Internet And Email Evidence (Part 2)

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

Email evidence is subject to many of the same analyses that have traditionally applied to non-electronic evidence. But there are some important twists to know about.

PART 1 of this article examined the evidentiary challenges presented by the near-ubiquity of Internet evidence, discussing authentication of website data, self-authentication, judicial notice, chat room evidence, Internet archives, temporary Internet files, search engines, social networking sites, and the like. This Part will discuss the challenges raised by email evidence.

EMAIL EVIDENCE • Like Internet evidence, email evidence raises both authentication and hearsay issues. The general principles of admissibility are essentially the same since email is simply a distinctive type of Internet evidence — namely, the use of the Internet to send personalized communications.

Authentication

The authenticity of email evidence is governed by Fed. R. Evid. 901(a), which requires only "evidence sufficient to support a finding that the item is what the proponent claims it is." Under Fed. R. Evid. 901(b)(4), email may be authenticated by reference to its "appearance,

contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances." *See generally, United States v. Siddiqui*, 235 F.3d 1318, 1322 (11th Cir. 2000), *cert. denied*, 533 U.S. 940 (2001); *Bloom v. Commw. of VA.*, 542 S.E.2d 18, 20-21 (Va. Ct. App. 2001), *aff'd*, 554 S.E.2d 84 (Va. 2001)); *Manuel v. State*, 2011 Tex. App. LEXIS 7152, *17-18 (Tex. App. Aug. 31, 2011), *review denied*, 2011 Tex. Crim. App. LEXIS 1711 (Tex. Crim. App., Dec. 14, 2011).

If email is produced by a party opponent from the party's files and on its face purports to have been sent by that party, these circumstances alone may suffice to establish authenticity when the email is offered against that party. *See, e.g., Wells v. Xpedx*, 2007 U.S. Dist. LEXIS 67000, at *10 (M.D. Fla. Sept. 11, 2007) ("Documents produced during discovery are deemed authentic when offered by a party opponent"); *Sklar v. Clough*, 2007 U.S. Dist. LEXIS 49248 (N.D. Ga. July 6, 2007), *aff'd*, 319 Fed. App'x 798 (11th Cir. 2009) ("The e-mails in question were produced by Defendants during the discovery process. Such documents are deemed authentic when offered by a party opponent"); *accord, Bruno v. AT&T Mobility, LLC*, 2011 U.S. Dist. LEXIS 59795 (W.D. Pa. June 3, 2011); *Superhighway Consulting, Inc. v. Techwave, Inc.*, 1999 U.S. Dist. LEXIS 17910, at *6 (N.D. Ill. Nov. 15, 1999); *Dominion Nutrition, Inc. v. Cesca*, 2006 U.S. Dist. LEXIS 15515, at *16 (N.D. Ill. March 2, 2006).

This rule applies only to emails produced by a party opponent. The party offering an email into evidence cannot point to his or her own act of production as authenticating it. *Jimena v. UBS AG Bank, Inc.*, 2011 U.S. Dist. LEXIS 68560, at *13 (E.D. Cal. June 24, 2011) ("No party-opponent offered these documents in discovery so as to permit attribution of the identity and authenticity of the e-mails to [the defendants]").

Further, a party's failure to challenge as inauthentic emails sent by it or its counsel may be deemed sufficient evidence of the emails' authenticity. *Lemme v. County of Yuma*, 2006 U.S. Dist. LEXIS 76317, at *23 (D. Ariz. Oct. 19, 2006) ("Because Plaintiff and her counsel have the ability to authenticate those documents, but do not specifically challenge the authenticity thereof, the objections are overruled"). Authenticity may also be established by testimony of a witness who sent or received the emails — in essence, that the emails are the personal correspondence of the witness. *Read v. Teton Springs Golf & Casting Club, LLC*, 2010 U.S. Dist. LEXIS 134621 (D. Idaho, Dec. 14, 2010) (testimony from recipient of email sufficient to authenticated it); *In re Second Chance Body Armor, Inc.*, 434 B.R. 502, 504-05 (Bankr. W.D. Mich. 2010) (discussing Fed. R. Evid. 901: "[w]hen the document involved is an e-mail communication, a 'participant in, or recipient of, that communication' will generally be able to authenticate the communication, so long as the person 'was able to perceive who communicated what.'"); *EEOC v. Olsten Staffing Servs. Corp.*, 2009 U.S. Dist. LEXIS 88903, at *11 (W.D. Wis. Sept. 28, 2009) ("Testimony from someone who personally retrieved the e-mail from the computer to which the e-mail was allegedly sent is sufficient for this purpose"); *Fenje v. Feld*, 301 F. Supp. 2d 781, 809 (N.D. Ill. 2003), *aff'd*, 398 F.3d 620 (7th Cir. 2005) ("E-mail communications may be authenticated as being from the purported author based on an affidavit of the recipient"); *Maier v. Pac. Heritage Homes, Inc.*, 72 F. Supp. 2d 1184, 1190 (D. Or. 1999) ("Since Rockwell was a...recipient of the memorandum, his affidavit suffices to authenticate the exhibits[, including the memorandum].'); *Tibbetts v. RadioShack Corp.*, 2004 U.S. Dist. LEXIS 19835, at *44 (N.D. Ill. Sept. 30, 2004).

