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), "The requirement of authentication...is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." *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 materials purporting to be newspapers or periodicals"). 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 (effective December 1, 2011), 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 in that it is...capable of accurate and ready determination by resort to 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 209 (6th Cir. 2004), *cert. denied*, 544 U.S. 949 (2005); *Scurmont*, supra, 2011 U.S. Dist. LEXIS 75715, at *49 n.11 ("Courts have... taken judicial notice, pursuant to Fed. R. Evid. 201, of information taken from government and media websites."); *Chisolm v. McElvogue*, 2011 U.S. Dist. LEXIS 40377, at *7 n.4 (D.S.C. Mar. 16, 2011) ("The Court may take judicial notice of court records and factual information located in postings on government websites"); *In re Katrina Canal Breaches Consol. Litig.*, No. 05-4182, 2008 U.S. Dist. LEXIS 86538, at 271-72 (E.D. La. Sept. 8, 2008) (collecting cases reflecting that federal courts may take judicial notice of governmental websites, including court records); *Renaissance Greeting Cards, Inc. v. Dollar Tree Stores, Inc.*, 405 F. Supp. 2d 680, 684 n.9 (E.D. Va. 2005), *aff'd*, 227 Fed. App'x 239 (4th Cir. 2007) *cert. denied*, 552 U.S. 951 (2007) (taking judicial notice of website information in trademark infringement action); *Wang v. Pataki*, 396 F. Supp. 2d 446, 448 n.2 (S.D.N.Y. 2005) (taking judicial notice of the contents of a website).

A court may take judicial notice of information publicly announced on a party's website, as long as the website's authenticity is not in dispute and it is capable of accurate and ready determination, within Fed. R. Evid. 201. *Doron Precision Sys., Inc. v. FAAC, Inc.*, 423 F. Supp.2d 173 (S.D.N.Y. 2006); *Town of Southold v. Town of East Hampton*, 406 F. Supp.2d 227 (E.D.N.Y. 2005), *aff'd in relevant part*, 477 F.3d 38 (2d Cir. 2007).

Chat Room Evidence

A proffer of chat room postings generally implicates the same authenticity issues discussed above in connection with website data, but with a twist. While it is reasonable to indulge a presumption that the contents of a website are fairly attributable to the site's owner, that does not apply to chat room evidence. By definition, chat room postings are made by third parties, not the owner of the site. Further, chat room participants usually use screen names (pseudonyms) rather than their real names.

Since chat room evidence is often of interest only to the extent that the third party who left a salient posting can be identified, the unique evidentiary issue concerns the type and quantum of evidence necessary to make that identification — or to permit the finder of fact to do so. Evidence sufficient to attribute a chat room posting to a particular individual may include, for example:

- Evidence that the individual used the screen name in question when participating in chat room conversations (either generally or at the site in question);
- Evidence that, when a meeting with the person using the screen name was arranged, the individual in question showed up;
- Evidence that the person using the screen name identified him- or herself as the individual (in chat room conversations or otherwise), especially if that identification is coupled with particularized information unique to the individual, such as a street address or email address;
- Evidence that the individual had in his or her possession information given to the person using the screen name (such as contact information provided by the police in a sting operation);
- Evidence from the hard drive of the individual's computer reflecting that a user of the computer used the screen name in question.

See generally, United States v. Tank, 200 F.3d 627, 630-31 (9th Cir. 2000); *United States v. Simpson*, 152 F.3d 1241, 1249-50 (10th Cir. 1998); *United States v. Burt*, 495 F.3d 733, 738-39 (7th Cir. 2007) *cert. denied*, 552 U.S. 1063 (2007); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1154 (C.D. Cal. 2002). *Compare, People v. Von Gunten*, No. C035261, 2002 WL 501612 (Cal. App. April 4, 2002) (assault prosecution; email excluded because, inter alia, unlike *Tank*, the exchange did not include facts known only to the witness and the fight participant and there

was no direct evidence linking the fight participant to the screen name).

