The Trouble with Authenticating Internet Postings and Other E-Evidence

By Matthew J. Kelly Jr. and William G. Kelly

The first questions concerning any proffer of evidence have always been and, for the foreseeable future, will remain: What is the evidence being offered to prove? Is it admissible for that purpose? Whether the evidence is a bloody glove purportedly from a crime scene or a printout from a since-vanished Internet web page, attorneys must always answer these questions. No matter how much money is spent developing sophisticated databases or doing computer searches, and regardless of how many litigation-support personnel are employed, unless these fundamental questions are sufficiently answered, no judge will consider, and no jury will ever see, that potential evidence. This article focuses on the admissibility of Internet postings and, more specifically, on how the foundation for evidence—authentication—remains important as electronic discovery in all its forms grows by leaps and bounds.

The Corporate Website
Consider a corporation’s website, where information can take a variety of forms. There are blatant advertisements that regale browsers with the benefits of a product or service. Often there are news and press-release pages that offer the latest reports on positive goings-on, such as quarterly earnings and sunny outlooks on potential sales. We can also find “blogs” and other interactive commentary sections where authorized (or, dangerously, unauthorized) representatives of the company answer questions or make statements on behalf of the company.

Each of these aspects of a website is potential fodder for litigation. For example, the blog or comments section might contain material misrepresentations of fact about a company looking to be acquired or misstatements about products for sale. A question might be posted on a seller’s website regarding atypical and unforeseen uses of a product: “I know your ladder says to not stand above this step, but I need to stand on top to reach the ceiling. Is that OK?” A company response could potentially turn an unforeseeable use into a foreseeable one, thereby also turning a safe product into a defective one: “Sure, go ahead and stand on your tiptoes!”

Admissibility: Gagliardi, Lorraine, and Other Significant Decisions
Printouts and other evidence of Internet postings are often offered to prove that the company has made a representation (whether admission of guilt, a showing of notice, or foreseeability of a potential problem) or a misrepresentation that another has acted upon to his or her detriment. But is such evidence admissible?

To be admissible, potential evidence must first be authenticated. “The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.” This requirement does not vanish simply because the evidence comes from an electronic source.

In a case involving the admissibility of Internet “chat room” transcripts, the Second Circuit has recently indicated that the bar is not necessarily high for the offering party. “The proponent need not rule out all possibilities inconsistent with authenticity, or to prove beyond any doubt that the evidence is what it purports to be.” Rather, the standard for authentication is one of “reasonable likelihood,” which is described as “minimal.”

The Gagliardi standard is forgiving not only in prose but also in practice. In Gagliardi, the defendant was accused of enticing a minor to engage in illegal sexual activity via Internet chat rooms. The government offered testimony by an informant as well as printouts of “chats” engaged in by the defendant. Both the informant and an FBI agent testified as to the printouts’ authenticity. To complicate matters, however, the government did not use the original version of the emails and chats. Instead, the government cut and pasted certain emails, chat-room lines, and other portions of Internet text into word-processing files, which, according to the defense argument, not only permitted improper editing by the government but also complete fabrication. Yet the Second Circuit gave the defense argument short shrift, holding that testimony by the informant

Matthew J. Kelly Jr.

William G. Kelly

Matthew J. Kelly Jr. is with Schnader Harrison Segal & Lewis LLP in New York, New York.

William G. Kelly is with Goldberg Segalla, LLP in White Plains, New York.
A court following Gagliardi could permit the jury to decide the authenticity of cut-and-pasted compilations of Internet evidence.

Gagliardi has serious implications for corporate litigation. A court following Gagliardi could permit the jury to decide the authenticity of cut-and-pasted compilations of Internet evidence—the common “it goes to weight, not admissibility” scenario—even if the web page or chat room no longer exists.

Not all jurisdictions admit this kind of evidence so easily. Some courts have held that testimony from a mere visitor to a website may not be enough to authenticate web page printouts. Examples are Internet Specialties West, Incorporated v. ISPWest, which held that printouts of third-party websites were properly authenticated by a visitor to a website who could not establish the accuracy of the printouts, and United States v. Jackson, which held that evidence taken from the Internet had not been properly authenticated where the offering party was unable to show that the information had been posted by the organization to which she attributed it.

Internet Specialties West and Jackson suggest that a party cannot personally authenticate a printed web page. Nor could a party authenticate the proffered Internet content merely by printing out—or worse, cutting and pasting excerpts from—blogs or other comment web pages, even if the party himself or herself had directly participated in the online conversation. Authorities like these suggest that to authenticate Internet content, testimony would be required either from the author of the content—that is, the webmaster who placed the content online—or from a blogger or browser of the content who possesses foundational knowledge sufficient to authenticate the entire content.

A case in point is Perfect 10, Incorporated v. Cybernet Ventures, Incorporated. In Perfect 10, the proponent declared that certain printouts, which contained appropriate web addresses and dates of printing, were true and accurate copies of Internet content. This declaration was deemed sufficient to authenticate the web pages. The court stated that if the proffered documents bear “circumstantial indicia of authenticity (such as the dates and web addresses that appear thereon)” and the declarant is credible, a court would likely find an adequate foundation.

These latter decisions, however, appear to have relied largely on the personal knowledge of the witness authenticating the proposed printouts. This focus reserves too much to the particular facts of the cases and does not necessarily offer a road map for authentication and admissibility.

In Lorraine v. Markel American Insurance Company, a 2007 decision from the U.S. District Court of Maryland, Chief Magistrate Judge Paul Grimm attempted to provide a road map for authenticating and admitting electronic evidence. The 101-page opinion explores various forms of electronic discovery, from chat room transcripts to email to website postings. Judge Grimm surveyed the range of decisions on the subject handed down by other courts, noting that courts can be quite harsh in their distrust of the Internet: “While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation.” Yet at times, courts can also be overly forgiving, as with Perfect 10’s “reduced evidentiary standard.”

