2014

§ 9:9 Authenticating email, social media, web pages, text messages, instant messaging, electronic signatures

Laird Kirkpatrick
George Washington University Law School, lkirkpatrick@law.gwu.edu

§ 9:9 Authenticating email, social media, web pages, text messages, instant messaging, electronic signatures

In the electronic communication era, email and web pages and social media, not to mention twitter and texting and Instant Messaging, have become increasingly important types of evidence.[1] Yet electronic evidence, because of the ease with which it can be created, altered, and manipulated, presents challenging issues of authentication.[2]

Email, text messages, instant messaging. Material of this sort is

---

[1]*D.C. Circuit:* U.S. v. Safavian, 435 F. Supp. 2d 36 (D.D.C. 2006) (referring to our "age of technology and computer use" in which email is a "normal and frequent" mechanism for the majority of us, including "the professional world").

[2]See Jerry E. Smith, Email Evidence in the Age of Instant Communication: A View from the Bench, Address at ALI-ABA CLE Seminar on Evidence Issues

often proved by computer printout or electronic images. The evidentiary hurdles are minimal with respect to authenticating printouts as accurate copies. A witness who has seen the email or text message or instant message need only testify that a printout offered is an accurate reproduction.[3] With printouts, and also with electronic images, the proponent can show the manner in which a computer makes the image or gathers the data and sends those data to a printer: Rule 901(b)(9) allows this form of authentication, authorizing a showing that a process "produces an accurate result."[4] A court may even take judicial notice of these processes. There is no Best Evidence problem with respect to printouts or electronic images, because Rule 1001(d) defines "original" to include "any printout—or other output readable by sight—if it accurately reflects the information."[5]

Authenticating the email itself, or a text message or instant message, can also be simple, depending on the purpose for which it is offered. A witness can authenticate such material as having

---

and Jury Instructions in Employment Cases (Feb. 10, 2005) (commenting that it is "easier to forge email than to forge hard copies," by access to "an unlocked computer or a carelessly placed Blackberry"); Jay M. Zitter, Authentication of Electronically Stored Evidence, Including Text Messages and Email, 34 A.L.R. 6th 253 (2008).

Fourth Circuit: But see Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 543 (D. Md. 2007) (rejecting argument that emails or text messages are unreliable because of "relative anonymity" and fact that message "can rarely be connected to a specific author" with certainty; similar uncertainties exist with written documents).

Pennsylvania: But see In re F.P., 878 A.2d 91, 95 (Pa. Super. 2005) (rejecting contention that emails and other electronic communications are "inherently unreliable" and noting that "the same uncertainties" with written documents).

[3]*Tenth Circuit:* U.S. v. Simpson, 152 F.3d 1241, 1249–1250 (10th Cir. 1998) (admitting printout of alleged chat room discussion between defendant and undercover police officer based on evidence it was what government claimed).

Mississippi: Kearley v. State, 843 So. 2d 66, 70 (Miss. App. 2002) (witness vouched for accuracy of email printouts, thus authenticating them).

[4]See discussion of Rule 901(b)(9) in § 9:20, infra.

Tenth Circuit: U.S. v. Meienberg, 263 F.3d 1177, 1181 (10th Cir. 2001) (questions on accuracy of printouts, "whether resulting from incorrect data entry or the operation of the computer program," would affect weight, not admissibility).

Washington: State v. Andrews, 293 P.3d 1203 (Wash. App. 2013) (admitting photograph of text message as duplicate admissible under Rule 1003).

[5]See discussion of Rule 1001(3) in § 10:9, infra.

been sent by the witness himself by identifying it as such.[6] Similarly, one who receives an email, text message, or instant message, can authenticate it as having been received simply by so testifying, but of course it is another matter to prove the identity of the author of such an email, text or instant message.[7] Testimony by the recipient indicating receipt of such material satisfies Rule 901(b)(1) because it is testimony by a witness with knowledge "that an item is what it is claimed to be," namely an email (or text or instant message) that the witness received.[8] As indicated below, often the recipient can provide additional testimony that proves not only receipt of a particular email or text or instant message, but the source as well.