With respect to the dialog itself, a participant in the chat room conversation may authenticate a transcript with testimony based on firsthand knowledge that the transcript fairly and accurately captures the chat. *Ford v. State,* 617 S.E.2d 262, 265-66, (Ga. Ct. App. 2005), *cert. denied,* 2005 Ga. LEXIS 789 (Ga. Sup. Ct. Nov. 7, 2005) ("we find this situation analogous to the admission of a videotape, which is admissible where the operator of the machine which produced it, or one who personally witnessed the events recorded, testifies that the videotape accurately portrayed what the witness saw take place at the time the events occurred. Here, [the witness] personally witnessed the real-time chat recorded in Transcript B as it was taking place, and he testified that the transcript accurately represented the on-line conversation. Under these circumstances, [his] testimony was tantamount to that of a witness to an event and was sufficient to authenticate the transcript") (internal quotations, citations and original brackets deleted); *Adams v. Wyoming,* 117 P.3d 1210, 1219 (Wyo. 2005) ("Although [the defendant] questioned the authenticity of this document under W.R.E. [Wyoming Rule of Evidence]. 901, the State's witnesses testified the entire dialogue was contained in the folder and no additions or deletions were made;" held, authenticity established; best evidence objection to use of computer printout also overruled because, under Rule 1001(3), '[a]n original is defined as including any computer printout or other readable output of data stored in a computer or similar device, which is "shown to reflect the data accurately.... The State's witness testified that the chat log exhibits were exact copies of the communication between the parties contained in the computer and thus, they were either appropriate computer 'originals' or duplicates which were properly authenticated. Whether they accurately reflected the contents of the instant messages sent between the parties was an issue for the jury to decide").

Internet Archives

Websites change over time. Lawsuits focus on particular points in time. The relevant webpage may be changed or deleted before litigation begins. Various Internet archive services exist that provide snapshots of webpages at various points in time. To the extent that those services, in the ordinary course of their business, accurately retrieve and store copies of the website as it appeared at specified points in time, the stored webpages are admissible. Generally, evidence from a knowledgeable employee of the Internet archive is sufficient to authenticate printouts as accurate representations of the website at issue at the relevant time. The testimony or certification should contain the same elements as set forth in the previous discussion of website data, with necessary modifications (e.g., the retrieval process may be automated, requiring authentication of the automated function, such as that it is used and relied on in the ordinary course of business and produces reliable results). *See, e.g., Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, 2004 U.S. Dist. LEXIS 20845, at *17-18 (N.D. Ill. Oct. 14, 2004) (Internet archive evidence properly authenticated via certification of archive employee, presumably offered pursuant to Fed. R. Evid. 902(11)); *St. Luke's Cataract & Laser Inst. v. Sanderson,* 2006 U.S. Dist. LEXIS 28873, at *5-*6 (M.D. Fla. May 12, 2006) (exhibits excluded for lack of authentication; held, "to show that the printouts from Internet Archive are accurate representations of the...websites [at issue] on various dates since 2000, Plaintiff must provide the Court with a statement or affidavit from an Internet Archive representative with personal knowledge of the contents of the Internet Archive website.... [A]n affidavit by...[a] representative of Internet Archive with personal knowledge of its contents, verifying that the printouts Plaintiff seeks to admit are true and accurate copies of Internet Archive's records would satisfy Plaintiff's obligation to this Court"); *Specht v. Google, Inc.,* 758 F. Supp. 2d 570 (N.D. Ill. Dec. 17, 2010) (authentication of screen shots from Internet

archive requires affidavit from knowledgeable employee of archive); *Audi AG v. Shokan Coachworks,* Inc., 592 F. Supp.2d 246, 278 (N.D.N.Y. 2008) (Internet archive search results require authentication of a 'knowledgeable employee' of the Internet archive); *St. Luke's Cataract & Laser Inst., P.A. v. Sanderson,* 2006 WL 1320242, at *2 (M.D. Fla. May 12, 2006) ("Plaintiff must provide the Court with a statement or affidavit from an Internet Archive representative with personal knowledge of the contents of the Internet Archive website").

