as discussed below). A few examples illuminate the sweeping range of questions that remain unanswered in this rapidly developing field.

12. See Pornography Conviction Alarms Users of Internet, CHI. TRIB., July 31, 1994, § 1, at 11.
Microsoft is eyeing the possibility of vastly increasing the volume of electronic software distribution, offering a program that could eventually wipe out many software middlemen and distributors while increasing net proceeds and channeling effectiveness for software developers. Software could be downloaded directly from the Internet, circumventing the necessity of in-store or mail-order purchasing. Other companies are investigating similar methods for distributing digitized recorded music, thus allowing consumers to purchase and download the contents of entire albums without entering a store. These distribution schemes could have a devastating effect on traditional distribution channels, and for this reason alone may be challenged as impediments to fair trade. It remains to be seen how the Justice Department, as well as the courts, will respond to the market impact of this distribution streamlining.

Another example of a troubling aspect of the online distribution of digitized products involves the question of export laws. Here the concerns mentioned previously, with regard to Internet access by an unforeseeable audience, are becoming a reality. Philip Zimmermann, who created and distributed online the highly popular encryption program “Pretty Good Privacy” (“PGP”), may soon be indicted for violating export regulations. Zimmermann made the program available on the Internet, where “international borders don’t exist.” As a result, it has been downloaded “countless times” by foreigners. Under United States export laws, cryptography tools, such as PGP, are treated the same as “munitions,” and thus exporters of such tools are subject to severe penalties. If convicted, Zimmermann could face up to five years in prison and a million-dollar fine. The fact that Zimmermann is potentially criminally liable for a seemingly legal activity demonstrates the often unforeseeable dangers involved in doing business in cyberspace.

In the area of online distribution of digitized products, the law is understandably undeveloped. Courts and federal officials are just beginning to grapple with and understand the possibilities of cyberspace. The following suggestions apply to anyone transmitting or receiving products online:

15. Id.
16. Zimmermann has established a legal defense fund to help pay his legal fees. Ironically, Zimmermann has suggested that contributors send credit-card donations via Internet e-mail, using PGP encryption. WWW page: Legal Issues, URL: http://www.math.ucla.edu/pgp/volume2/Legal Issues.html, created by Philip Zimmermann, viewed Nov. 15, 1995.
• For those uploading software, review licensing and intellectual property policies prior to making software universally available.
• For those uploading software, carefully assess scope of potential audience—as well as particular laws of jurisdictions in which software will be made available.
• For those downloading software, be aware of any licensing and intellectual property restrictions on use or dissemination of product.

B. Contracting

Traditional contract law presupposes a pen and paper—or, at the very least, a verbal agreement. Cyberspace eliminates all that. The thorny issues of offer, acceptance, and rejection are resurrected in a new form. With the recent move towards the consumerization of online transactions, enforceability becomes a complex question. In the past, businesses have negotiated "electronic trading partner" agreements, which posed fewer problems because parties initially executed a written, paper agreement establishing protocols for electronic authentication and digital signatures. But now, online contracting is moving toward a system where users simply log on, point, and click—and a contract is formed. The reliability and integrity of such an approach depends upon both technology (e.g., encryption and secure digital signatures) and changes in existing laws. Most state laws do not adequately address the use of digital records, as opposed to paper records. For example, state "quill pen" laws, requiring medical records to be written on paper, are still on the books. These laws are slowly changing, and contract law will likely adapt to our growing dependence on cyberspace transactions.