Testimony from a witness with knowledge that the emails were exchanged with another person comprises prima facie evidence of authenticity. *Ussery v. State*, 2008 Tex. App. LEXIS 741, at *22 (Tex. App. Jan. 30, 2008) (approving admission where the victim "testified, identifying the e-mail communications as fair and accurate copies of ac-

tual e-mails she exchanged with appellant. She thus provided testimony authenticating the e-mails"); *United States v. Gagliardi,* 506 F.3d 140, 151 (2d Cir. 2007) ("[T]he standard for authentication is one of 'reasonable likelihood'...and is 'minimal'...both the informant and Agent Berglas testified that the exhibits were in fact accurate records of [defendant's] conversations with Lorie and Julie. Based on their testimony, a reasonable juror could have found that the exhibits did represent those conversations, notwithstanding that the e-mails and online chats were editable"). If, however, an unsolicited email is received ostensibly from a sender whom the recipient has never been in contact with, mere testimony from the recipient may be insufficient to link it to the person whose name appears as sender. *Jimena,* supra, 2011 U.S. Dist. LEXIS 68560, at *15-16 (E.D. Cal. June 24, 2011) (Nigeria-based scam; testimony from recipient that he received an email purportedly from an individual at UBS, standing alone, held insufficient to link it to that person or to UBS where the recipient was never in contact with either other than through email traffic: "When a letter, signed with the purported signature of X, is received 'out of the blue,' with no previous correspondence, the traditional 'show me' skepticism of the common law prevails, and the purported signature is not sufficient as authentication, unless authenticity is confirmed by additional facts.... Likewise, when the recipient of an e-mail attempts to prove that the message was authored by a particular individual whose name appears in the header, such self-identification by designated sender is insufficient to establish authorship. Self-identification in an unsolicited e-mail supports authenticity, but is not, by itself, considered sufficient.... Here there is no signature of Clive Standish which any person with familiarity with the signature purports to identify") (internal quotes and citations omitted).

Testimony from a witness (at least, a hostile witness) that email appeared to be written in her "style" and that the content of the email — which was familiar to the witness — would by its nature be known to few others may suffice to constitute circumstantial evidence of authentication. *People v. Whicker,* 2007 Cal. App. Unpub. LEXIS 5197 (Cal. Ct. App. June 26, 2007) (among other things, the witness said she could not remember whether she had sent the email, although "I won't say I didn't because I don't remember for sure if I did or not;" she acknowledged that there were a few emails that she and the ostensible recipient sent back and forth; and she testified that the document "does look like my style of writing." Note: the recipient also testified that she remembered receiving the email).

It is important, for authentication purposes, that email generated by a business or other entity on its face generally reflects the identity of the organization. The name of the organization, usually in some abbreviated form, ordinarily appears in the email address of the sender (after the "@" symbol). This mark of origin has been held to self-authenticate the email as having been sent by the organization, under Fed. R. Evid. 902(7), which provides for self-authentication of: "***Trade Inscriptions and the Like.*** An inscription, sign, tag, or label purporting to have been affixed in the course of business and indicating origin, ownership, or control." *Superhighway Consulting, Inc. v. Techwave, Inc.,* 1999 U.S. Dist. LEXIS 17910, at *6-7 (N. D. Ill. Nov. 15, 1999). When the email reflects the entire email name of a party (and not just the mark of origin), it has been held to comprise a party admission of origin. *Middlebrook v. Anderson,* 2005 U.S. Dist. LEXIS 1976, at *14 n.7 (N.D. Tex. Feb. 11, 2005) (jurisdictional motion).

Independently, circumstantial indicia that may suffice to establish that proffered email were sent, or were sent by a specific person, include evidence that:

- A witness or entity received the email;
- The email bore the customary format of an email, including the addresses of the sender and recipient. *Ecology Servs. v. GranTurk Equip.,*

Inc., 443 F. Supp. 2d 756, 762 n.2 (D. Md. 2006) (excluding purported email which was not accompanied by an authenticating affidavit and which did not "bear the customary formatting of a printed e-mail message, indicating the sender, recipient, date, and subject");

- The address of the recipient is consistent with the email address on other emails sent by the same sender. *Shea v. State,* 167 S.W.3d 98, 105 (Tex. App. 2005);
- The email contained the typewritten name or nickname of the recipient (and, perhaps, the sender) in the body of the email. *Interest of F.P.,* 878 A.2d 91 (Pa. Super. Ct. 2005) ("He referred to himself by his first name"); *Commonwealth v. Capece,* 2010 Pa. Dist. & Cnty. Dec. LEXIS 506 (Ct. Com. Pl. Oct. 18, 2010);
- The email contained the electronic signature of the sender. *See, e.g., Sea-Land Serv., Inc. v. Lozen Int'l, LLC,* 285 F.3d 808, 821 (9th Cir. 2002) (email of one employee forwarded to party opponent by a fellow employee — containing the electronic signature of the latter — constitutes an admission of a party opponent);
- The email recited matters that would normally be known only to the individual who is alleged to have sent it (or to a discrete number of persons including this individual);
- The email was sent in reply to one sent to person ostensibly replying (the "reply letter doctrine"). *State v. Pullens,* 800 N.W.2d 202, 229 (Neb. 2011) ("Evidence that an e-mail is a timely response to an earlier message addressed to the purported sender is proper foundation analogous to the reply letter doctrine"); *accord, Varkonyi v. State,* 276 S.W.3d 27 (Tex. App. 2008), *review denied,* 2008 Tex. Crim. App. LEXIS 1634 (Tex. Crim. App. Oct. 29, 2008);
- Following receipt of the email, the recipient witness had a discussion with the individual who purportedly sent it, and the conversation reflected this individual's knowledge of the contents of the email.