Evidence that an Internet archive reflects that a site carried certain content may be corroborative of other evidence, such as a download from the site by a witness or testimony from a witness. Under Federal Rule of Evidence 104(a) and similar state provisions, in making its determination as to the admissibility of evidence, the court "is not bound by the rules of evidence except those with respect to privileges." With a proper foundation, Internet archive evidence may also form part of the basis of a forensic IT expert's testimony, in accordance with the strictures of Federal Rule of Evidence 703 and similar state rules.

Temporary Internet Files

When a computer user accesses the Internet, web browsers like Microsoft Explorer temporarily store all accessed images in a Temporary Internet Files folder so that, if the computer user attempts to view the same webpage again, the computer is able to retrieve the page much more quickly. Even deleted images in the temporary Internet files folder may be retrieved and viewed by an expert using an appropriate program, and expert testimony about this process is sufficient to authenticate the images. *See, e.g., United States v. Johnson,* 2006 U.S. Dist. LEXIS 62468, at *6-*8 (N.D. Iowa Aug. 31, 2006). The automatic creation of temporary Internet files has led to a holding that, in a prosecution for the possession of child pornography, "one cannot be guilty of possession for simply having viewed an image on a website, thereby causing the image to be automatically stored in the browser's cache, without having purposely saved or downloaded the image" (*United States v. Stulock,* 308 F.3d 922, 925 (8th Cir. 2002)), but that the same images may be admissible under Fed. R. Evid. 404(b) to establish the accused's knowledge and intent. *Johnson,* supra, 2006 U.S. Dist. LEXIS 62468, at *9-11.

Search Engines

The results generated by widely recognized search engines, like Google or Yahoo!, may be pertinent in litigation — for example, a trademark action to show dilution of a mark or a privacy/right of publicity action to show appropriation of a likeness. *See, e.g., McBee v. Delica Co.,* 417 F.3d 107, 112 (1st Cir. 2005).

Proper authentication would consist of testimony — or, under Federal Rule of Evidence 902(11) or (12), a certification — from a witness that the witness typed in the website address of the search engine; that he or she logged on to the site; the precise search run by the witness; that the witness reviewed the results of the search; and that a printout or other exhibit fairly and accurately reflects those results. The witness should be someone capable of further averring that he or she, or the witness's employer, uses the search engine in the ordinary course of business and that it produces accurate results. Further, the testimony or certification should reflect that the witness logged onto some of the websites identified by the search engine to demonstrate, as a circumstantial matter, that the particular search generated accurate results.

Social Networking Sites

Electronic conversations on social networking sites are authenticated in the same way that chat room evidence is generally authenticated. Thus, for example, a conversation, or chat, on a social networking site is sufficiently authenticated by testimony from a participant in that conversation that:

- He or she knows the user name on the social networking site of the person in question;
- That printouts of the conversation appear to be accurate records of his or her electronic conversation with the person; and
- A portion of the contents of the communications are known only to the person or a group of people of whom the person in question is one.

Ohio v. Bell, 2009 Ohio App. LEXIS 2112 (Ohio Ct. App. May 18, 2009); *People v. Goins*, 2010 WL 199602, at *1-2 (Mich. Ct. App. Jan. 21, 2010).

Separate from chats — comments posted more or less publicly on a page — social networks frequently permit members to send electronic messages to one another. Standing alone, the fact that an email communication is sent on a social network and bears a person's name is insufficient to authenticate the communication as having been authored or sent by that person. As discussed below in connection with email evidence generally, there must be confirming circumstances sufficient to permit the inference that the purported sender was in fact the author. *See, e.g., Commonwealth v. Purdy*, 945 N.E.2d 372 (Mass. 2011). *See also, People v. Fielding*, 2010 WL 2473344, at *3-5 (Cal. Ct. App. June 18, 2010), *review den.*, (Cal. Sept. 1, 2010); *People v. Clevenstine*, 891 N.Y.S.2d 511, 513-15 (N.Y. App. Div. 2009), *leave to appeal denied*, 14 N.Y.3d 799, 925 N.E.2d 937, 899 N.Y.S.2d 133 (N.Y. 2010); *Dockery v. Dockery*, 2009 Tenn. App. LEXIS 717 (Tenn. Ct. App. Oct. 29, 2009).

