Internet And Email Evidence (Part 1)

Gregory P. Joseph
is principal of Gregory P. Joseph Law Offices LLC, New York. President, American College of Trial Lawyers (2010-11); Chair, American Bar Association Section of Litigation (1997-98); member, U.S. Judicial Conference Advisory Committee on the Federal Rules of Evidence (1993-99). Editorial Board, ***Moore's Federal Practice*** (3d ed.). Author, ***Modern Visual Evidence*** (Supp. 2011); ***Sanctions: The Federal Law of Litigation Abuse*** (4th ed. 2008); ***Civil RICO: A Definitive Guide*** (3d ed. 2010). The author wishes to express his gratitude to Professor Patrick L. Jarvis of the University of St. Thomas for reviewing technical aspects of this discussion and for his invaluable insights.

Gregory P. Joseph

The facts may be new, but the rules are familiar.

THE EXPLOSIVE GROWTH of the Internet, electronic mail, text messaging, and social networks is raising a series of novel evidentiary issues. The applicable legal principles are familiar — this evidence must be authenticated and, to the extent offered for its truth, it must satisfy hearsay concerns. The novelty of the evidentiary issues arises out of the novelty of the media — thus, it is essentially factual. These issues can be resolved by relatively straightforward application of existing principles in a fashion very similar to the way they are applied to other computer-generated evidence and to more traditional exhibits.

INTERNET EVIDENCE • There are primarily three forms of Internet data that are offered into evidence:

- Data posted on the website by the owner of the site or, in a social networking setting, the creator of a page on the site ("website data");
- Data posted by others with the owner's or creator's consent (a chat room is a convenient example); and
- Data posted by others without the owner's or creator's consent ("hacker" material).

The wrinkle for authenticity purposes is that, because Internet data is electronic, it can be manipulated and offered into evidence in a distorted form. Additionally, various hearsay concerns are implicated, depending on the purpose for which the proffer is made.

Authentication Of Website Data

Corporations, government offices, individuals, educational institutions and innumerable other entities post information on their websites, or on social networking websites, that may be relevant to matters in litigation. Alternatively, the fact that the information appears on the website may be the relevant point. Accordingly, courts routinely face proffers of data (text or images) allegedly drawn from websites. The proffered evidence must be authenticated in all cases, and, depending on the use for which the offer is made, hearsay concerns may be implicated.

The authentication standard is no different for website data or chat room evidence than for any other. Under Rule 901(a), "To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." *United States v. Simpson*, 152 F.3d 1241, 1250 (10th Cir. 1998); *Johnson-Wooldridge v. Wooldridge*, 2001 Ohio App. LEXIS 3319 at *11 (Ohio Ct. App. July 26, 2001).

In applying this rule to website evidence, there are three questions that must be answered, explicitly or implicitly:

- What was actually on the website?
- Does the exhibit or testimony accurately reflect it?
- If so, is it attributable to the owner of the site?

In the first instance, authenticity can be established by the testimony — or, under Federal Rule of Evidence 902(11) or (12), a certification — of any witness that the witness typed in the URL associated with the website (usually prefaced with "www"); that he or she logged on to the site and reviewed what was there; and that a printout or other exhibit fairly and accurately reflects what the witness saw. *See Johnson-Wooldridge v. Wooldridge*, supra. *See also, Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1154 (C.D. Cal. 2002); *Hood v. Dryvit Sys., Inc.*, 2005 U.S. Dist. LEXIS 27055, at *6-7 (N.D. Ill Nov. 8, 2005); *Ampex Corp. v. Cargle*, 27 Cal.Rptr.3d 863 (Cal. Ct. App. 2005); *Miriam Osborn Mem. Home Ass'n v. Rye*, 800 N.Y.S.2d 909 (N.Y. Sup. Ct. 2005). *But see, Alston v. Metropolitan Life Ins. Co.*, 2006 WL 3102970 (M.D.N.C. Oct. 27, 2006) (attorney affidavit held insufficient on summary judgment because attorney was ethically precluded from appearing as a witness in the case on behalf of his client and, therefore, was not an adequate affiant). This last testimony is no different than that required to authenticate a photograph, other replica or demonstrative exhibit. *See, e.g., ACTONet, Ltd. v. Allou Health & Beauty Care*, 219 F.3d 836, 848 (8th Cir. 2000) ("HTML codes may present visual depictions of evidence. We conclude, therefore, that HTML codes are similar enough to photographs to apply the criteria for admission of photographs to the admission of HTML codes"). The witness may be lying or mistaken, but that is true of all testimony and a principal reason for cross-examination. Unless the opponent of the evidence raises a genuine issue as to trustworthiness, testimony of this sort is sufficient to satisfy Rule 901(a), presumptively authenticating the website data and shifting the burden of coming forward to the opponent of the evidence. It is reasonable to indulge a presumption that material on a website (other than chat room conversations) was placed there by the owner of the site.