See generally Siddiqui, supra, 235 F.3d 1318, 1322-23 (11th Cir. 2000). *See also United States v. Safavian,* 435 F. Supp. 2d 36, 40 (D.D.C. 2006) (emails admissible pursuant to (1) Fed. R. Evid. 901(b)(4) because they bear "many distinctive characteristics, including the actual e-mail addresses containing the '@' symbol, ... the name of the person connected to the address...[,] the name of the sender or recipient in the bodies of the e-mail, in the signature blocks at the end of the e-mail, in the 'To:' and 'From:' headings, and by signature of the sender [and t]he contents of the e-mails also authenticate them as being from the purported sender and to the purported recipient, containing as they do discussions of various identifiable 'matters," and (2) Fed. R. Evid. 901(b)(3), under which otherwise unauthenticated emails may be authenticated by the jury, which may compare them to the emails authenticated pursuant to Rule 901(b)(4)"). *State v. Taylor,* 632 S.E.2d 218, 231 (N.C. App. 2006) (quoting and following *Safavian*); *Dominion Nutrition, Inc. v. Cesca,* 2006 U.S. Dist. LEXIS 15515, at *16 (N.D. Ill. March 2, 2006) ("E-mail communications may be authenticated as being from the purported author based on an affidavit of the recipient; the e-mail address from which it originated; comparison of the content to other evidence; and/or statements or other communications from the purported author acknowledging the e-mail communication that is being authenticated") (quoting *Fenje*, supra; *Bloom*, supra; *Massimo v. State,* 144 S.W.3d 210, 215-16 (Tex. App. 2004); *Simon v. State,* 632 S.E.2d 723, 726-27 (Ga. Ct. App. 2006); *Swanton v. Brigeois-Ashton,* 2006 Wash. App. LEXIS 2067, at *6-7 (Wash. Ct. App. Sept. 18, 2006); cf. *Doe v. Nevada,* 2006 U.S. Dist. LEXIS 63971, at *37 (D. Nev. Sept. 7, 2006) (email deemed unauthenticated "absent proper authentication, or other evidence indicating that the email was sent or that [the alleged recipient] actually received the docu-

ment"); *Hardin v. Belmont Textile Mach. Co.,* 2010 U.S. Dist. LEXIS 61121, at *16 (W.D.N.C. June 7, 2010) ("Like in *Safavian,* the distinctive characteristics of Hardin's emails allow for their authentication. The e-mails in this case are provided on a printout that is in the familiar Microsoft Outlook format..., and they provide 'many distinctive characteristics, including…the name of the person connected to the address.'... The e-mails also discuss 'various identifiable matters' related to Hardin's employment ... which sufficiently authenticate the e-mails as being 'what its proponent claims.'"); *EEOC v. Olsten Staffing Servs. Corp.,* 657 F. Supp. 2d 1029, 1034 (W.D. Wis. 2009) ("even without a custodian, e-mails may be authenticated through the e-mail addresses in the headers and other circumstantial evidence, such as the location where the e-mail was found"); *Pullens,* supra (inclusion of sender's social security and telephone numbers); *Gary v. Combined Grp. Ins. Servs., Inc.,* 2009 WL 2868485, at *6 (N.D. Tex. Sept. 4, 2009) ("Because [the exhibits] have distinctive e-mail characteristics and because Plaintiff has stated in her affidavit that she wrote and sent these emails, the Court finds that they meet the threshold for authentication for summary judgment purposes"); *Cantu v. Vitol, Inc.,* 2011 U.S. Dist. LEXIS 11512, at *10-11 (S.D. Tex. Feb. 7, 2011) ("Courts have found that emails are properly authenticated by testimony as to their authenticity and distinctive characteristics of emails.... The emails have the distinctive characteristics of emails.... Vitol's human resources director, testified in a sworn affidavit that he collected the emails from Vitol's email system.... They are properly authenticated"); *Commonwealth v. Amaral,* 941 N.E.2d 1143 (Mass. App. Ct. 2011).