Particularly in civil litigation, the authenticity of such material can be established in pretrial discovery, including identification at a deposition, in an answer to an interrogatory, or in response to a request for admission. These mechanisms can often establish not only receipt of such material, but authorship, and these matters are sometimes accomplished in pretrial settings by informal means, even inadvertently, paving the way to admit the material at trial (or sometimes simply making the task of authentication easier by paving the way for a witness to testify that the matter was conceded).[9]

The more difficult challenge is to establish authorship of emails, and of text messages and instant messages, where the purported author is unavailable or unable or unwilling to acknowledge the

---

[6]*Seventh Circuit:* Fenje v. Feld, 301 F. Supp. 2d 781, 809 (N.D. Ill. 2003), *aff'd,* 398 F.3d 620 (7th Cir. 2005) (can authenticate emails by "statements or other communications" from purported author "acknowledging" them).

Mississippi: Kearley v. State, 843 So. 2d 66, 70 (Miss. App. 2002) (defendant admitted to sending emails).

[7]*Seventh Circuit* B.S. ex rel. Schneider v. Board of School Trustees, 255 F. Supp. 2d 891, 893–894 (N.D. Ind. 2003) (affidavit of recipient is "acceptable method" of authentication).

Mississippi: Kearley v. State, 843 So. 2d 66 (Miss. App. 2002) (in sexual battery trial, minor victim could authenticate emails from defendant).

Texas: Shea v. State, 167 S.W.3d 98, 105 (Tex. App. 2005) (testimony of complainant that she received the emails).

[8]See discussion of Rule 901(b) in § 9:3, supra.

See generally Note, "God Mail": Authentication and Admissibility of Electronic Mail in Federal Courts, 34 Am. Crim. L. Rev. 1387 (1997).

[9]*Fifth Circuit:* Middlebrook v. Anderson, 2005 WL 350578 (N.D. Tex. 2005) (statements in defendant's affidavit that he "did not intend" email messages to be viewed in a particular state was a concession that he sent them).

Seventh Circuit: Superhighway Consulting, Inc. v. Techwave, Inc., 1999 WL 1044870 (N.D. Ill. 1999) (production of email during discovery from party files justifies finding of authenticity).

point. Here the proponent must rely on other methods. Certainly testimony by a person who saw the purported author write and send such material would suffice. If the computer, or for that matter the cellphone or "android" from which such material was sent is owned by a particular person, was seized from that person's possession, or there are other compelling circumstances linking the computer to that person, such facts may be enough to authenticate the material as having come from that person.[10] If it is a shared computer, or one to which others had access, additional evidence linking the purported author to the email seems essential. For example, proof that the person in question was the one using the computer when the message was sent should suffice to connect the message to that person. Particularly in criminal cases where establishing authorship, and where a jury may have to be persuaded beyond a reasonable doubt that the defendant was the author in order to convict him, prosecutors sometimes call technical witnesses who do a trace. For emails, an expert may rely on the coded Internet Protocol Address appearing in the email header and trace it back to the service provider who relayed the message and sometimes back to a particular computer,[11] and electronic data can sometimes be authenticated by reference to metadata stored in documents and by "hashtags" used to encrypt data, and specifically by SHA ("secure hash algorithm") or the MD5 algorithm.[12]

If the email message was encrypted by means of a digital signature and was therefore only available to a receiver who had a private key or access to a public key, a technical expert should be called to explain the encryption process and establish the necessary linkages to authenticate the email.[13]

The most common method of authenticating emails, text mes-

---

[10]*Fifth Circuit:* U.S. v. Luncy, 676 F.3d 444 (5th Cir. 2012) (alleged attempt at sex with underage girl; defendant was "on the phone talking with [alleged victim] when he was arrested is enough" to prove his authorship of text messages).

[11]*Ninth Circuit:* Clement v. California Dept. of Corrections, 220 F. Supp. 2d 1098, 1111 (N.D. Cal. 2002), *aff'd,* 364 F.3d 1148 (9th Cir. 2004) (major email providers include coded Internet Protocol address or IP address in email header; IP address lets recipient "identify the sender by contacting the service provider").

[12]*Fourth Circuit:* Lorraine v. Markel American Ins. Co., 241 F.R.D. 34, 543 (D. Md. 2007) (citing use of "hash values" as a means of authenticating electronic evidence, as well as metadata).