The opponent of the evidence must, in fairness, be free to challenge that presumption by adducing facts showing that proffered exhibit does not accurately reflect the contents of a website, or that those contents are not attributable to the owner of the site. First, even if the proffer fairly reflects

what was on the site, the data proffered may have been the product of manipulation by hackers (uninvited third parties). *See, e.g., Wady v. Provident Life & Accident Ins. Co. of Am.,* 216 F. Supp. 2d 1060, 1064-65 (C.D. Cal. 2002) ("Defendants have objected on the grounds that [counsel] has no personal knowledge of who maintains the website, who authored the documents, or the accuracy of their contents" — objections sustained). Second, the proffer may not fairly reflect what was on the site due to modification — intentional or unintentional, material or immaterial — in the proffered exhibit or testimony. Third, there may be legitimate questions concerning the ownership of the site or attribution of statements contained on the site. *See, e.g., Boim v. Holy Land Found.,* 511 F.3d 707 (7th Cir. 2007) *opinion vacated,* 2008 U.S. App. LEXIS 12925 (7th Cir. June 16, 2008), *aff'd in part, rev'd in part,* 549 F.3d 685 (7th Cir. 2008), *cert. denied,* 130 S.Ct. 458 (2009) (plaintiff's expert relied in part on Internet website postings in which the terrorist organization Hamas took credit for the murder of plaintiffs' decedent; held, the expert failed sufficiently to elucidate the basis for his conclusion that the website statements were attributable to Hamas and, therefore, the statements were insufficiently authenticated).

Detecting modifications of electronic evidence can be very difficult, if not impossible. That does not mean, however, that nothing is admissible because everything is subject to distortion. The same is true of many kinds of evidence, from testimony to photographs to digital images, but that does not render everything inadmissible. It merely accentuates the need for the judge to focus on all relevant circumstances in assessing admissibility under Fed. R. Evid. 104(a) — and to leave the rest to the jury, under Rule 104(b).

In considering whether the opponent has raised a genuine issue as to trustworthiness, and whether the proponent has satisfied it, the court will look at the totality of the circumstances, including, for example:

- The length of time the data was posted on the site;
- Whether others report having seen it;
- Whether it remains 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;
- Whether the data has been republished by others who identify the source of the data as the website in question.

A genuine question as to trustworthiness may be established circumstantially. For example, more by way of authentication may be reasonably required of a proponent of Internet evidence who is known to be a skilled computer user and who is suspected of possibly having modified the proffered website data for purposes of creating false evidence. *See, e.g., United States v. Jackson,* 208 F.3d 633, 638 (7th Cir. 2000), *cert. denied,* 531 U.S. 973 (2000) ("Jackson needed to show that the web postings in which the white supremacist groups took responsibility for the racist mailings actually were posted by the groups, as opposed to being slipped onto the groups' web sites by Jackson herself, who was a skilled computer user").

In assessing the authenticity of website data, important evidence is normally available from the personnel managing the website ("webmaster" personnel). A webmaster can establish that a particular file, of identifiable content, was placed on the website at a specific time. This may be done through direct testimony or through documentation, which may be generated automatically by the software of the web server. It is possible that the content provider — the author of the material appearing on the site that is in issue — will be someone other than

the person who installed the file on the web. In that event, this second witness (or set of documentation) may be necessary to reasonably ensure that the content which appeared on the site is the same as that proffered.

