# E-Commerce Law

*Edited by the Law Firm of Grimes & Battersby*

VOLUME 1

NUMBER 10

OCTOBER 2001

## FEATURES



## COLUMNS



## PRACTICE AID



ASPEN
LAW & BUSINESS

# Proving Publication in Cyberspace

**William R. Wohlsifer**

Increasingly, content published in digital format over the Internet creates legal rights and relationships. Internet content is forming the basis of numerous legal disputes, ranging from Internet fraud and defamation to simple breach of contract when a contract and its terms have been established through electronic commerce. Oddly enough, the actual electronic communication is the only true form of original evidence of such content or communication. When digital data is ultimately reduced to a tangible physical form, issues arise regarding its admissibility and reliability.

The essential problem with proving digital content is that what you see or rely on today may not exist tomorrow. Internet publications are not tangible and, therefore, defy traditional means of authentication.

## The Problem with Internet Publication

Although the growth and use of digital content has certainly exploded, this information is intangible, ephemeral, and constantly in flux. It can be frequently changed, updated, or deleted by its authors. In addition, it can be downloaded by a reader and altered on the reader's computer either by changing the content or by manipulating the time stamp indicating the date of the download. However, authentication can be accomplished by obtaining the evidence through neutral disinterested third-party authentication services. Such diligence will enhance the evidence's probative value and will contribute to maintaining social justice in alignment with technological advancement.

The magnitude of content published and disseminated daily over the Internet is enormous, and it continues to grow. The number of pages on the World Wide Web in 2000 was estimated to be in excess of one billion.[1] In the United States, e-commerce was estimated to exceed $235 billion in 2000 and $830 billion by 2005.[2] America Online subscribers alone spent $6.7 billion while shopping on the Internet during the first quarter of 2001.[3]

**William R. Wohlsifer** provides legal and business counsel through his offices in West Palm Beach, FL and Washington, DC. He can be reached at *willywo@bellsouth.net*.

Consumers and online viewers trustingly rely on the warranties and representations made within a Web site, while retailers rely on their disclaimers and click agreements. Meanwhile, insurance companies are writing exemptions and limitations into policies that exclude coverage for losses arising out of Internet exposure. Consequently, business clients are exposed to unforeseen risks and liability as a result of publishing content on the Internet.

Furthermore, with the advent of the Internet, countless bricks-and-mortar businesses, both large and small, have created Web sites that advertise their goods and services. Thus, "Mom and Pop" have become authors and publishers. Many also have become copyright and trademark infringers, being unaware of what they cannot reproduce without permission. Counsel should be aware and advise such clients that they will be held to the standards of a publisher and, accordingly, that they should be aware of and exercise the same due diligence as the traditional publishing community.

## Proffering Internet Evidence

In the traditional world of tangible documents, legal norms can be readily applied to show ownership or to offer admissible evidence of such material. Hardcopy of tangible writings and even recordings can be physically deposited with the US Copyright Office, a court clerk, or a private registry to establish authorship and publication. Rules of evidence can be applied to admit tangible documents into evidence. However, the transient nature of electronic communications results in new problems that require solutions.

For example, how can counsel defend against challenges to a client's claim to ownership in content appearing within the client's published Web site, especially when the content can be appropriated or misappropriated in its entirety with a simple click of a mouse? Are you confident that a copy of an electronic publication will be admitted into evidence in support of your client's defamation claim when opposing counsel objects to it as hearsay or as unreliable? What do you do when you return to the subject Web page and find the content you intended to proffer has disappeared

before you credibly captured and authenticated it? Is that professional negligence?

Are you prepared to overcome objections to introducing only portions of a Web site, even though it is beyond your means to capture the whole site? How do you introduce proof of content that is technologically unrecordable? Although almost anyone can capture and store a digital file on a tangible medium, such as a floppy disk or magnetic tape, and offer the medium as evidence of the existence of the embedded content, a number of deficiencies result when an interested party attempts to preserve cybercontent.