[13]See generally Effross, *Notes on PKI and Digital Negotiability: Would the Cybercourrier Carry Luggage?*, 38 Jurimetrics J. 385 (Spring 1998); Froomkin, Flood Control on the Information Ocean: Living with Anonymity, Digital Cash and Distributed Databases, 15 J. Law & Commerce 395, 411–24 (1996); Froom-

sages, and instant messages involves showing "appearance, contents, substance, internal patterns, or other distinctive characteristics . . . , taken together with all the circumstances," which can suffice Rule 901(b)(4).[14] Included in the relevant circumstances are indications in the message itself of its source (whether name, phone number, or URL),[15] connections between statements in the communication itself and known facts about the sender,[16] behavior by the sender and the recipient that point

---

kin, Symposium: Innovation and the Information Environment: The Essential Role of Trusted Third Parties in Electronic Commerce, 75 Or. L. Rev. 49 (1996).

[14] *North Dakota:* State v. Thompson, 777 N.W.2d 617, 626 (N.D. 2010) (in trial of wife for assaulting husband, admitting her text messages to him with "profane and threatening language," on circumstantial evidence that she wrote them, including proof of her phone number and fact that her "distinctive signature" showed on message; complainant testified that messages from her appeared on his phone labeled "Fr: Jen," which appears on messages) (citing this Treatise).

Pennsylvania: In re F.P., 878 A.2d 91, 94–95 (Pa. Super. 2005) (distinguishing features in emails contributed to finding that they were authentic).

Texas: Massimo v. State, 144 S.W.3d 210, 215–216 (Tex. App. 2004) (same).

Shea v. State, 167 S.W.3d 98, 105 (Tex. App. 2005) (same).

[15] *D.C. Circuit:* U.S. v. Safavian, 435 F. Supp. 2d 36 (D.D.C. 2006) (emails authenticated by distinctive characteristics, including actual email address containing the "@" symbol, name of the person connected to that address, name of senders and receiver in headers and bodies of email).

Seventh Circuit: Fenje v. Feld, 301 F. Supp. 2d 781, 810 (N.D. Ill. 2003), *aff'd,* 398 F.3d 620 (7th Cir. 2005) (emails authenticated by testimony that purported sender sent emails, source email address, matching that on purported sender's letterhead, and content, which was consistent with other evidence).

Eleventh Circuit: U.S. v. Siddiqui, 235 F.3d 1318, 1322–1323 (11th Cir. 2000) (fact that alleged sender's name and address appeared on email counts).

[16] *D.C. Circuit:* U.S. v. Safavian, 435 F. Supp. 2d 36 (D.D.C. 2006) (emails authenticated by distinctive characteristics, content discussing personal and professional matters relating to individuals in question).

Tenth Circuit: U.S. v. Simpson, 152 F.3d 1241, 1250 (10th Cir. 1998) (admitting instant messaging chat on basis that person using name "Stavron" told officer his name was Simpson and gave street address; later exchanges indicated email address belonging to Simpson; pages near computer in home noted name, address, email address and phone number that officer gave in chat room).

Arkansas: Todd v. State, 2012 WL 5424516 (Ark. App. 2012) (in trial for internet stalking of child, admitting chat log; defendant "arrived at the agreed store" at the "agreed date and time").

North Carolina: State v. Wilkerson, 733 S.E.2d 181, 183–184 (N.C. App. 2012) (in robbery trial, admitting message sent from defendant's cellphone and stored there referencing some of the stolen property found in his trunk).

toward the two as being sender and recipient,[17] a course of conduct or dealing between two people that regularly employs emails, texts, or instant messages and showing that the material in question fits into that course of dealing,[18] and connections between the person in question and the phone in question, coupled with other information about behavior as it relates to content.[19]

The fact that a person's name appears in the header as the "sender" should not be enough to authenticate the email as being from that person, just as self-identification by a telephone caller is insufficient to authenticate the call as being from that person.[20] However, self-identification can complement other authenticating factors such as circumstances, content, internal patterns and extrinsic evidence.[21]

Stronger circumstantial evidence would be a showing that the actual email address, e.g., mailto:johndoe@aol.com, matches an account in that person's name with the indicated internet service provider, although this is not necessarily sufficient by itself because it is not technically difficult to send an email message using another's email address.

In most modern cases, courts have relied primarily on the content of the message as a basis for authenticating emails.[22] If an email contains particularized information that only the purported sender is likely to know, this will authenticate the

---

[17]*New York:* People v. Green, 2013 WL 3029447 (N.Y. App. Div. 2013) (in trial for rape and related offenses, admitting text messages from defendant to complainant, since content made no sense unless they were sent by him).

[18]*Ohio:* State v. Huge, 2013 WL 2325637 (Ohio App. 2013) (in trial of father for killing his infant daughter, admitting text messages to victim's mother on basis of her testimony that "texting was her normal means of communicating with" him, and that message had been sent by him and "saved to her phone").