Profile pages on websites raise authentication issues analogous to those raised by websites and chats. An anonymous personal profile on a social networking site may be authenticated through an admission of the party posting it, a forensic review of the computer or other device of the person allegedly creating it, evidence from the social networking site, or circumstantial evidence sufficient to link it to the purported creator of the site. *Griffin v. State*, 19 A.3d 415, 427-28 (Md. 2011); *People v. Al-Shimary*, 2010 WL 5373826 (Mich. App. Dec. 28, 2010), *appeal denied*, 797 N.W.2d 155, 626-27, 629 (Mich. 2011); *People v. Padilla*, 2010 WL 4299091, at *19-20 (Cal. Ct. App. Nov. 1, 2010), *review denied*, (Cal. Feb. 16, 2011). In assessing authenticity, it is important to bear in mind that essentially anyone is free to create a profile page using whatever name they choose, so the mere existence of a profile page in someone's name does not necessarily reflect that the purported creator had anything to do with its creation. *Griffin*, supra.

Hearsay Issues With Internet Evidence

Authenticity aside, every extrajudicial statement drawn from a website must satisfy a hearsay exception or exemption if the statement is offered for its truth. *See United States v. Jackson*, 208 F.3d 633, 637 (7th Cir. 2000) ("The web postings were not statements made by declarants testifying at trial, and they were being offered to prove the truth of the matter asserted. That means they were hearsay"), *cert. denied*, 531 U.S. 973 (2000); *Savariego v. Melman*, 2002 U.S. Dist. LEXIS 8563, at *5 (N.D. Tex. May 10, 2002) (excluding on summary judgment "unauthenticated hearsay from an Internet search"); *Monotype Imaging, Inc. v Bitstream Inc.*, 376 F. Supp. 2d 877, 884-85 (N.D. Ill 2005) ("The Court refused to admit Exhibits 15 and 17 for the truth of the matter asserted in them because these exhibits are inadmissible hearsay. The Court admitted Exhibits 15 and 17 only for the limited purpose of proving that the diagrams in those exhibits were displayed on the respective websites on the dates indicated on the exhibits"); *United States v. Hernandez*, 2007 CCA LEXIS 183, at *27 (U.S. Navy-Marine Corps Ct. Crim. App. June 12, 2007) (error to admit evidence of telephone call usage drawn from databases available on the Internet to determine the time zones called and recipients' names because the Internet evidence "was categorically hearsay, and the [pro-

ponent] failed to establish any foundation bringing that source within any hearsay exception"); *Osborn v. Butler,* 3712 F. Supp.2d 1134 (D. Idaho 2010) (authenticated website evidence excluded as hearsay). Note, however, that there is rarely a hearsay problem with images derived from the Internet — just as there is rarely a hearsay problem with photographic evidence — because hearsay consists of extrajudicial statements offered for their truth. *United States v. Cameron,* 762 F. Supp.2d 152 (D. Me. 2011). Bear in mind, however, that a particular image may contain hearsay. *See, e.g. People v. Morgutia,* 2009 Cal. App. Unpub. LEXIS 5805 (Cal. Ct. App. July 17, 2009).

To establish that material appeared on a website, it is sufficient for a witness with knowledge to attest to the fact that the witness logged onto the site and to describe what he or she saw. That obviates any hearsay issue as to the contents of the site. *Van Westrienen v. Americontinental Collection Corp.*, 94 F. Supp.2d 1087, 1109 (D. Or. 2000) ("The only remaining question is whether the content of the website is hearsay under FRE 801.... Here, [plaintiff], by his own account, personally viewed the website and submitted an affidavit detailing specifically what he viewed. Therefore, the contents of the website are not hearsay for purposes of this summary judgment motion"); *Rapose,* supra, (unpublished opinion) (affirming admission of Internet and email documents because "each exhibit was identified and authenticated by the person testifying from personal knowledge of the contents").