A Web site may include embedded graphic and sound files, the capturing of which may be beyond the technical capabilities of many users, their attorneys, and investigators. Counsel should be aware that data that appears on a monitor might not reside within the Web page or Web site; rather, it might be purposefully and legally generated and imposed by another server and another source, or it might be linked to a database that is not recordable by ordinary downloading processes. As the underlying technology of Web sites evolves, more technology-based objections become available and should be used when appropriate.

## Using Neutral, Disinterested Third-Party Services to Prove Internet Publication

Because the Internet is currently without a centralized publication recordation system, Internet content should be corroborated to enhance credibility and admissibility. In one instance, a court reporter documented Internet evidence by taking a sworn statement from a witness as she navigated the Internet. The attorney deposing the witness said, "Please tell the court reporter the URL you are typing at this time." The attorney then asked the witness to tell the court reporter which Web page the URL retrieved. Finally, the attorney asked the witness to print the Web page and directed the court reporter to attach the printout to the sworn statement. This method of authentication can be effective, but it is costly and cumbersome.

To overcome the technological challenges and objections, particularly the commonly used hearsay objection (based on the grounds that the Internet publication is an out-of-court statement offered for the truth of the matter asserted), counsel should be aware of independent disinterested third-party services that purport to authenticate Internet evidence for use in litigation as part of their regularly conducted business activities. Third-party authentication services help overcome objections to admissibility and always increase the weight of the proffered evidence. Such services are founded on the business records exception to the hearsay rule. Under Rule 803(6) of the Federal Rules of Evidence, "records of regularly conducted activity," such as a "memorandum, report, record, or data compilation, in any form of acts, events, conditions, opinions, or diagnoses, made at or near the time, by or from information transmitted by a person with knowledge, if kept in the regular practice of that business activity to make the memorandum report, record, or data compilation" are deemed credible and are not barred by the hearsay rule.

Cyberight Corporation (*http://www.cyberight.com*)[4] is one company that provides authentication services. Cyberight developed its Proof-of-Publication in Cyberspace process in response to the lack of a central depository and records custodian available to verify publication of text, images, and sounds appearing on the Web. The Cyberight process is modeled after the method sovereigns use to record liens on real property and to register copyrights and trademarks. In contrast to the method used by sovereigns in which the recording party provides the copy of the material, in the Cyberight process, a neutral, disinterested third party creates and records the original copy. Specifically, Cyberight captures, archives, indexes, and preserves an entire Web site offline in the same manner as court clerks assign book and page numbers to deeds and recorded liens. The entire Web site is printed and bound like a deposition transcript. Each Web page is followed by a printed page showing a table of links of all URLs associated with the particular Web page. The bound copies and a CD-ROM of the entire recorded Web site are sent to the requesting party, along with an affidavit from Cyberight's records custodian providing the predicate for the business records exception and attesting to the authenticity of the downloaded material.

When authenticating Internet content, it is important to capture the whole Web site to show the relevant hierarchy of the disputed information, the number of other Web pages that refer to the page(s) containing the subject content, and the links to other topics, products, or entities that are associated in any way with the subject matter. Such information will often allow counsel to expand a client's claim for damages by showing a broader scope of impact. The content should be captured from the site

available to the general public rather than obtained directly from the server or archive of the Web site's host. Capturing what was available to the public assures that the captured content is a true and correct copy of what was actually presented at the time of recording. The evidence can be obtained without discovery, without a court order, without costly invasion of a hard drive, and even without filing a legal action.

## Using Neutral, Disinterested Third-Party Services to Prove Digital File Creation

Several Internet-accessible companies, including FirstUse.com and Surety.com, authenticate third-party files by encoding a digital "fingerprint" into the submitting party's digital file. After the file is fingerprinted, the hash code is transmitted via a secure Internet connection to a remote server, where it can be stored for 10 years. When the fingerprint is matched to the third-party file, the date and time that the fingerprint was created is verified, thus providing a method for establishing the existence of a document at a given time, provided that the file is never changed, lost, or revised in any manner. Throughout the process, neither company copies or views the fingerprinted file.