[19]*Florida:* Symonette v. State, 100 So.3d 180 (Fla. App. 2012) (in robbery trial, admitting text messages apparently sent by defendant to driver of getaway car and by her to him; driver identified messages and context; they were also found on defendant's phone, retrieved on his arrest).

[20]See § 9:16, supra.

Third Circuit: Victaulic Co. v. Tieman, 499 F.3d 227, 236 (3d Cir. 2007) (error to take judicial notice of facts about plaintiff company based on website, which was not authenticated; anyone may purchase web address, so trade name in URL does not authenticate website; can only notice matters not subject to reasonable dispute).

[21]See generally B.S. ex rel. Schneider v. Board of School Trustees, 255 F. Supp. 2d 891, 893–894 (N.D. Ind. 2003); Kearley v. State, 843 So. 2d 66 (Miss.. App. 2002); Shea v. State, 167 S.W.3d 98, 105 (Tex. App. 2005)

[22]*D.C. Circuit:* U.S. v. Safavian, 435 F. Supp. 2d 36 (D.D.C. 2006) (emails authenticated in part by content disclosing personal and professional matters relating to individuals in question).

email to the same extent that such knowledge would authenticate a written message.[23] Obviously the more specialized or unique the information, the more such content tends to authenticate the message as being from a particular sender who has such knowledge.

Particularized content may include information about serial numbers, credit card numbers, ordering information, personal transactions, private communications, particular relationships, coded communications, and other types of private information, or at least information that is not known to the general public.[24]

A common type of content used to authenticate is content given in reply to an earlier email message.[25] An email purporting to be a reply to an earlier message sent to a particular person is likely to be authored by that person. Often an email message will include the message to which it is responding as an attachment or even in the body of the message. Even though it is possible that a reply is sent by a person other than the recipient of the original message, the danger is no greater here than for written messages.

Other circumstances that can be used to help authenticate an email include the fact that the purported sender promised to send an email to the recipient and one was later received, the fact that previous messages sent to a particular email address

---

See generally B.S. ex rel. Schneider v. Board of School Trustees, 255 F. Supp. 2d 891, 893–894 (N.D. Ind. 2003); Kearley v. State, 843 So. 2d 66 (Miss. App. 2002); Shea v. State, 167 S.W.3d 98, 105 (Tex. App. 2005)

See also Note, When the Postman Beeps Twice: The Admissibility of Electronic Mail Under the Business Records Exception to the Federal Rules of Evidence, 64 Fordham L. Rev. 2285 (1996).

[23]See §§ 9:6 to 9:9, supra.

[24]*Eleventh Circuit:* U.S. v. Siddiqui, 235 F.3d 1318, 1322 (11th Cir. 2000) (in trial for submitting fraudulent recommendations for National Science Foundation award, admitting emails from defendant; they showed knowledge of actions only he would have, apologized for things he had done, came from his email address, were signed with his nickname, and he made similar points in conversations thereafter).

[25]*Fifth Circuit:* U.S. v. Barlow, 568 F.3d 215, 220 (5th Cir. 2009) (in trial for seeking sex with underage female, admitting chatroom log on testimony by freelance undercover agent posing as girl, indicating that transcripts "fairly and fully reproduced" chats between her, posing as Rebecca, and defendant; agent was the other participant in year-long "relationship' " and had direct knowledge of chats and could authenticate chat log).

Virginia: See Bloom v. Com., 542 S.E.2d 18, 20–21 (Va. App. 2001), *aff'd,* 554 S.E.2d 84 (Va. 2001) ("internal links" between earlier and later internet communications between defendant and victim authenticity).

See discussion of the "reply doctrine" in § 9:7, supra.

reached the purported sender of the email in question,[26] or the fact that actions were taken by the purported sender in response to emails sent to the purported sender's address,[27] such as the shipping of merchandise. Many other circumstances count as well.[28]

Emails can also be authenticated under Rule 901(b)(3), which authorizes "comparison with an authenticated specimen by an expert witness or the trier of fact." Thus emails that are not clearly identifiable on their own can be authenticated by allowing the jury to compare them with specimens that have been previously authenticated.[29] Even if an email is successfully authenticated, it is not admissible to prove the truth of its content unless an additional foundation is laid showing that it fits an exception to the hearsay rule. If the email is shown to be from a party opponent, this will ordinarily suffice to allow its introduction into evidence as an admission.[30] An email forwarding another email may sometimes constitute an adoptive admission of the original email by the person forwarding it.[31] In unusual circumstances, an email statement may qualify as a present sense impression or an excited utterance.[32]

Emails, even if made in the course of business, do not necessar-

---

[26]*Eleventh Circuit:* U.S. v. Siddiqui, 235 F.3d 1318, 1322–1323 (11th Cir. 2000) (alleged sender had previously received email at that address).