Data Entry

Some website data is entered into Internet-readable format in the same way that a bookkeeper may enter numbers into a computer. This act of data entry is an extrajudicial statement — i.e., assertive nonverbal conduct within Rule 801(a) — which means that the product is hearsay, within Rule 801(c). Since each level of hearsay must satisfy the hearsay rule, under Rule 805 (Hearsay within Hearsay), the act of data entry must be addressed separately from the content of the posted declaration.

Data entry is usually a regularly conducted activity within Rule 803(6) (or, in the context of a government office, falls within Rule 803(8) (public records exception)). It also often falls within Rule 803(1) (present sense impression exception).

The real question about the data entry function is its accuracy. This is, in substance, an issue of authenticity and should be addressed as part of the requisite authentication foundation whenever a genuine doubt as to trustworthiness has been raised. If the foundational evidence establishes that the data have been entered accurately, the hearsay objection to the data entry function should ordinarily be overruled. *See also,* Rule 807 (residual exception).

Much Internet evidence does not involve data entry, in the sense described above. If the webmaster is simply transferring an image or digitally converting an electronic file into web format, that is a technical process that does not involve assertive non-verbal conduct within Rule 801(a) and is best judged as purely an authentication issue. The difference, analytically, is between the grocery store clerk who punches the price into the checkout computer (this is assertive non-verbal conduct), and the clerk who simply scans the price into the computer (non-assertive behavior). Only assertive non-verbal conduct raises hearsay issues and requires an applicable hearsay exception or exemption.

Business And Public Records

Businesses and government offices publish countless documents on their websites in ordinary course. Provided that all of the traditional criteria are met, these documents will satisfy the hearsay exception for "records" of the business or public office involved, under Rules 803(6) or (8). Reliability and trustworthiness are said to be presumptively established by the fact of actual reliance in the regular course of an enterprise's activities. *Johnson-Wooldridge v. Wooldridge,* 2001 Ohio App. LEXIS

3319, at *12-*13 (Ohio App. July 26, 2001) (Internet public record). (Recall that public records which satisfy Rule 803(8) are presumptively authentic under Rule 901(b)(7) (if they derive from a "public office where items of this nature are kept") and even self-authenticating under Rule 902(5).

As long as the website data constitute business or public records, this quality is not lost simply because the printout or other image that is proffered into evidence was generated for litigation purposes. Each digital data entry contained on the website is itself a Rule 803(6) or (8) "record" because it is a "data compilation, in any form." *See, e.g., United States v. Sanders,* 749 F.2d 195, 198 (5th Cir. 1984) (dealing with computerized records); *United States v. Catabran,* 836 F.2d 453, 456-57 (9th Cir. 1988) (same). Consequently, if each entry has been made in conformance with Rule 803(6) or Rule 803(8), the proffered output satisfies the hearsay exception even if it:

- Was not printed out at or near the time of the events recorded (as long as the entries were timely made);
- Was not prepared in ordinary course (but, for example, for trial); and
- Is not in the usual form (but, for example, has been converted into graphic form).

See, e.g., United States v. Russo, 480 F.2d 1228, 1240 (6th Cir. 1973), *cert. denied,* 414 U.S. 1157 (1974) (dealing with computerized records).

If the data are simply downloaded into a printout, they do not lose their business record character. To the extent that significant selection, correction, and interpretation are involved, their reliability and authenticity may be questioned. *See, e.g., Potamkin Cadillac Corp. v. B.R.I. Coverage Corp.,* 38 F.3d 627, 631, 633 (2d Cir. 1994) (dealing with computerized business records).

While website data may constitute business records of the owner of the site, they are not business records of the website hosting company. This is a service that may be provided by an Internet service provider (for example, America Online, MSN, ATT), and the cases frequently blend the two concepts in discussing the function of website hosting companies. "Internet service providers...are merely conduits.... The fact that the Internet service providers may be able to retrieve information that its customers posted...does not turn that material into a business record of the Internet service provider." *United States v. Jackson,* 208 F.3d 633, 637 (7th Cir. 2000), *cert. denied,* 531 U.S. 973 (2000) ("The Internet service providers did not themselves post what was on [the relevant] web sites. [Defendant] presented no evidence that the Internet service providers even monitored the contents of those web sites").