Self-Authentication

Government offices publish an abundance of reports, press releases, and other information on their official websites. Internet publication of a governmental document on an official website constitutes an "official publication" within Federal Rule of Evidence 902(5). Under Rule 902(5), official publications of government offices are self-authenticating. *See, e.g., United States ex rel. Parikh v. Premera Blue Cross,* 2006 U.S. Dist. LEXIS 70933, at *10 (W.D. Wash. Sept. 29, 2006); *Hispanic Broad. Corp. v. Educ. Media Found.,* 2003 U.S. Dist. LEXIS 24804, *20 n. 5 (C.D. Cal. Nov. 3, 2003); *E.E.O.C. v. E.I. Du Pont de Nemours & Co.*, No. Civ. A. 03-1605, 2004 WL 2347559 (E.D. La. Oct. 18, 2004); *Sannes v. Jeff Wyler Chevrolet, Inc.,* 1999 U.S. Dist. LEXIS 21748 at *10 n. 3 (S.D. Ohio March 31, 1999); *Tippie v. Patnik,* 2008 Ohio 1653, 2008 Ohio App. LEXIS 1429 (Ohio Ct. App. April 4, 2008) (dissenting opinion); *Harvard Mortg. Corp. v. Phillips,* 2008 Ohio 1132, 2008 Ohio App. LEXIS 1045 (Ohio. App. March 14, 2008) (concurring opinion). *See also, Elliott Assocs., L.P. v. Banco de la Nacion,* 194 F.R.D. 116, 121 (S.D.N.Y. 2000)); *Williams v. Long,* 585 F. Supp. 2d 679, 686-88 & n. 4 (D. Md. 2008); *Weingartner Lumber & Supply Co. v. Kadant Composites,* LLC, 2010 U.S. Dist. LEXIS 24918 (E.D. Ky. Mar. 16, 2010); *McGaha v. Baily,* 2011 U.S. Dist. LEXIS 73389 (D.S.C. July 7, 2011); *Scurmont LLC v. Firehouse Restaurant Grp.*, 2011 U.S. Dist. LEXIS 75715 (D. S.C. July 8, 2011). *But see State v. Davis,* 10 P.3d 977, 1010 (Wash. 2000). There is reason to believe, however, that *Davis* may be limited to its facts. *See State v. Rapose,* 2004 WL 585586, at *5 (Wash. Ct. App. Mar. 25, 2004) (unpublished opinion).

Similarly, newspaper articles taken from the Internet may be self-authenticating under Fed. R. Evid. 902(6) ("***Newspapers and Periodicals.*** Printed material purporting to be a newspaper or periodical"). The court may rely on distinctive newspaper and website designs, dates of publication, page numbers and web addresses. *Ciampi v. City of Palo Alto,* 2011 U.S. Dist. LEXIS 50245 (N.D. Cal. May 11, 2011).

Under the 2011 amendments to the Federal Rules of Evidence, newspaper and periodical materials that appear only on the web and not in hard copy — for example, a Reuters, Bloomberg, Dow Jones, or AP wire story that may never appear in print anywhere, or an article in an Internet-only publication like Slate — are also self-authenticating. Rule 902(6) (quoted in the preceding paragraph) provides for self-authentication of "printed material." Federal Rule of Evidence 101(b)(6), effective December 1, 2011, expands "printed" to include the purely electronic, by providing that: "[A] reference to any kind of written material or any other medium includes electronically stored information." Therefore, Rule 902(6)'s reference to "printed material" extends to information that never reaches hard copy but exists only in cyber space.

Judicial Notice

Under Federal Rule of Evidence 201(b) and (d), when requested, a court must take judicial notice of facts that are "not subject to reasonable dispute because it can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Government website data — particularly data that may be confirmed by the court's accessing the site — are subject to mandatory judicial notice under Rule 201. *See, e.g., Denius v. Dunlap,* 330 F.3d 919 (7th Cir. 2003) (district court abused its discretion in withdrawing its judicial notice of information from National Personnel Records Center's official website); *accord, Dingle v. BioPort Corp.,* 270 F. Supp. 2d 968 (W.D. Mich. 2003), *aff'd,* 388 F.3d