Judge Grimm addressed evidentiary issues specific to websites, most notably “the possibility that third persons other than the sponsor of the website were responsible for the content of the postings.” This possibility, Judge Grimm noted, has caused some courts, such as the Seventh Circuit, to require the proponent to prove that the Internet host actually posted or authorized the posting of the statements sought to be admitted.

To provide clear guidance on introducing Internet postings into evidence, Judge Grimm adopted the three-step inquiry proposed by Gregory P. Joseph. The three questions to be posed are “(1) What was actually on the website? (2) Does the exhibit or testimony accurately reflect it? (3) If so, is it attributable to the owner of the site?” Judge Grimm also adopted the following factors for consideration: the length of time the data was posted on the site; whether other persons report having seen it; whether the data has remained on the website for the court to verify; whether the data is of a type ordinarily posted on that website or websites of similar entities (e.g., financial information from corporations); whether the owner of the site has elsewhere published the same data, in whole or in part; whether others have published the same data, in whole or in part; and whether the data has been republished by others who identify the source of the data as the website in question.

Judge Grimm posited that the authentication rules most likely to apply to Internet postings are Federal Rules of Evidence 901(b)(1) (witnness with personal knowledge), 901(b)(3) (expert testimony), 901(b)(4) (distinctive characteristics), 901(b)(7) (public records), 901(b)(9) (system or process capable of producing reliable results), and 902(5) (official publication). Whenever Internet evidence is proffered, attorneys should stop and consider which of these rules could be of service. Is a representative available who has personal
knowledge of the posting or of the business practice or technology that facilitated the posting? Was the posting from a government website or posted pursuant to city, state, or federal law? It is important to ask these questions and to address admissibility issues early on, even during the discovery process. “[A] failure to authenticate [Internet evidence] almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation.”

Use of Internet postings can take another form that has become significant, particularly in the trademark context. In In re IP Carrier Consulting Group, the Trademark Trial and Appeal Board analyzed the website “Wikipedia,” which is an online encyclopedia that is collaborative in nature, allowing anyone to edit the entries. In re IP involved the application for two trademarks, “ipiPICS” and “ipiPIPE.” The applications were rejected because the names were said to be merely descriptive of the services provided. On appeal, the applicant cited Wikipedia’s entry on “Internet Service Provider” to show that “ISP,” rather than “IP,” is the most common abbreviation for Internet service provider. Although the Board ultimately ruled against the applicant, the Board accepted this argument, relying on the Wikipedia pages as evidence.

In considering Wikipedia as proffered evidence, the Board recognized the “inherent problems regarding the reliability of Wikipedia entries” due to the fact that anyone with access to the Internet can edit the entries. The Board noted that Wikipedia itself gives notice that entries, particularly newer ones, are subject to misinformation, omissions, and unsubstantiated information that may require removal; accordingly, “like any online source, unfamiliar information should be checked before relying on it.” Notwithstanding, the Board stated that Internet evidence in general is admissible, especially in trademark cases. “[T]he information provided there [Wikipedia] is not so inherently unreliable as to render inadmissible any opinion that references it, especially when the opposing party may ‘apply the tools of the adversary system to his report.’” In admitting the Wikipedia postings into evidence, the Board recognized the importance of allowing both the non-offering party to rebut the evidence and the offering party to supply corroborating evidence from other reliable sources.

**Conclusion**

It is easy to get lost in a landslide of documents as electronic discovery continues to expand, and particularly as more litigants avail themselves of the amended federal rules on electronic discovery. It is also easy to expand factual investigations into the far reaches of the Internet. Yet we must remember that the Internet’s vast universe of information is only potential evidence, which, to be admissible, must be properly authenticated. All the old rules governing admissibility still apply, and attorneys must take pains to ensure that the potential evidence goes before the judge or jury; otherwise the Internet data, and potentially your case, will vanish faster than the click of a mouse.

**Endnotes**

1. Pizzi, R. Evio. 901(a).
2. U.S. v. Gagliardi, 506 F.3d 140, 150 (2d Cir. 2007) (internal quotation marks omitted) (citing U.S. v. Pluta, 176 F.3d 43, 49 (2d Cir. 1999)).
3. Gagliardi, 506 F.3d at 150 (citing Pluta, 176 F.3d at 49 and U.S. v. Tin Yat Chin, 371 F.3d 31, 38 (2d Cir. 2004)).
4. Id. at 150.
5. Gagliardi, 506 F.3d at 149–51.
6. Regarding websites that no longer exist or that have changed the content of their pages, there are Internet resources that store the history of a website’s changes, for example archive.org (http://www.archive.org/about/about.php). However, even if one were to access the content of a web page from a specific date in the past, foundational problems would still arise. A proponent would need to establish that this is how the website appeared on a given date (i.e., chain of custody), that it was in the control of the opposing party or a third-party on the precise day, and so forth.
8. 208 F.3d 633, 638 (7th Cir. 2000).
12. Id. at 534 (citing St. Clair v. Johnny’s Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774–75 (S.D. Tex. 1999)).
13. Jackson v. Perfect 10, 241 F.R.D. at 554–55 (citing Jackson, 208 F.3d at 638); see also Boim v. Holy Land Found. for Relief & Dev., 511 F.3d 707, 753 (7th Cir. 2007) (calling for caution regarding expert testimony that relies on information on third-party websites when expert has not offered foundation for conclusion that websites controlled by certain group).

Published in Proof, Volume 17, Number 2, Winter 2009. © 2009 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.