[27]*Eleventh Circuit:* U.S. v. Siddiqui, 235 F.3d 1318, 1322–1323 (11th Cir. 2000) (in later phone call, alleged sender repeated request that appeared in email).

[28]*Tenth Circuit:* U.S. v. Simpson, 152 F.3d 1241, 1249–1250 (10th Cir. 1998) (admitting printout of chat room discussion between defendant and undercover officer on proof that person calling himself "Stavron" gave officer his name as Simpson and his street address; later exchanges indicated email address belonging to him; pages found near computer in his home contained notation of name, street address, email address and phone number that officer gave in chat room).

[29]*D.C. Circuit:* U.S. v. Safavian, 435 F. Supp. 2d 36 (D.D.C. 2006) (can authenticate emails by comparing them with other emails that had been authenticated by content and distinctive characteristics).

[30]*Ninth Circuit:* Van Westrienen v. Americontinental Collection Corp., 94 F. Supp. 2d 1087, 1109 (D. Or. 2000) (representations made by defendants on website are admissions of party-opponent).

[31]*Ninth Circuit:* Sea-Land Service, Inc. v. Lozen Intern., LLC., 285 F.3d 808, 821 (9th Cir. 2002) (employee of plaintiff "incorporated and adopted the contents" of an email message from another of plaintiff's employees when she forwarded it to defendant with a cover note that "manifested an adoption or belief in the truth" of information contained in original email).

[32]*First Circuit:* U.S. v. Ferber, 966 F. Supp. 90 (D. Mass. 1997) (admitting email as present sense impression).

ily qualify for admission as business records.[33] While emailed billing statements and similar records may qualify, routine personal and professional email communications, like routine written correspondence, often fail to satisfy the exception because they lack the regularity and systematic checking of information that justifies making business records an exception to the hearsay rule.[34]

The procedures for authenticating printouts of online conversations in internet "chat rooms" are essentially the same as those for authenticating emails.[35]

Oregon: State v. Cunningham, 40 P.3d 1065, 1076 n8 (Or. App. 2002), *rev'd on other grounds,* 99 P.3d 271 (Or. 2004), *cert. denied,* 544 U.S. 931 (2005) (noting that email may be admissible as excited utterance).

[33]For a discussion of the application of the business records exception to email, see Note, When the Postman Beeps Twice: The Admissibility of Electronic Mail Under the Business Records Exception of the Federal Rules of Evidence, 64 Fordham L. Rev. 2285 (1996).

[34]*First Circuit:* U.S. v. Ferber, 966 F. Supp. 90, 98 (D. Mass. 1997) (it may have been employee's routine practice to make email records; there was not enough evidence that employer required such records; business records exception requires business duty to make and maintain records).

Ninth Circuit: Monotype Corp. PLC v. International Typeface Corp., 43 F.3d 443, 450 (9th Cir. 1994) (electronic documents may fit business records exception, but email is "far less of a systematic business activity than a monthly inventory printout" and is instead "an ongoing electronic message and retrieval system").

[35]*Fifth Circuit:* U.S. v. Barlow, 568 F.3d 215 (5th Cir. 2009) (transcripts of "chat log" of conversations between agent and defendant authenticated by agent's testimony that they were accurate).

Ninth Circuit: U.S. v. Tank, 200 F.3d 627, 629–631 (9th Cir. 2000) (in T's trial for sexual exploitation, from transactions in Internet chat room called the Orchid Club, where members trade digital child porn, admitting logs kept on R's computer; R was a club member and he deleted "nonsexual conversations and extraneous material, such as date and time stamps," but remainder of logs implicated T; reviewing court rejects claim that changes might have introduced "undetectable material alterations," since R explained how he created logs, and they "appeared to be an accurate representation" of conversations; government connected logs with T by showing he used screen name "Cessna" which appeared in printouts of logs).