On the whole, cyberspace contracting should be undertaken with an eye on the formalities of traditional contract law—at least until electronic contracts become standard practice. Meanwhile, a number of pre-

17. Electronic trading partners allowed better customer service and the ability to "turn orders around quickly." David R. Dodge, Building a Firm Foundation with EDI; Electronic Data Interchange of Playtex Holdings Inc. and Playtex Apparel Inc., BOBBIN, Nov. 1993, at 83.


cautions should be taken to avoid the potential legal wrangles of online contracting:

- Assess the security and risk factors involved in a system of electronic contracting.
- Be familiar with local rules on contract establishment, and develop online contracting in accordance with such rules.
- Establish safety measures that liken the process to standard contract formation. For example: a) create a paper archive or confirmation record; b) make the acceptance process interactive to assure a bilateral contract; c) use “electronic trading partner” master agreements with regular customers; and d) include an opt-out process to allow negotiation.
- As with any business contract, but in particular with online contracts, review safety measures to ensure that only authorized employees enter into contracts on behalf of the company. Such measures could include: a) the use of passwords, the unauthorized use of which being grounds for dismissal; b) informing business associates of those employees authorized to enter into contracts; and c) establishing an internal tracking system.
- Evaluate the adequacy of liability insurance and bond coverage.

C. Transmitting and Receiving

1. Intellectual Property

Much of the recent legal activity surrounding the Internet has concerned intellectual property issues; this is not surprising, given the fact that the Internet is largely a forum for exchanging information. In cyberspace, information is transmitted in digitized form, making it cheap, easy, and fast to copy, with the copy being a perfect replica of the original. Sites for uploading information for others to download can be set up and broken down within twenty-four hours, with thousands of users making unauthorized copies during that time period. Software may even enter cyberspace before hitting the store shelves. It is difficult, if not impossible, to trace the source of copied digitized information, because there is no physical trail left: A copied piece of information can appear identical to an authorized version. When information—whether software, a document, an image, or a digitized film—is copied or transmitted without authorization, a potential violation of copyright, trademark, and patent laws is presented.

---

22. For example, test versions of Microsoft Windows 95 were available over the Internet long before it was released. Clinton Wilder, Highway Robbery, INFORMATION Week, Nov. 14, 1994, at 22. IBM's new operating system, OS/2 Warp, also became available over the Internet soon before or shortly after it was officially released. Id.
a. Copyright

Words, pictures, music and computer software are all subject to copyright laws, and all may be transmitted over computer networks. The Copyright Act provides copyright protection for "original works of authorship fixed in any tangible medium of expression." The copyright holder is provided with a host of exclusive rights pertaining to the copyrighted work, including: the right to reproduce the work; the right to prepare derivative works based upon the copyrighted work; the right to distribute copies of the work to the public; the right, when appropriate, to perform the work; and the right, when appropriate, to display the work. The copyright holder also has the exclusive right to authorize others to undertake any of these activities. Copyright infringement is a strict liability crime—innocent infringement is infringement nonetheless.

Courts have used various theories to impose copyright liability on cyberspace residents. First, they may consider the network operator a direct infringer of the copyright holder's exclusive rights. Second, courts may impose liability for contributory infringement on those who contribute to acts of direct infringement. Third, courts may impose liability on a theory of vicarious liability against those who control and benefit from the infringing acts of others.

Regarding direct infringement, a system operator has been found directly liable when copyrighted works were placed on his bulletin board. In Playboy Enterprises, Inc. v. Frena, the court addressed the liability of George Frena, who operated a subscription computer bulletin board service containing directories of adult photographs, some of which were copies of Playboy Magazine's copyrighted photographs. Frena conceded that the photographs were being downloaded by subscribers without Playboy's consent, but he claimed that subscribers had uploaded them and that he removed them as soon as he discovered them. Reading the exclusive right to "display" broadly, the court found him liable. Frena was found personally liable because he operated a bulletin board which

25. Id. § 102(a).
26. Id. § 106.
27. Id.
30. Id. at 1554.
31. Id.
32. Id. at 1556-57.
displayed unauthorized copies, despite the fact that he had not personally put the copies there. The court explained that copyright infringement is a strict liability offense, thus, Frena's lack of intent did not bar a finding of infringement.

If this case signals the reasoning courts will use in assessing cyberspace copyright infringement, then copyright holders will be afforded the same protection online as offline but, importantly, copyright rights can only be protected when copiers are caught, and the decentralized nature of the Internet unfortunately provides a limitless arena for un-enjoinable copyright violations. In other words, this court's logic—that direct copyright infringement is prohibited online—only has practical application when the prohibited use can be traced to the party responsible.