There are several disadvantages to relying on digital fingerprinting alone. Encryption purports to prove *creation* of a file, but it does not establish whether the file was ever *published*. Fingerprinting is disfavored as proof of origination for two additional reasons: First, it fails to provide proof of who was in actual possession of the key when the fingerprint was created. The "key," usually being no more than a series of passwords and PIN codes, can be voluntarily shared or otherwise accessed by someone other than the key holder. Second, absent a land-based agreement that a digital fingerprint will be binding on the parties, it should not be given full effect under standard contract law.[5]

## Proving Warranties and Representations Made in Cyberspace Through Third-Party Endorsements

"The next phase of Internet endeavor will be about bringing order to the wild, wild Web [by replacing] the anonymity of the early Internet [with] a set of badges and labels that identify the netizens."[6] Businesses are increasingly subscribing to services that purport to acknowledge the credibility of or endorse their Web sites. A Web site subscribing to these services generally displays the third-party's icon on its homepage or privacy page. When the icon is clicked, a notice is displayed that corroborates or endorses certain representations being made by or pertaining to the subject Web site. Generally, the displayed notice actually resides in the third-party's server. Counsel should refer to these endorsements because they may support or rebut presumptions pertaining to the reasonableness of a viewer's reliance in the relevant Web content. Consider the following examples:

- The Better Business Bureau, at *BBBOnLine.org*, allows Web sites to display the "BBB OnLine Reliability Seal."
- Truste, at *Trust-e.org*, allows Web sites to display the Truste "Licensee Validation Page." This page advises online viewers that "Trust-e is an independent, non-profit initiative whose mission is to build users' trust and confidence in the Internet by promoting the principles of disclosure and informed consent."
- Good Housekeeping offers the *GoodHousekeeping.com* seal of approval, signifying that the site "Meets Standards for Good Housekeeping Web Site Certification."
- VeriSign.com's "The Sign of Trust on the Net" indicates that "All information sent to this site, if in an SSL session, is encrypted, protecting against disclosure to third parties."
- Gomez.com allows a Web site to claim that they are "Gomez Certified," which means that they meet the minimum standards for "shoppability" and that "the merchant has a reasonable Internet store."
- BizRate.com allows Web sites to display the "BizRate.com Report Card," which provides the e-store's profile and customer evaluations.
- WebAssured.com allows Web sites to display the WebAssured.com seal to "tell prospective customers that the site subscribes to ethical standards of conduct."

## Who Publishes the Internet?

The Internet is self-published. US Supreme Court Justice John Paul Stevens has written, perhaps in *dicta*, that "[a]ny person or organization with a computer connected to the Internet can 'publish' information.[7] 'Publishers' include government agencies, educational institutions, commercial entities, advocacy groups, and

individuals."[8] The uploading of files or Web pages is similar to the printing and distribution traditionally performed by large-scale book and music publishers. As a result of the ease of publication and distribution, the Internet inadvertently failed to include any form of notice of publication on Web sites.

Unlike Copyright Management Information (CMI), Web pages do not contain publication information. Publication notices appear on sound recordings (compact discs, cassettes, and their packaging) and in printed materials (books and magazines) in the form of the stated year of publication and the name and location of the publishing company, often accompanied by the publication notice symbol (℗). The notice of publication that appears with both sound recordings and printed matter appears in addition to the copyright notice and symbol (©) and documents the fact of publication. (Note: The inclusion of the geographical location claiming or indicating where a Web site purports to be published likely will resolve certain Internet-based jurisdictional issues.) The omission of such publication information makes it virtually impossible to prove the event of *past* Internet publication, absent a timely recording of the content from the World Wide Web by private citizens or companies that specialize in documenting such proof.