Tenth Circuit: U.S. v. Simpson, 152 F.3d 1241, 1249–50 (10th Cir. 1998) (chat room logs sufficiently authenticated).

See J. Allan Cobb, Evidentiary Issues Concerning Online "Sting" Operations: A Hypothetical-Based Analysis Regarding Authentication, Identification, and Admissibility of Online Conversations—A Novel Test for the Application of Old Rules to New Crimes, 39 Brandeis L. J. 785, 805–820, 823–834 (2001).

Eleventh Circuit: U.S. v. Lanzon, 639 F.3d 1293, 1301 (11th Cir. 2011) (in sex offense trial, admitting instant message transcripts where detective testified that he participated in online chats and transcripts were accurate).

Web pages. It was only a matter of time before courts were asked to consider the matter of authenticating internet web pages (or websites) and web postings. Clearly such material is subject to the authentication requirement, and authenticating such material can be a matter of some difficulty. Particularly in the case of private websites, authenticating proof is necessary,[36] although government websites appear to be self-authenticating under Rule 902(5) as a publication "purporting to be issued by a public authority."[37]

Just as a phone call can sometimes be authenticated by proof that the calling party "dialed" the number assigned by the phone company to another, coupled usually with proof that the ensuing conversation was the sort of conversation that would go forward if the caller got the intended number, it is usually sufficient to show that a web surfer looked up a particular person or company in a directory or found it by using a search engine, and went to that site and was able to place an order or conduct business that would be expected at such a site. Although these questions are just now beginning to appear, it is clear that authentication should be required in this setting.[38]

Some of the early judicial opinions indicated extreme skepticism toward this form of evidence. One court described the Internet as "one large catalyst for rumor, innuendo, and misinformation" and suggested that there is a presumption that information discovered on the Internet is "inherently untrustworthy."[39] Other decisions have been more receptive and approving. There is no reason why evidence from websites should

---

[36]*Fifth Circuit:* Bibolotti v. American Home Mortgage Servicing, Inc., 2013 WL 2147949 (E.D. Tex. 2013) (Internet websites are not self-authenticating; no proof of authenticity here; striking proffered printouts from record).

Eighth Circuit: Fraserside IP LLC v. Netvertising Ltd., 902 F.Supp.2d 1165, 1179 n2 (N.D. Iowa 2012) (private websites are not self-authenticating; must produce some statement or affidavit by person with knowledge).

[37]*Hawaii:* Child Envorcement Agency v. MSH, 2013 WL 1829647 (the ".gov" internet domain generally denotes a website administered by a government entity, and as such it is self-authenticating under Rule 902(5)).

[38]For a helpful discussion of authentication of website contents, see Joseph, Modern Visual Evidence § 15.02[1] (2006).

Fifth Circuit: U.S. v. Baker, 538 F.3d 324, 331–333 (5th Cir. 2008), *cert. denied,* 129 S. Ct. 962 (2009) (in trial for distributing child porn, error to admit images uploaded to website; insufficient evidence that defendant uploaded them).

[39]*Fifth Circuit:* St. Clair v. Johnn's Oyster & Shrimp, Inc., 76 F.Supp. 2d 773, 774–775 (S.D. Tex. 1999) (some look to Internet as innovative vehicle for communication, but court "warily and wearily" views it as "catalyst for rumor, innuendo, and misinformation," which provides "no way of verifying the authenticity" of contentions plaintiff wishes to use in response to defense mo-

not be admissible for certain purposes, provided it has been adequately authenticated.

Website postings may have particular value when offered against the owner of the website, for example, as an admission by that party or for a nonhearsay purpose such as establishing the price of a product, representations to induce a sale, the terms of a contract, or a warranty.

To authenticate a printout of a web page, the proponent must offer evidence that: (1) the printout accurately reflects the computer image of the web page as of a specified date; (2) the website where the posting appears is owned or controlled by a particular person or entity; and (3) the authorship of the web posting is reasonably attributable to that person or entity. Evidence that may corroborate these points could include testimony of others who saw the posting on the website, continuation of the posting on the website so that it is available to be seen by the court, or evidence that the party to whom the posting is attributed made similar postings or published the same information elsewhere.[40] Some services take "snapshots" of websites as they appeared on particular dates and store that information in an archive. The testimony of an expert familiar with how those services work may be sufficient to authenticate an image purporting to depict the appearance of a website on a date in question.[41]

---

tion; plaintiff cannot overcome "presumption" that information discovered on Internet is "inherently untrustworthy," as anybody can post "anything" there; no website is monitored for accuracy, and nothing is under oath or subject to verification; moreover, "hackers can adulterate" content on any website for anywhere).