In evaluating circumstantial evidence of authenticity, there is a distinction to be drawn between an email address that is, on its fact, linked to a business (e.g., @pepsi.com) and an email address from a publicly available service (e.g., @gmail.com). The inference of authenticity is stronger in the former circumstance because, from the address, it appears that an employer has assigned an email address to an employee. Free public email services allow anyone to appropriate any username they choose, subject to availability. *See, e.g., Jimena*, supra ("The e-mail addresses used by the author of the Standish E-mails, clive standish@yahoo.com and customerservices@privateclientsubs.cjb.net, are also self-serving. In contrast to the e-mails discussed in *Safavian,* 435 F. Supp.2d at 40-41, the e-mail addresses here are not work e-mail addresses which are issued by an employer and include the employee's name in the e-mail address. Rather, they are from publicly available e-mail providers, available to and sendable by anyone"). As with all other forms of authentication, the testimony of a witness with knowledge is prerequisite to authenticate email. *Petroleum Sales, Inc. v. Valero Refining Co.,* 2006 U.S. Dist. LEXIS 90419, at *32 (N.D. Cal. Dec. 14, 2006), *aff'd on other grounds,* 304 Fed. App'x 615 (9th Cir. 2008) (emails excluded on summary judgment absent any evidence of the "accuracy or genuineness of the documents based on personal knowledge or otherwise"); *Ryan v. Shawnee Mission Unified School Dist.,* 437 F. Supp. 2d 1233, 1235-36 (D. Kan. 2006) (same; arguably dicta). It is insufficient to proffer email through a witness with no knowledge of the transmissions at issue, unless the witness has sufficient technical knowledge of the process to be in a position to authenticate the email through expert testimony. *See, e.g., Richard Howard, Inc. v. Hogg,* 1996 Ohio App. LEXIS 5533 at *8 (Ohio Ct. App. Nov. 19, 1996) (affirming exclusion of email where the authenticating witness "was neither the recipient nor the sender of the E-mail transmissions and he offered no other details establishing his personal knowledge that these messages were actually sent or received by the parties involved. Furthermore, the transmissions were not authenticated by any other means").

Transcriptions of email or text message exchanges, the originals of which have been lost through no fault of the proponent, may be authen-

ticated by testimony of a witness with knowledge that he or she transcribed them and that they accurately reflect the contents of the email or text message exchange. *See, e.g., United States v. Culberson*, 2007 U.S. Dist. LEXIS 31044 (E.D. Mich. April 27, 2007) (cell phone text messages transcribed before ISP deleted them); *Laughner v. Indiana*, 769 N.E.2d 1147 (Ind. Ct. App. 2002), *cert. denied*, 538 U.S. 1013 (2003) (AOL instant messages).

There are a variety of technical means by which email transmissions may be traced. *See, e.g., Clement v. California Dep't of Corrections*, 220 F. Supp. 2d 1098, 1111 (N.D. Cal. 2002), *aff'd per curiam*, 364 F.3d 1148 (9th Cir. 2004) ("major e-mail providers include a coded Internet Protocol address (IP address) in the header of every e-mail.... The IP address allows the recipient of an e-mail to identify the sender by contacting the service provider"). Therefore, if serious authentication issues arise, a technical witness may be of assistance. (Since authentication issues are decided by the court under Fed. R. Evid. 104(a), live testimony from such a witness is not essential; an affidavit or declaration may be equally effective.) This may become important, for example, in circumstances where a person or entity denies sending an email, or denies receipt of an email and has not engaged in conduct that furnishes circumstantial evidence of receipt (such as a subsequent communication reflecting knowledge of the contents of the email). *See, e.g., Hood-O'Hara v. Wills*, 873 A.2d 757, 760 n.6 (Pa. Super. Ct. 2005) (authenticity not established where person to whom email name belonged denied sending email and testified that problems in the past had required her to modify her email account on at least one prior occasion); *Ellison v. Robertson*, 189 F. Supp. 2d 1051, 1057 n.7 (C.D. Cal. 2002), *aff'd in relevant part*, 357 F.3d 1072 (9th Cir. 2004) ("Plaintiff has provided no evidence that AOL actually did receive the email. To the contrary, Plaintiff's former counsel states that while she received an acknowledgment of receipt for her April 17, 2000 email from [a local Internet provider], no such acknowledgment came from AOL"); *Carafano v. Metrosplash.com, Inc.*, 207 F. Supp. 2d 1055, 1072 (C.D. Cal. 2002), *aff'd on other grounds*, 339 F.3d 1119 (9th Cir. 2003) ("Plaintiff provides no evidence that [defendant Internet service] ever received the reply email in response to its welcome confirmation email").

Absent a showing of reason to disbelieve a sender's or recipient's representations concerning the authenticity of email, the court may decline to permit discovery into the computer system of the sender/recipient in light of the intrusion that forensic discovery would involve. *Williams v. Mass. Mut. Life Ins. Co.*, 226 F.R.D. 144, 146 (D. Mass. 2005).

While it is true that an email may be sent by anyone who, with a password, gains access to another's email account, similar uncertainties exist with traditional documents. Therefore, there is no need for separate rules of admissibility. *See, e.g., Interest of F.P.*, 878 A.2d 91, 95 (Pa. Super. Ct. 2005) (just as an email can be faked, a "signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationary can be copied or stolen. We believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework of Pa. R.E. 901 and Pennsylvania case law").

Hearsay

The hearsay issues associated with email are largely the same as those associated with conventional correspondence. An email offered for the truth of its contents is hearsay and must satisfy an applicable hearsay exception. *See, e.g., Hood-O'Hara*, supra, 873 A.2d at 760. Merely notarizing an email does not render it non-hearsay. *Shah v. Flagstar Bank*, 2007 Mich. App. LEXIS 2678 (Mich. App. Nov. 29, 2007) ("Although the signature of the vice-president on a copy of the email was notarized, it was not the equivalent of an affidavit because the author did not swear to the accuracy of his answers or indicate that his answers were based on personal knowledge"). A

certification satisfying Fed. R. Evid. 902(11) or (12), however, may operate to satisfy hearsay concerns, as those Rules provide an alternative means of satisfying the business records exception to the hearsay rule without the necessity of calling a live witness. As discussed below, the application of the business records exception to email is uneven.