Rules 803(6) and (8) effectively incorporate an authentication requirement. Rule 803(6) contemplates the admission of hearsay, if its criteria are satisfied, "unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness." Rule 803(8) contains substantially identical language. This trustworthiness criterion parallels the Rule 901(a) requirement of "evidence sufficient to support a finding that the matter in question is what its proponent claims." As a result, untrustworthy proffers of business or public records may be excluded on hearsay as well as authenticity grounds. *United States v. Jackson,* supra.

Market Reports And Tables

Rule 803(17) excepts from the hearsay rule "Market quotations, tabulations, lists, directories, or other published compilations, generally used and relied upon by the public or by persons in particular occupations." A number of cases have applied this rule to commercial websites furnishing such data as interest rates, *Elliott Assocs., L.P. v. Banco de la Nacion,* 194 F.R.D. 116, 121 (S.D.N.Y. 2000), and blue-book prices of used cars. *See, e.g., State v. Erickstad,* 620 N.W.2d 136, 145 (N.D. 2000) (*citing, Irby-Greene v. M.O.R., Inc.,* 79 F. Supp.2d 630, 636

n.22 (E.D.Va. 2000)).This rationale plainly extends to the other sorts of traditional information admitted under Rule 803(17), such as tables reflecting the prices of such items as stock, bonds and currency; real estate listings; and telephone books.

ADMISSIONS • Website data published by a litigant comprise admissions of that litigant when offered by an opponent. *See, e.g., Van Westrienen v. Americontinental Collection Corp.,* 94 F. Supp.2d 1087, 1109 (D. Or. 2000); *Telewizja,* supra, 2004 U.S. Dist LEXIS 20845, at *16-17; *United States v. Porter,* 2006 U.S. App. LEXIS 14166, at *4-*5 (2d Cir. June 5, 2006), *cert. denied,* 550 U.S. 926 (2007); *United States v. Burt,* supra, 495 F.3d at 738; *Langbord v. U.S. Dep't of Treasury,* 2011 U.S. Dist. LEXIS 71779 (E.D. Pa. July 5, 2011); *Doctors Med. Ctr. of Modesto v. Global Excel Mgmt., Inc.,* 2009 U.S. Dist. LEXIS 71634 (E.D. Cal. Aug. 14, 2009); *Greater New Orleans Fair Hous. Action Ctr. v. St. Bernard Parish,* 648 F. Supp. 2d 805, 806 n.2 (E.D. La. 2009); *TIP Sys., LLC v. SBC Operations, Inc.,* 536 F. Supp. 2d 745, 756 n.5 (S.D. Tex. 2008).

Accordingly, even if the owner of a website may not offer data from the site into evidence, because the proffer is hearsay when the owner attempts to do so, an opposing party is authorized to offer it as an admission of the owner. *Potamkin,* supra, 38 F.3d at 633-34 (2d Cir. 1994) (dealing with computerized business records); *Momah v. Bharti,* 182 P.3d 455 (Wash. Ct. App. 2008) (posting self-laudatory article and other hearsay on website held an adoptive admission); *Mannatech Inc. v. Glycobiotics Int'l, Inc.,* 2007 U.S. Dist. LEXIS 91946, at *16 (N.D. Tex. Dec. 14, 2007) (customer testimonials contained on party's website admitted; without deciding the issue, the Court indicated that the testimonials could be admissible under Rule 801(d)(2) — presumably 801(d)(2)(A), (B) or (C) — citing *PharmaStem Therapeutics, Inc. v. ViaCell, Inc.,* 491 F.3d 1342, 1351 (Fed. Cir. 2007), for the proposition that: "[T]here is no prohibition against using the admissions of a party, whether in the form of marketing materials or otherwise, as evidence in an infringement action....").