## The Fifth Intellectual Property

The World Wide Web possesses a new and unique form of protectable intellectual property. I refer to this phenomenon as the "fifth intellectual property." Historically, there have been three major forms of intellectual property—patents, trademarks, and copyrights—and subsets, such as trade dress and trade secrets. With the advent of the Internet, domain names have become a form of intellectual property in that domain names no longer serve simply as electronic addresses; rather, they have become clear identifiers of sources of goods or services, much like trademarks and service marks.

Web pages are similarly emerging as a form of intellectual property. An evolved Web page is often a combination of original works of authorship, borrowed and licensed works, extraneously imposed content, text, graphics, and sounds with look-and-feel and navigational features all compiled into a single medium. It is highly likely that such particularized combinations and compilations do not appear as a single form anywhere else but as Web pages. This frequently changing combination of proprietary and non-proprietary material is a form of intellectual property in and of itself. Copyright protection of this intellectual property depends on the owner's ability to prove publication in cyberspace, including significant changes to the Web site. Thus, a third-party Web capturing service should be used to corroborate the event of electronic publication.

## Is Content Displayed in Cyberspace Deemed Published?

It is unclear whether material posted on the Internet is deemed "published," as that term is used in US copyright law. The 1976 Copyright Act defines "publication" in part as "[t]he offering to distribute copies or phonorecords to a group of persons for purposes of further distribution, public performance or public display."[9] However, the "public performance or display of a work does not of itself constitute publication."[10] In this author's opinion, posting content on the Internet clearly falls within this definition of publication.

However, the US Copyright Office stated that one consideration should be whether the computer of the person viewing the Internet content is connected to a printer.[11] Register of Copyrights, Mary Beth Peters, indicated that downloading an entire Web site should constitute publication, but she believes it is unlikely that anyone downloads an entire site.[12] In the author's opinion, whether the viewing computer is connected to a printer or the full site is downloaded should have no effect on determining whether the online work is deemed published. Such scenarios cannot be reasonably proved; thus, the caveat is illusory. Further, a viewer can read the publication from the monitor and then respond to it, reasonably rely on it, or infringe it without either printing or downloading the displayed material. A better rule is to recognize that by the very nature of the World Wide Web, all content made available over the Internet is essentially being used in commerce and, as such, should be deemed "published."

Although proof and preservation of this "fifth intellectual property" can be obtained through formal copyright registration (and arguably through the common law), most Web sites in the United States are not registered with the US Copyright Office. On average, less than 600,000 statutory copyrights are obtained each year.[13] Of those 600,000 applications, only 180,000 are Form TX.[14] (Form TX refers to the form used for copyright application of text, the most likely application form to be used for a Web site). Of those 180,000, it is estimated that only 100 Web sites per week apply for copyright registration.[15] This is far below the immeas-

urable, but believed to be approximately 3 billion, Web pages and multi-million Web sites now published daily on the World Wide Web.

Registration with the US Copyright office greatly affects the rights of the content owner. For example, registration is necessary before an infringement action may be filed. If made before or within 5 years of publication, registration is *prima facie* evidence of the validity of the copyright and of the facts stated in the copyright certificate. Moreover, if registration is made within 3 months after publication of the work or prior to an infringement of the work, statutory damages and attorney's fees will be available to the copyright owner. Otherwise, only an award of actual damages and profits is available to the copyright owner. The year of publication may determine the duration of copyright protection for anonymous and pseudonymous works (when the author's identity is not revealed in the records of the Copyright Office) and for works made for hire. Thus, counsel should advise clients to register their Web sites with the US Copyright Office. For Web sites that change frequently, counsel should secure credible proof of publication in cyberspace and be aware of the availability of the following copyright registration options for Web sites:

- Serial registration (group registration for works updated weekly for up to three months under a single application);
- Newsletters registration (daily changes up to one month under a single application);
- Database registration (up to three months of traditional compilation database updates under a single application); and
- Derivative works registration (per each cumulative change to the prior registered Web site).