Regarding contributory liability, Sega Enterprises recently brought an action to enjoin the uploading and downloading of copyrighted computer game software by the operator of a bulletin board system. In Sega Enterprises Ltd. v. MAPHIA, the defendant sold devices which could be used to copy Sega video games, and also sold access to a bulletin board, where subscribers were encouraged to upload and download Sega games. The court held that the defendant would likely be held liable for contributory infringement, due to its "role in the copying, including provision of facilities, direction, knowledge and encouragement." Regarding the knowledge element, the court did not require the defendant to know exactly when the infringing uploading or downloading occurred, but found more general knowledge evidenced by the circumstances to suffice.

A possible defense to a finding of contributory liability exists, however, when a device used to commit infringing acts also has a commercially significant non-infringing use. In Sony Corp. v. Universal City Studios, the Supreme Court determined that the sale of copying equipment (in this case, video cassette recorders) does not constitute contributory infringement because the equipment is "capable of substantial non-infringing uses." Many online network providers have asserted that they should not be liable for contributory infringement because bulletin boards, like video cassette recorders, are capable of non-infringing use. Still, it remains to be seen whether this doctrine will be extended to cover online products and services.

34. Id.
36. Id. at 683-84.
37. Id. at 687.
38. Id. at 686-87.
Another possible defense involves the transnational nature of cyberspace. Because the Copyright Act has no extraterritorial effect, it does not reach unauthorized downloading that occurs in other countries. The viability of this defense is unclear. It has not yet been tested, nor is it entirely accurate from a technological standpoint. That is, in an international transmission, the transmitted material does not instantly move from point A to point B. Packets of data are transmitted from server to server across the network, with intermediate copies being created over the network during the course of transmission. If some of these intermediate copies reside on servers within the United States, a finding of infringement is possible.

As for vicarious liability, no court has yet held a system operator liable under this theory. Vicarious liability would apply if the operator is considered to have control over the infringer and has a direct financial interest in the infringing. Since system operators cannot control what their subscribers upload and download, many commentators argue that vicarious liability should not apply.

In addition to potential civil liability, the copyright infringer can also be criminally liable, but only if the infringing was done "willfully and for purposes of commercial advantage or private financial gain." Where more than one co-defendant acts for the profit of only one defendant, all may be culpable for criminal copyright infringement. In other words, a system operator need not profit from the infringing in order to be held liable. A system operator may also be liable for aiding and abetting the infringement of another. But, because the copyright infringer must intend to earn a profit in order to be held criminally liable, the system operator probably would not be indicted if he does not charge a fee.

b. Trademark

The Lanham Act provides a trademark registrant with the "exclusive right to use the registered mark in commerce on or in connection with the goods or services specified in the registration." Trademark violation can occur under two possible theories: Likelihood of confu-

---

40. See Subafilms, Ltd. v. MGM-Pathe Communications Co., 24 F.3d 1088 (9th Cir. 1994) (addressing the effect of the Copyright Act's territorial scope on the issue of contributory infringement in a non-computer software context).
mission or false designation of origin. In other words, the owner of the mark can prevent others from using confusingly similar marks, and from stripping off the identifying mark and identifying the goods as their own. A violation of trademark under the likelihood of confusion standard gives rise to a private right of action in favor of the registrant of the trademark. A violation under the false designation of origin standard, on the other hand, gives rise to a private right of action in favor of any person who "is or is likely to be damaged" by the false designation. Civil remedies include injunctive relief, destruction of counterfeit items, and, subject to the principles of equity, recovery of damages, to be trebled in cases where the infringement is intentional and extenuating circumstances do not exist.