The prevalence and ease of use of email, particularly in the business setting, makes it attractive simply to assume that all email generated at or by a business falls under the business records exception to the hearsay rule. That assumption would be incorrect, although the cases are not entirely in accord as to where precisely to draw the line between business record emails and non-business emails.

What Is A Business Record? Or A Present Sense Impression?

In *United States v. Ferber,* 966 F. Supp. 90 (D. Mass. 1997), the government offered into evidence a multi-paragraph email from a subordinate to his superior describing a telephone conversation with the defendant (not a fellow employee). In that conversation, the defendant inculpated himself, and the email so reflected. Chief Judge Young rejected the proffer under Fed. R. Evid. 803(6) because, "while it may have been [the employee's] routine business practice to make such records, there was no sufficient evidence that [his employer] required such records to be maintained.... [I]n order for a document to be admitted as a business record, there must be some evidence of a business duty to make and regularly maintain records of this type." *Id.* at 98. The Ferber Court nonetheless admitted the email, but under 803(1), the hearsay exception for present sense impressions. *See also State of New York v. Microsoft Corp.,* 2002 U.S. Dist. LEXIS 7683, at *9 (D.D.C. Apr. 12, 2002) ("While Mr. Glaser's email [recounting a meeting] may have been 'kept in the course' of RealNetworks regularly conducted business activity, Plaintiffs have not, on the present record, established that it was the 'regular practice' of RealNetworks employees to write and maintain such emails") (separately holding the present sense impression exception inapplicable); *Rambus, Inc. v. Infineon Techs. AG,* 348 F. Supp. 2d 698, 707 (E.D. Va. 2004) ("Email is far less of a systematic business activity than a monthly inventory printout"), quoting, *Monotype Corp. v. Intl. Typeface Corp.,* 43 F.3d 443, 450 (9th Cir. 1994); *Trade Finance Partners, LLC v. AAR Corp.,* 2008 U.S. Dist. LEXIS 32512 (N.D. Ill. Mar. 31, 2008), *aff'd,* 573 F.3d 401 (7th Cir. 2009) (email from defendant's principal recounting conversation with non-party held not a present sense impression but an inadmissible "calculated narration").

Cases finding email, in various circumstances, to constitute business records include: *United States v. Stein,* 2007 U.S. Dist. LEXIS 76201, at * 4-5 (S.D.N.Y. Oct. 15, 2007) (rejecting the contention that the proponent must "show — that the e-mails at issue were created pursuant to established company procedures for the systematic or routine making of company records." Held, "regularity of making such records and of the business activity is all that is required. Although the phrase 'business duty' appears frequently in Rule 803(6) cases, the defendants read the phrase too narrowly. The phrase 'business duty' is used interchangeably with phrases such as '[being] part of a business routine' or '[acting] in the regular course' to describe the requirement that the declarant be someone inside the business, not a third party"); *LeBlanc v. Nortel Networks Corp.,* 2006 U.S. Dist. LEXIS 17785, at *16 (M.D. Ga. Mar. 30, 2006) (finding emails likely to be admissible under the business records exception of Fed. R. Evid. 803(6)); *State v. Sherrills,* 2008 Ohio Ct. App. LEXIS 1662 (Ohio Ct. App. Apr. 24, 2008) (properly authenticated emails sent by criminal defendant established to be business records of IT Security Manager, who had custody and control of the server that captured all emails sent from the business) (note: this appears to be an authentication analysis framed in hearsay terms, which is understandable in light of the trustworthiness require-

ment of Rule 803(6)); *State v. Reynolds*, 2007 Iowa App. LEXIS 232 (Iowa App. Feb. 28, 2007), vacated, 746 N.W. 2d 837 (Iowa 2008) (email received by Bank from Federal Reserve in ordinary course of business admissible in light of evidence that "[t]he bank customarily kept these reports and relied upon them as part of its business").

Hearsay Within Hearsay

Because business records are written without regard for the rules of evidence, they commonly contain multiple layers of hearsay. Under Fed. R. Evid. 805, each layer of hearsay must independently satisfy an exception to the hearsay rule. Absent that, any hearsay portion of an email that is offered for the truth will be excluded. *See, e.g., Microsoft Corp.*, supra, 2002 U.S. Dist. LEXIS 7683 at *14 (D.D.C. April 12, 2002) ("'If both the source and the recorder of the information, as well as every other participant in the chain producing the record, are acting in the regular course of business, the multiple hearsay is excused by Rule 803(6). If the source of the information is an outsider, Rule 803(6) does not, by itself, permit the admission of the business record. The outsider's statement must fall within another hearsay exception to be admissible because it does not have the presumption of accuracy that statements made during the regular course of business have'") (citation omitted); *Trade Finance Partners*, supra (email from defendant's principal recounting conversation with non-party excluded; catchall exception of Fed. R. Evid. 807 not satisfied).