[40] *Ninth Circuit:* Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1154 (C.D. Cal. 2002) (in copyright case, declarations that printouts were "true and correct" copies of internet pages, "in combination with circumstantial indicia of authenticity (such as the dates and web addresses)" would support reasonable juror belief that documents are what proponent claims).

Ohio: See Johnson-Wooldridge v. Wooldridge, 2001 WL 838986, *4 (Ohio App. 2001) (party who printed documents from a website "could have authenticated the documents himself via an affidavit or through his own testimony").

[41] See generally Eltgroth, Best Evidence and the Wayback Machine: Toward a Workable Authentication Standard for Archived Internet Evidence, 78 Fordham L. Rev. 181 (2009).

Third Court: U.S. v. Bansal, 663 F.3d 634, 667 (3d Cir. 2011) (in drug conspiracy case, admitting screenshots of defendant's online pharmacy operation where government obtained images from company that maintained "Wayback Machine," a historical database of all internet websites, and witness testified about operation and reliability of company's operations, and stated that

If authorship or responsibility for the web posting cannot be sufficiently established, exclusion will normally be required.[42]

If the web posting is offered for the truth of what it asserts, it is necessary to lay an additional foundation to admit it under an exception to the hearsay rule. A distinction must of course be drawn between authenticating a web posting as being from a particular person and offering it to prove the truth of any assertions it contains. In the case of admissions, these issues conflate. If the web posting is adequately authenticated as being from a party opponent, it normally will be admissible as an admission. If the web posting is by a third party and is offered for its truth, an additional foundation is necessary to admit it as an exception to the hearsay rule.[43]

In the case of government-maintained websites, courts are divided on whether information posted thereon is admissible to

---

screenshots were authentic based on comparison with previously authenticated and admitted images from defendant's website).

Seventh Circuit: Telewizja Polska USA, Inc. v. Echostar Satellite Corp., 65 Fed. R. Evid. Serv. 673 (N.D. Ill. 2004) (noting that while such archiving technology does not fall within any of the examples listed in Rule 901, there was no evidence that it was unreliable or biased; and holding that the affidavit of an expert affiliated with an archiving company was sufficient to authenticate an exhibit purporting to depict a website as of a particular date).

Eighth Circuit: Jones v. National American University, 608 F.3d 1039, 1045–46, 257 Ed. Law Rep. 866, 82 Rule Serv. 1236 (8th Cir. 2010) (online employment advertisements authenticated by testimony from (a) university president that he was familiar with employment section of university's website, and that advertisements offered by plaintiff were in same format of web postings, and (b) university employees that they had seen advertisement for director of admissions position) (authentication was sufficient even though posting differed in format from other advertisements and author was not identified).

[42]*Seventh Circuit:* U.S. v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000) (in trial for defrauding UPS by suggesting that African-American artwork had been damaged by white supremacist group when defendant did it, purported web pages of white supremacist group taking credit were not authenticated; defendant was savvy computer user and made no showing that pages were posted by supremacist group rather than defendant herself).

Ninth Circuit: Costa v. Keppel Singmarine Dockyard PTE, Ltd., 2003 WL 24242419 (C.D. Cal. 2003) (excluding webpage describing defendant's corporate structure; no showing that defendant directed placement of information on website).

Wady v. Provident Life and Accident Ins. Co. of America, 216 F. Supp. 2d 1060, 1064–65 (C.D. Cal. 2002) (postings from defendant's website not authenticated; proponent could not establish who maintained website or authorship or accuracy of contents).

[43]*Seventh Circuit:* U.S. v. Jackson, 208 F.3d 633, 637 (7th Cir. 2000) (web postings offered to prove matter asserted must satisfy hearsay exception).

prove the matter asserted, with some allowing[44] and some rejecting such evidence.[45] The resolution of this issue should depend on the reasons for the existence of the government website. If its purpose is to function as the equivalent of an official government publication, properly authenticated web postings should be admissible under Rule 902(5).[46]

Electronic signatures. Because so much commerce is now in electronic form, Congress passed the Electronic Signatures in Global and National Commerce Act (E-Sign) in 2000.[47] The Act provides that in transactions affecting interstate or foreign commerce "a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form" and the contract itself may not be denied legal effect "solely because an electronic signature or electronic record was used in its formation."[48]

The Act has broad effect in affirming the legal status of a wide variety of records in electronic format, including business records, public records, and insurance documents.[49] It authorizes the retention of records in electronic form under a variety of existing statutes that require record retention.[50]

The Act defines an electronic signature as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person

---

[44]*Second Circuit:* Elliott Associates, L.P. v. Banco de la Nacion, 194 F.R.D. 116, 121 (S.D. N.Y. 2000) (prime rates published on Federal Reserve Board web site satisfy Rule 803(17) as market reports).