The courts have already applied trademark law to cases of online commerce. In two recent cases, the bulletin board operators were liable for trademark violations (in addition to copyright infringement, as discussed above). In one case, the court found the defendant liable because the software programs were transmitted with plaintiff's marks on them. The court did not require the plaintiff to show that the users of the bulletin board were actually confused, because "once a product is put into commerce, confusion, mistake, or deception occurring at some future time is sufficient to establish liability for trademark infringement." In the second case, the court found the defendant liable for trademark infringement under both the false designation of origin and the likelihood of confusion theories, because some of the displayed photographs had plaintiff's mark on them, while others had the mark removed.

As under the Copyright Act, liability may be imposed under the Lanham Act for contributory infringement. However, contributory infringement under trademark law is narrower than it is under copyright law. One can be held liable for contributory trademark infringement only by intentionally inducing another to infringe, or by supplying goods to

---

46. The Lanham Act is violated by unauthorized "use in commerce [of] any reproduction, counterfeit, copy or colorable imitation of a registered mark ... [where] such use is likely to cause confusion, or to cause mistake, or to deceive." 15 U.S.C. § 1114(1).
47. 15 U.S.C. § 1125(a)(1) states that the Lanham Act is violated by "any person who ... in connection with any goods ... , uses in commerce ... any false designation of origin ... , which is likely to cause confusion, or to cause mistake, or to deceive."
49. Id. § 1125(a).
50. Id. § 1117.
52. Id. at 688.
53. Id.
54. Sony, 464 U.S. at 439 n.19 (citing "fundamental differences" between copyright and trademark law).
others while knowing or having reason to know that they will engage in acts of trademark infringement.

c. Patent

Patent law is relevant to online commercial transactions with regard to computer software because patent law comes into play when patented software is disseminated through cyberspace. While software has traditionally fallen under the protection of the Copyright Act, some companies have recently attempted to use patent law instead because patent law is often better suited to protecting the "methods" and "processes" excluded from the Copyright Act’s scope.\(^5\) In order for a product to be patented, three general requirements must be met. The product must be useful, novel and nonobvious "at the time the invention was made to a person having ordinary skill in [that field]."\(^6\) Anyone who makes, uses, or sells a patented invention in the United States during the life of the patent and without authority of the patent owner is an infringer of that patent.\(^7\) As in copyright and trademark law, there is liability for contributory infringement.\(^8\)

In reducing one’s potential liability under intellectual property law, the current state of the law in “physical” space should be a guide. The Internet, or any other mode of online dissemination, is not a domain of lawlessness—violations may be harder to uncover, but they are violations nonetheless. The following guidelines should help protect valuable intellectual property, as well as avoiding infringement of someone’s rights:

- Regularly audit software inventory to ensure all license fees have been paid.
- Educate employees regarding the need to respect intellectual property rights of third parties, through implementation of a frequently updated and circulated office technology policy.
- Review downloading license terms in online service agreements.
- Monitor the Internet to make sure intellectual property rights are not being infringed. Have employees monitor the Internet as well, and report any apparent infringements to management (as opposed to responding directly).
- Make sure all dissemination of intellectual property abides by registration and notice requirements of various laws.

\(^5\) 17 U.S.C. § 102(b). "In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work." \(Id.\)


\(^7\) 35 U.S.C. § 271(a).

\(^8\) \(Id.\) § 271(c).
Beware of international dissemination of intellectual property (beyond the scope of protection).

2. Defamation, Threats, and Obscenity

Intellectual property issues clearly are important to anyone conducting business in cyberspace. Three additional areas of potential liability for information dissemination in cyberspace exist: The transmission of defamatory statements, the transmission of threats, and the distribution of obscene materials. While these areas of liability are not unique to cyberspace, the free-form, loose nature of cyberspace culture often leads cyberspace residents to be looser with their tongues (or keyboards), thus increasing the likelihood of legal trouble. But, as with intellectual property, the laws of the land also apply to cyberspace.

a. Defamation

Defamation is a false communication that injures the reputation of another. Since every transmission over a computer network is potentially a communication of some sort, the potential for damage in cyberspace is high. Clearly, the one who posts the defamatory statement on the Internet (or online service) is liable. But even inadvertent disclosure of a false statement may result in a successful suit for defamation, which means that online service providers could be liable for defamatory messages posted by members of the public on online bulletin boards. The extent to which providers of an online forum can be held liable for defamatory statements uploaded by others remains undecided.