Admission Of Party Opponent

Under Fed. R. Evid. 801(d)(2), emails sent by party opponents constitute admissions and are not hearsay. *See, e.g., United States. v. Brown*, 459 F.3d 509, 528 n. 17 (5th Cir. 2006), *cert. denied*, 550 U.S. 933 (2007); *Safavian*, supra, 435 F. Supp. 2d at 43-44 (D.D.C. 2006); *MGM Studios, Inc. v. Grokster, Ltd.*, 454 F. Supp. 2d 966, 973-74 (C.D. Cal. 2006); *Riisna v. ABC, Inc.*, 219 F. Supp. 568, 572 (S.D.N.Y. 2002); *State v. Hibberd*, 2006 Wash. App. LEXIS 11151, at *24-25 (Wash. App. June 14, 2006). The email address itself, which reflects that it originates from a party, may be admissible as a party admission. *Middlebrook v. Anderson*, 2005 U.S. Dist. LEXIS 1976, at *14 (N.D. Tex. Feb. 11, 2005) (jurisdictional motion). *See also, Discover Re Managers, Inc. v. Preferred Employers Group, Inc.*, 2006 U.S. Dist. LEXIS 71818, at *22 (D. Conn. Sept. 28, 2006) ("e-mail correspondence with their e-mail addresses designating where they may be located [i.e., reflecting the authors' respective corporate employers' names after the @ symbol] combined with the subject matter of the e-mail itself" coupled with testimony of a witness with knowledge constitutes sufficient circumstantial evidence of the authors' agency relationships with their corporate employers for purposes of Fed. R. Evid. 801(d)).

Further, an email from a party opponent that forwards another email may comprise an adoptive admission of the original message, depending on the text of the forwarding email. *Sea-Land Serv., Inc. v. Lozen Int'l, LLC*, 285 F.3d 808, 821 (9th Cir. 2002) (one of plaintiff's employees "incorporated and adopted the contents" of an email message from a second of plaintiff's employees when she forwarded it to the defendant with a cover note that "manifested an adoption or belief in [the] truth" of the information contained in the original email, within Fed. R. Evid. 801(d)(2)(B)). If there is not an adoptive admission, however, the forwarded email chain may comprise hearsay-within-hearsay. *Rambus*, supra, 348 F. Supp. 2d at 707.

Excited Utterance

In dicta, the Oregon Court of Appeals has indicated that, in appropriate circumstances, an email message might fall within the excited utterance exception to the hearsay rule. *State v. Cunningham*, 40 P.3d 1065, 1076 n.8 (Or. Ct. App. 2002). (The federal excited utterance exception, contained in Fed. R

Evid. 803(2), is substantively identical to the Oregon exception, Oregon Fed. R. Evid. 803(2).)

State Of Mind

Email may be admissible to demonstrate a party's then-existing state of mind, within Fed. R. Evid. 803(3). *Safavian,* supra, 435 F. Supp. 2d at 44; *Dodart v. Young Again Prods.,* 2006 U.S. Dist. LEXIS 72122, *78-79 (D. Utah Sept. 29, 2006); *Leelanau Wine Cellars, Ltd. v. Black & Red, Inc.,* 452 F. Supp. 2d 772, 786 (W.D. Mich. 2006), *aff'd,* 502 F.3d 504 (6th Cir. 2007). Email may also be admissible to prove state of mind as non-hearsay under Fed. R. Evid. 801(c). *Brown,* supra, 459 F.3d at 528 n. 17 (5th Cir. 2006).

Other Non-Hearsay Uses

Not all extrajudicial statements are hearsay or, more precisely, need not be offered for hearsay purposes:

- The contents of an authenticated email may, for example, constitute a verbal act — e.g., constitute defamation or the offer or acceptance of a contract. *Middlebrook,* supra, 2005 U.S. Dist. LEXIS 1976, at *14 (N.D. Tex. Feb. 11, 2005) (jurisdictional motion); *Tibbetts v. RadioShack Corp.,* 2004 U.S. Dist. LEXIS 19835, at *44-45 (N.D. Ill. Sept. 30, 2004);
- An email may itself reflect the conduct at issue. *See Safavian,* supra, 435 F. Supp. 2d at 44 (certain emails themselves comprised "lobbying work" of defendant Jack Abramoff);
- Email may be received reflect (as opposed to assert) consumer confusion in a trademark infringement or unfair competition action. *Dodart,* supra, 2006 U.S. Dist. LEXIS 72122, *77-78;
- Email may be admitted to reflect the fact of third party statements. *Damon's Restaurants, Inc. v. Eileen K Inc.*, 461 F. Supp. 2d 607 (S.D. Ohio 2006) (consumer complaints in a franchise dispute); *United States v. Dupre,* 462 F.3d 131 (2d Cir. 2006) (non-testifying investors emails admitted in fraud prosecution to provide context for emails sent by defendant, which were admissions pursuant to Rule 801(d)(2));
- An email may also be admissible to show a non-party's state of mind. *See Trade Finance Partners,* supra (email from non-party to defendant admissible to show non-party "strongly disfavored new long term contracts with [defendant]").

Email Address

A party's chosen email address may itself be admissible as evidence of the party's state of mind. *See, e.g., Illinois v. Mertz,* 842 N.E.2d 618 (Ill. 2005), *cert. denied,* 549 U.S. 828 (2006) (murder prosecution; proper for trial court to admit evidence that defendant's email address was "Cereal Kilr 2000" because it provided insight into his frame of mind).

Privilege

Privilege issues — particularly, waiver issues — arise in a number of ways in connection with email.