## Regulatory Compliance and Industry Standards

In response to the lack of unified standards regarding Internet publication, regulatory agencies, self-regulated trade associations, the legal community, and the business community are creating mechanisms to control content displayed on the Internet and imposing Internet publication standards. Consider the following:

- The Securities and Exchange Commission is seeking federal regulations designed to protect investors who are influenced by journalistic content appearing on the same Web page as broker-sponsored advertisements.[16]
- The FBI conducted a sting operation, known as "Operation Cyber Loss," during which it charged 88 people in 10 days with Internet fraud. Operation Cyber Loss was part of a nationwide investigation into schemes that victimized more than 56,000 people, causing losses in excess of $117 million through fraudulent Internet representations.[17]
- The Beer Institute promulgated a voluntary code that provides guidance to Institute members on the placement of advertisements in relation to the type of content presented on Web sites. The Institute's goal is to avoid advertising beer near content likely to be viewed by minors.[18]
- Lawyers increasingly rely on Web pages as evidence in court.[19]
- Over-the-counter software, such as Adobe's Web Capture, offers users the ability to record Web sites in a manner that may enhance the credibility of Internet evidence captured.[20]

## Conclusion

Counsel should use the utmost diligence to identify and capture evidence that is or was published on the Internet, and opposing counsel should aggressively challenge the proffering party to enable the fact-finder to fully consider the credibility of the downloaded evidence. The legal communities' commitment to thoroughly document the fact of Internet publication will ultimately curtail fraudulent Internet transactions, protect ownership rights in intellectual property, prove virtual contractual terms, provide online consumer protections, enhance confidence in electronic commerce, and advance social justice in the Internet's commercial environment. This can best be accomplished through the use of neutral, disinterested third parties that specialize in authenticating digital evidence or Internet publication. Proper capturing and authenticating of content that was published over the Internet facilitates the application of existing laws to cyberspace. With hard copy in hand, cyberspace can touch down to the ground.

## Notes

1. *The Internet and Computers*, World Almanac and Book of Fact 2001 (World Almanac and Education Group, Inc. 2001), at 566.
2. *Id.* at 567.

3. Staff Writers, "In Brief: AOL Time Warner" *The Washington Post*, May 24, 2001, at E5.
4. William R. Wohlsifer is one of the founders of Cyberight Corporation.
5. *See* Uniform Computer Information Transactions Act (UCITA) § 105 cmt 3 and § 503 cmt 4.
6. Sebastian Mallaby, *The Washington Post*, April 2, 2001.
7. Reno v. ACLU, 521 U.S. 844 (1997).
8. *Id.*
9. 17 U.S.C. § 101.
10. *Id.*
11. Circular 65, *Copyright Registration for Automated Databases,* US Copyright Office (June 1999).
12. Mary Beth Peters, US Register of Copyrights, Remarks at the Annual Meeting of the American Intellectual Property Law Association, October 2000.
13. Peter Vankevich, Head, Information Section, US Copyright Office, Results of FOIA Request, February 27, 2001.
14. *Id.*
15. Jeff Cole, Head of Literary Section, Examining Division, US Copyright Office, Remarks at the Annual Meeting of the American Intellectual Property Law Association (Oct. 2000).
16. Neil Irwin, "Finance Web Sites May Face Regulation," *The Washington Post*, May 24, 2001, at E4.
17. Tamra Santana, "FBI Charges 88 in Internet Fraud Sweep," *The Washington Post*, May 24, 2001, at E4.
18. Mary M. Luria and Craig M. Mersky, "Beer Advertising and Sweepstakes on the Internet," 6 *E-Commerce Law* 28 (June 2001).
19. James L. Dam, "Lawyers Are Getting Website Admitted as Evidence at Trial," *Lawyers Weekly USA*, May 28, 2001, at 1, 18.
20. Paul Bernstein, "Perform Litigation Tricks with Adobe Acrobat," *Trial*, at 90, 92 (Feb. 2001).