In one case, CompuServe, an online service provider, was held not liable for an allegedly defamatory statement posted on a bulletin board it carried, primarily because CompuServe did not edit the forum, but rather received it under contract from a separate content provider who uploaded the forum as a whole into CompuServe's system. The court considered CompuServe to be a distributor, rather than a publisher of the forum and thus only liable if it knew or had reason to know of defamatory uploaded content. What remains unclear is whether the existence of the third party content provider distinguishes this case from the ordinary sysop situation, where the service provider edits the forum itself. Also unclear is whether an online provider will become responsible for defamatory content once it receives notice of the content.

board. The court ruled that computer bulletin board operators generally should be treated as distributors under defamation law, but held that Prodigy was a special case. Because Prodigy touted its service as having editorial control superior to its competitors, Prodigy should be treated like a publisher—and could be held liable for defamation. The Prodigy case may solidify the following distinction: If you retain control over editorial content then, like a publisher, you have a corresponding duty to edit; but if you retain no control, you are viewed as a common carrier, without liability. Still unanswered is the question of one's duty to remove, after notice, any defamatory material.

What these cases demonstrate is that defamation for online liability draws a great deal from previous, non-cyberspace defamation law. The publisher/distributor distinction rests on common sense principles of editorial control: Service providers should make claims about online content with caution. Finally, it remains evident that persons publishing defamatory language (which merely involves communication to a third person who understands the language) will be liable in cyberspace just as in the physical world.

These cases also demonstrate a unique characteristic of cyberspace: The vast amount of unsubstantiated information floating around. The Internet provides an arena where statements with no factual basis appear as "news"—but reader beware. Much of what passes for news on the Internet is not news at all. Prodigy learned the hard way that online information is often relied upon. After the defamatory statement (which accused Stratton Oakmont and its President of criminal activity and fraud during the underwriting of Solomon-Page Group Ltd. stock) was published, that stock's price plummeted considerably. It is quite possible that the person who posted the statement (who, because of the nature of the Internet, may never be caught) had improper financial motives—he could be a short-seller. Until people are more wary of the non-factual nature of much online information, such market manipulation and other cyberspace fraud will continue to occur.

b. Threats

Not surprisingly, the law regarding online threats is the same as the law regarding "offline" threats: In order for a transmitted threat to be

65. Id.
actionable, it must be a "true threat."\textsuperscript{66} As such, a recent court quashed an indictment against Jake Baker, a University of Michigan student who sent private e-mail detailing his desire to do violence to young girls.\textsuperscript{67} The court reasoned that "Baker's e-mail messages, on which the . . . indictment is based, were not publicly published but privately sent . . . While new technology such as the Internet may complicate analysis and may sometimes require new or modified laws, it does not in this instance qualitatively change the analysis under the statute or under the First Amendment."\textsuperscript{68} Threats in cyberspace, then, are still subject to the same rules as threats mailed, published, or verbalized in physical space.

c. Obscenity

One trend in the recent worldwide shift toward cyberspace is the proliferation of online obscenity—in the form of profane bulletin board postings, uncensored chat groups, and pornographic digitized photographs and movies. One study suggests that pornographic pictures are the most transmitted item in cyberspace.\textsuperscript{69} Private e-mail is difficult to regulate under existing laws—at least in the specific instance of communicated threats. But legislators are currently working to increase the scope of regulation of obscenity on public areas of cyberspace, in a manner that has many First Amendment scholars and activists very worried.\textsuperscript{70} The U.S. Senate has already approved by an overwhelming majority a measure sponsored by Senator Jim Exon that imposes fines of up to $100,000 and prison terms of up to two years for "people who knowingly transmit indecent material over a computer network accessible to people under the age of 18."\textsuperscript{71} If the "Exon amendment" becomes law, online service providers are not the only cyberspace businesses in trouble: Employers could face liability for the publication of obscene material by their employees. Additionally, when pornographic materials are downloaded and digitally "pinned up" on computer screens, an unwary employer could become liable for sexual harassment (in promoting a hostile work environment).