First, a question of waiver may be presented depending on the security of (and reasonable expectation of privacy for) any email that is sent over a particular email system. Privilege may be lost by using an email system that is known by the user to be open to inspection by a person outside the privileged relationship. Thus, for example, an employee's use of a corporate computer to transmit or receive privileged communications waives the privilege when the employee is on notice that the employer reserves the right to review the communications. *United States v. Etkin,* 2008 U.S. Dist. LEXIS 12834 (S.D.N.Y. Feb. 19, 2008) (employees do not have a reasonable expectation of privacy in the contents of their work computers when their employers communicate to them via a flash-screen warning when they log on a policy under which the employer may monitor or inspect the computers at any time); *In re Asia Global Crossing, Ltd.,* 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005) (four-part waiver test: "(1) does the corpora-

tion maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?"); *Curto v. Medical World Communications., Inc.,* 2006 U.S. Dist. LEXIS 29387 (E.D.N.Y. May 15, 2006) (no waiver where employee deleted all her personal files, including emails, from two company-issued laptops before returning them to her employer, where the laptops were not connected to the corporate server, and there was no monitoring of her email traffic during her employment; irrelevant that, two years later, her employer's forensic computer consultant was able to retrieve deleted data from the laptops).

Second, waiver issues arise in connection with the logging of privileged emails in accordance with provisions such as Fed. R. Civ. P. 26(b)(5)(A), which requires a privilege log identifying all relevant information that is subject to a claim of attorney-client privilege or work product protection.

Failure to log a privileged email that its not produced may be held to waive the privilege otherwise attaching to the email. Compare *Nnebe v. Daus,* 2007 U.S. Dist. LEXIS 32981, at *3 (S.D.N.Y. May 3, 2007) ("Withholding privileged materials without including the material on a privilege log pursuant to Rule 26(b)(5) 'may be viewed as a waiver of the privilege or protection.' Fed. R. Civ. P. 26 advisory committee's note") with *C.T. v. Liberal School District,* 2007 U.S. Dist. LEXIS 38177, at *15 (D. Kan. May 24, 2007) ("While the court could find that plaintiff...has waived his claims of privilege due to the insufficiency of his privilege log, 'in the absence of bad faith on the part of the non-moving party in preparing the...privilege log,...the Court will decline to find waiver' and instead require the non-moving party to supplement his privilege log").

Even logging a privileged email may be insufficient to afford protection to attachments to the email, unless the attachments are themselves logged. *C.T. v. Liberal School Dist.,* 2008 U.S. Dist. LEXIS 5863, at *30-31 (D. Kan. Jan. 25, 2008) (where plaintiff listed a series of emails on his privilege log, but did not separately list the attachments, held: "any claim of privilege plaintiff might wish to raise as to those documents has been waived, and the attached documents, to the extent they are responsive to defendants' document requests, shall be produced. Plaintiff has had ample opportunity to list these attachments on...the privilege logs...").

Third, privilege may attach to otherwise unprivileged emails that are sent to an attorney in the course, and for the purpose, of obtaining legal advice. *Barton v. Zimmer Inc.,* 2008 U.S. Dist. LEXIS 1296, at *17 (N.D. Ind. Jan. 7, 2008) ("the very fact that non-privileged information was communicated to an attorney may itself be privileged, even if that underlying information remains unprotected." "As applied to e-mails, this means that even though one e-mail is not privileged, a second e-mail forwarding the prior e-mail to counsel might be privileged in its entirety...."). Nevertheless, the transmitted, inherently unprivileged email will have to be produced in some form. If it were not, that would raise serious spoliation issues.

Text Messages: Authenticity

Text messages are effectively emails sent by cell phone but they present unique problems because they are transitory. A recurring factual scenario involves one party transcribing or copying text messages only to realize thereafter that the texts have been purged by the carrier. Generally, testimony of accurate transcription, together with whatever other corroboration may be available, is sufficient prima facie evidence of authenticity. For example, in *United States v. Culberson,* 2007 U.S. Dist. LEXIS 31044 (E.D. Mich. April 27, 2007), a drug conspiracy prosecution, the DEA executed a search warrant to obtain, inter alia, the defendant's cell phone. The DEA agent found text messages found on the

phone. He testified that he accurately transcribed all texts verbatim, including the time, date and all senders and recipients. He did not immediately print out the texts and, two weeks later, when the agent reviewed the phone again, he realized that the contents were no longer stored on it. A subpoena served on the carrier was fruitless because the carrier had purged the texts from its system as well. The government sought to introduce the written transcript as evidence at trial, and the defense objected because it did not have an opportunity to review the original emails. The *Culberson* Court held that, under the liberal standards of Fed. R. Evid. 901(a), the transcription was held sufficiently authenticated by the testimony of the agent, one of the co-conspirators, and (iii) perhaps other co-conspirators as to the accuracy of the transcription.

Otherwise, text messages are largely authenticated in the same way as emails. *Manuel v. State*, supra ("An e-mail is properly authenticated if its appearance, contents, substance, or other distinctive characteristics, taken in conjunction with circumstances, support a finding that the document is what its proponent claims.... Characteristics to consider in determining whether e-mail evidence has been properly authenticated include (1) consistency with the e-mail address in another e-mail sent by the alleged author; (2) the author's awareness, shown through the e-mail, of the details of the alleged author's conduct; (3) the e-mail's inclusion of similar requests that the alleged author had made by phone during the time period; and (4) the e-mail's reference to the author by the alleged author's nickname.... Text messages can be authenticated by applying the same factors."); *accord State v. Thompson,* 777 N.W.2d 617 (N.D. 2010) (relying on email authentication case law to analyze admissibility of text messages).