However, the fact that a litigant posts on its website material from another website may not constitute an admission as to the contents of the second website, depending on the purpose of the posting. *Janus Capital Group, Inc. v. First Derivative Traders,* 131 S.Ct. 2296, 2305 n.12 (2011) (10b-5 suit against mutual fund advisor for misstatements by its client mutual fund; adviser posted allegedly fraudulent documents on its website: "Merely hosting a document on a Web site does not indicate that the hosting entity adopts the document as its own statement or exercises control over its content"); *Aikens v. County of Ventura,* 2011 Cal. App. Unpub. LEXIS 4986 (Cal. Ct. App. June 30, 2011) (county's posting of a hydrology, hydraulics, and sedimentation study performed by federal government did not constitute adoptive admission of the truth of the contents of the posted study).

The postings of a party in a chat room conversation constitute admissions, and the non-party's half of the conversation is commonly offered not for the truth of the matter asserted (although it could be) but, rather, to provide context for the party's statements, which comprise admissions. *Burt,* supra, 495 F.3d at 738-39.

Non-Hearsay Proffers

Not uncommonly, website data is not offered for the truth of the matters asserted but rather solely to show the fact that they were published on the web, either by one of the litigants or by unaffiliated third parties. For example, in a punitive damages proceeding, the fact of Internet publication may be relevant to show that the defendant published untruths for the public to rely on. *See, e.g., Van Westrienen v. Americontinental Collection Corp.,* 94 F. Supp.2d 1087, 1109 (D. Or. 2000). Or, in a trademark action, Internet listings or advertisements may be relevant on the issue of consumer confusion or purchaser understanding. *See, e.g., T. Marzetti Co.*

v. Roskam Baking Co., 2010 WL 909582, at *2 (S.D. Ohio March 11, 2010); *Microware Sys. Corp. v. Apple Computer, Inc.*, 2000 U.S. Dist. LEXIS 3653 at *7 n.2 (S.D. Iowa March 15, 2000); *Mid City Bowling Lanes & Sports Palace, Inc. v. Don Carter's All Star Lanes-Sunrise Ltd.*, 1998 U.S. Dist. LEXIS 3297 at *5-*6 (E.D. La. March 12, 1998). In neither of these circumstances is the website data offered for its truth. Accordingly, no hearsay issues arise. Similarly, when a chat room discussion is offered against a party who participated in it, the non-party's half of the conversation is commonly offered not for the truth of the matter asserted (although it could be) but, rather, to provide context for the party's statements, which comprise admissions. *Burt*, supra, 495 F.3d at 738-39.

Because chats are conducted using screen names, an exhibit may be prepared that substitutes real names (otherwise established) for screen names. The Seventh Circuit has ruled that altering otherwise-authenticated chat room postings by substituting real names for screen names does not implicate hearsay concerns but, rather, converts the exhibit into a demonstrative exhibit, admissible in the discretion of the court, subject to Federal Rule of Evidence 403. *Burt*, supra, at 738-39

Judicial Skepticism

As they were with computerized evidence prior to the mid-1990s, some judges remain skeptical of the reliability of anything derived from the Internet. *See, e.g., St. Clair v. Johnny's Oyster & Shrimp, Inc.*, 76 F. Supp.2d 773, 774-75 (S.D. Tex. 1999) ("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.... Anyone can put anything on the Internet. No web-site is monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on any web-site from any location at any time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules found in Fed. R. Evid. 807"); *Terbush v. United States*, 2005 U.S. Dist. LEXIS 37685, at *16 n.4 (E.D. Cal. Dec. 7, 2005), *aff'd in relevant part*, 516 F.3d 1125 (9th Cir. 2008) ("Information on internet sites presents special problems of authentication.... It has been recognized that anyone with sufficient hacking ability can put anything on the internet; no web-site is monitored for accuracy, and nothing contained therein is subject to independent verification absent underlying documentation").

While there is no gainsaying a healthy judicial skepticism of any evidence that is subject to ready, and potentially undetectable, manipulation, there is much on the web that is not subject to serious dispute and which may be highly probative. To keep matters in perspective, there is very little in the way of traditional documentary or visual evidence that is not subject to manipulation and distortion. As with so many of the trial judge's duties, this is a matter that can only be resolved on a case-by-case basis.

Part 2 of this article, which will appear in the April issue, will discuss authentication, hearsay, business records, hearsay within hearsay, admissions, state of mind, privilege, and authenticity, best evidence, and hearsay as they relate to text messages.