\textsuperscript{68} Id. at 1390.
\textsuperscript{70} See Michael Smith, Senate OKs Strict Bill Regulating On-Line Sex, CHI. TRIB., June 15, 1995, at 15.
\textsuperscript{71} Id.
Cyberspace opens up more possibilities for liability based on claims of defamation, communication of threats, and obscenity. A few suggestions will help one steer clear of these legal problems:

- As with any material intended for publication, carefully check statements for truth prior to posting in cyberspace.
- Employers and online service providers should avoid making claims about screening capabilities.
- Do not rely on information posted in cyberspace, without consulting secondary sources.
- Do not do anything in cyberspace that is illegal in the physical world.
- Prohibit employees from downloading, transmitting, and possessing pornographic, profane, or sexually explicit materials while at work or while acting on the employer's behalf.
- Modify existing sexual harassment and discrimination policies to cover all electronic communications and data.

IV. COMPUTERS IN THE WORKPLACE

It is practically impossible to enter a modern office without encountering a computer. Computers are no longer used exclusively for word processing. Employee e-mail accounts, and even employee access to the Internet, are commonplace. But with widespread employee access to cyberspace, whether limited to e-mail or reaching beyond the office, numerous and assorted potential legal problems arise. The best policy here, whether advising a client or dealing with an in-house computer network, is, ironically, policy—the development of an Internet policy carefully crafted with all risks in mind. The policy must be formalized. The reasons for a policy will become evident upon elaboration of the many legal risks involved in workplace computer use.

A. PRIVACY

If employees have networking capability, then employers may wish to monitor computer communications (e-mail in particular). The law is not yet settled on the extent to which an employer can monitor its employee's e-mail. The issue may hinge on consent: Whether the employee has a reasonable expectation of privacy in the computer communications being monitored. At the very least, a business should obtain express consent, or warn employees of an intention to monitor e-mail, prior to accessing the e-mail accounts of employees. Establishing an e-mail policy is the first step in protecting an employer against possible liability, but implementation is the second. An employer's failure to

monitor e-mail, after instituting a monitoring policy, could unwittingly create an expectation of privacy.\textsuperscript{73}

Several federal and state laws exist regarding computer privacy, but they lack uniformity and consistency and are not comprehensive in the treatment of confidentiality and the protection of privacy. Under the Federal Electronic Communications Privacy Act ("ECPA"), the government and private citizens are generally forbidden to intercept electronic communications or access stored electronic communications, although a procedure does exist under the ECPA for the government to obtain necessary warrants and court orders, and exceptions exist exempting some private individuals from ECPA's general proscriptions.\textsuperscript{74} Under the ECPA, an employer, as the "provider" of the "electronic communications service," can monitor real-time transmissions of employee e-mail to the extent that such monitoring is a "necessary incident" to the provision of the e-mail service, or to the extent necessary to protect the employer's "rights or property."\textsuperscript{75} To the extent an e-mail is in "storage," though, an employer apparently has broader rights. The prohibition against accessing stored e-mail does not apply at all to the "person or entity providing a wire or electronic communications service."\textsuperscript{76} After accessing that stored e-mail, however, the employer cannot "divulge" it to others, except "as may be necessarily incident to the rendition of the service or to the protections of the [employer's] rights or property. . . ."\textsuperscript{77} In one case evaluating the propriety of a government search and seizure, private e-mail items addressed to individuals and residing on a bulletin board server were held to be "stored electronic communications" and so subject to the provisions of ECPA.\textsuperscript{78} But while the ECPA was passed specifically to deal with e-mail privacy, it is rarely invoked "due to widely conflicting interpretations of its directives."\textsuperscript{79}

Individual state laws do little to clarify the issue of e-mail monitoring. A host of laws exist which may or may not increase the employee's


\textsuperscript{75} 18 U.S.C. § 2511(2)(a)(i).