Like email, text messages have certain seemingly self-authenticating features, like the sender's cell phone number, which may be translated into a name, as by action of the recipient. But because, like email, texts could be generated by a third party, these features are generally considered circumstantial evidence of authenticity to be considered in the totality of the circumstances. *See, e.g., State v. Eleck*, 23 A.3d 818, 821 n.4 (Conn. App. Ct. 2011), *appeal granted,* 30 A.3d 2 (Conn. 2011) ("Typically, electronic messages do have self-identifying features. For example, e-mail messages are marked with the sender's e-mail address, text messages are marked with the sender's cell phone number, and Facebook messages are marked with a user name and profile picture. Nonetheless, given that such messages could be generated by a third party under the guise of the named sender, opinions from other jurisdictions have not equated evidence of these account user names or numbers with self-authentication. Rather, user names have been treated as circumstantial evidence of authenticity that may be considered in conjunction with other circumstantial evidence"); *Commonwealth v. Koch*, 2011 Pa. Super. LEXIS 2716, at *15-16 (Pa. Super. Ct. Sept. 16, 2011) ("In the majority of courts to have considered the question, the mere fact that an e-mail bears a particular e-mail address is inadequate to authenticate the identity of the author; typically, courts demand additional evidence. Text messages are somewhat different in that they are intrinsic to the cell phones in which they are stored.... However, as with e-mail accounts, cellular telephones are not always exclusively used by the person to whom the phone number is assigned").

Testimony from a participant in the exchange is probative, subject to the caveat that there must be sufficient evidence to permit the conclusion that the exchange is with the relevant person. *See, e.g., Adamah v. Tayson* (*In re E.D.T.*), 2010 U.S. Dist. LEXIS 54172, at *9-10 (E.D.N.Y. May 27, 2010) ("Even if they were not independently authenticat-

ed by the service provider or by a forensic specialist, Adamah's testimony concerning the text messages was sufficient to establish their authenticity"); *accord Sanders v. Mohtheshum*, 2011 U.S. Dist. LEXIS 145572 (D. Colo. Dec. 19, 2011).

Summarized excerpts of text message exchanges have been admitted on the basis of foundational testimony from a witness with knowledge that the excerpts are accurate, even where the full texts are available. The opponent's remedy is to compel introduction of the remainder of the messages, under Fed. R. Evid. 106, if the remainder ought in fairness be considered contemporaneously with it. *United States v Hunter*, 266 F. App'x 619, 621-22 (9th Cir. 2008), *cert. denied*, 554 U.S. 929 (2008).

Text Messages: Best Evidence

Transcriptions of text messages have been held not to violate the best evidence rule if the proponent satisfies Fed. R. Evid. 1004(a), which provides that an original is not required when "all the originals are lost or destroyed, and not by the proponent acting in bad faith...." *See, United States v. Culberson*, 2007 U.S. Dist. LEXIS 35276 (E.D. Mich. May 15, 2007) (holding that the defendant failed to carry his burden of establishing bad faith and that the DEA agent's testimony that the emails were unavailable, and that they could not be obtained from cell phone carriers, was sufficient to establish unavailability); *State v. Espiritu*, 176 P.3d 885, 892-93 (Haw. Sup. Ct. 2008) ("Although HRE [Hawaii Rule of Evidence] Rule 1002 would ordinarily preclude the admission of testimony about the text messages because such testimony is not an original, the testimony here is admissible because HRE Rule 1004 applies to the text messages such that other evidence may be admitted to prove the content of the text messages. HRE Rule 1004 provides an exception to the original writings requirement of HRE Rule 1002.... The plain language of HRE Rule 1004 states that an original or duplicate is not required to prove the contents of a writing or recording so long as the originals are lost or destroyed and such loss or destruction was not due to the bad faith of the proponent of the evidence").

Text Messages: Hearsay

Flagg ex rel. J. B. v. City of Detroit, 2011 U.S. Dist. LEXIS 126182, at *21 (E.D. Mich. Nov. 1, 2011) ("Each ...text message, of course, is an out-of-court statement, and therefore must be excluded from consideration as hearsay unless Plaintiffs are able to identify a ground for its admissibility"). The Hawaii Supreme Court relied on the exception for refreshed recollection under the state equivalent of Federal Rule of Evidence 612 to affirm the introduction of text messages read into the record from a police report, in *State v. Espiritu*, supra, 176 P.3d at 895 (Haw. Sup. Ct. 2008) ("Petitioner's argument that the Complainant was not using the report to refresh her memory but was instead using the report to recite verbatim the text messages is unpersuasive.... Petitioner accurately recalled the gist or the general nature of each text message prior to viewing the police report").

CONCLUSION • Internet and email evidence is here to stay. While they both present some novel challenges, the Rules of Evidence apply to them in fairly familiar ways. The better an attorney's grasp of the nuances of the Rules, the more useful — and powerful — this evidence can be.