\textsuperscript{76} 18 U.S.C. § 2702(a)(1).

\textsuperscript{77} Id. § 2702(b)(5).


\textsuperscript{79} Jeffrey Rothfeder, Faking Liberties, NETGuide, Mar. 1995, at 79; see also Pallasch, supra note 73 (stating that "the [ECPA] has no bearing on a company’s monitoring of in-house e-mail").
protection against monitoring by the employer. Privacy protection depends in part on jurisdiction, as individual states have varying laws dealing with forms of computer misuse, including "computer fraud, computer trespass, interference with the use of computers and violation of privacy." 81

As often occurs in rapidly progressing fields of law, case law and legislation cannot keep pace with business's accumulating concerns. State law should be thoroughly investigated before advising a client on e-mail privacy, and the ECPA should also be considered for its applicability. But until more case law appears, or until legislators clarify the issue of e-mail and privacy, the best policy, again, is caution.

Finally, on a related issue, e-mail will be treated like any other written document when it comes to discovery. For example, the Federal Rules of Civil Procedure consider e-mail, as computer-stored information, to be discoverable under the same rules that pertain to tangible, written materials. 82 As for costs associated with retrieving discoverable e-mail, a recent case held that the defendant company maintaining the e-mail system must cover the costs of retrieval, although the scope of the discovery request should be narrowed to reduce the burden of retrieval. 83 The fact that the defendant's e-mail system was particularly costly to search, because of the limitations of the search software, was not a bar to the court imposing all search costs on the defendant, because "[p]laintiffs should not be forced to bear a burden caused by [the defendant's] choice of electronic storage." 84 As such, a company anticipating litigation would be wise to implement an efficient, cheaply-searchable e-mail system to avoidShouldering excessive search costs upon discovery of e-mail.

B. SECURITY AND ERRANT EMPLOYEES

Once an office becomes fully networked, the possibilities multiply that unauthorized employees, or non-employees, may access files and communicate with others on behalf of the company. Again, implementation of a strict technology policy will considerably limit a business's legal exposure. A system of confidential authorization codes or passwords should be imposed, with online business associates made aware of which employees (and passwords) are authorized to conduct business on the company's behalf. An internal account tracking system can be installed

83. Id.
84. Id. at *6-7.
to monitor online time and transmissions, but employees should be fully aware that they are being monitored. If employees have access to the Internet, that access should be limited in time and scope—to avoid claims of defamation against the company based on unauthorized statements seemingly made on the company's behalf. To avoid copyright infringement claims, employees should be restricted in the downloading of information, and software agreements should be checked to ensure the legality of all foreseeable employee uses. Cyberspace is becoming more complicated every day, but consistent attention to the possibilities of liability will limit the dangers of new technology.

Limiting liability in the workplace can be summed up in the following suggestions:

* Implement a specific, detailed office technology policy, covering all aspects of electronic communication.
* Only monitor employee e-mail with express consent—and be sure employees are fully aware when, how, and why they are being monitored.
* Implement a strict password-control system.
* Limit or prohibit employee use of publicly accessible cyberspace—and monitor their use, with express consent, if necessary.

V. CONCLUSION

The law is complex enough when we are dealing with known properties: Written documents, physical confrontations—the age-old stuff upon which all legal precedent is based. But the leap into the great void of cyberspace, a fuzzy world of connected computers, where everything is neither here nor there, has caught many off guard. Yet, the laws of cyberspace must follow some logical path, and must conform to our current conceptions of reality. We must be wary, but we must not forget that cyberspace is merely an extension of our physical selves. Behind every computer terminal, responsible for every keystroke, is just another person—and we are all still subject to the laws of the land, which always, eventually, adapt. As the legislatures and the courts struggle to keep up with technology, caution and common-sense should be our guiding principles.