[45]*Indiana:* Dumes v. State, 718 N.E.2d 1171, 1178–1179 (Ind. App. 1999) (motor vehicle department records obtained via internet not admissible).

Washington: State v. Davis, 10 P.3d 977, 1009–1010 (Wash. 2000) (printout from state website on population statistics was not self-authenticating official publication; did not satisfy public records exception).

[46]Sannes v. Jeff Wyler Chevrolet, Inc., 1999 WL 33313134, n3 (S.D. Ohio 1999) (press release on FTCs website was self-authenticating official publication).

[47]15 U.S.C.A. §§ 7001 to 7006. See generally, Wittie & Winn, Electronic Records and Signatures Under the Federal E-SIGN Legislation and the UETA, 56 Bus. Law. 293 (2000); Note, The E-Sign Act of 2000: The Triumph of Function over Form in American Contract Law, 76 Notre Dame L. Rev. 1183 (2001); Comment, E-Commerce and E-Law: Is Everything E-okay? Analysis of the Electronic Signatures in Global and National Commerce Act, 53 Baylor L. Rev. 803 (2001).

[48]15 U.S.C.A. § 7001(a).

[49]15 U.S.C.A. § 7001(i) (noting intent that statute apply to insurance).

[50]15 U.S.C.A. § 7001(d).

with the intent to sign the record."[51] However, there is no specified procedure for authenticating such signatures in a court proceeding, and other provisions of the Act give little guidance on this point.[52] The Act provides that where law requires a signature under oath to be notarized, acknowledged, or otherwise made under oath, that requirement is satisfied "if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable statute, regulation, or rule of law, is attached to or logically associated with the signature or record."[53] However, the electronic signature of the notary or person administering the oath will also need to be authenticated.

Because there are so many potential forms of electronic signature, the authentication methods must necessarily vary with the type of signature used. Certainly a party can authenticate that party's own signature under Rule 901(b)(1), as can a knowledgeable witness who observed the signing or has another basis for recognizing the signature. Sometimes a signature can be authenticated by the out-of-court admissions of the purported signer and admitted under Rule 801(d)(2). It may be possible to authenticate an electronic signature under Rule 901(b)(3) by having an expert witness or even the trier of fact compare it to a specimen which has been authenticated.

In some cases, the signature can be authenticated by its "appearance, contents, substance, internal patterns, or other distinctive characteristics . . . , taken together with all the circumstances" under Rule 901(b)(4). Electronic signature systems sometimes use verification technologies that might fall within this section. Much as with email authentication, electronic signatures might be authenticated by particularized information that only the purported signer is likely to know, in the form of a verification password (e.g., a deceased pet's name or mother's maiden name) that must be entered before the signature is accepted. Similarly, some technologies may require that a user provide personal information that can then be checked indepen-

---

[51] 15 U.S.C.A. § 7006(5).

[52] The Secretary of Commerce is instructed to promote the use and acceptance of electronic signatures on an international basis in accordance with principles that "[p]ermit parties to a transaction to determine the appropriate authentication technologies and implementation models for their transactions, with assurance that those technologies and implementation models will be recognized and enforced" and to "[t]ake a nondiscriminatory approach to electronic signatures and authentication methods from other jurisdictions." 15 U.S.C.A. § 7031.

[53] 15 U.S.C.A. § 7001(g).

dently to confirm the signer's identity, such as credit card information. Other technologies might employ an email to the signer's email address that requires a response before the signature is accepted; a reply from an email address known to be used by the purported signer may be used to authenticate a signature.

In some cases, the electronic signature may be a sound rather than an image, and a tape of the sound may be used to demonstrate the digitally produced sound. A witness would then need to identify the sound as one establishing the signature on the document offered.

In many cases writings at issue in litigation that rely on electronic signatures will be signed and sent using encryption technology. In such cases a technical witness is necessary who should be able to authenticate the signature by explaining the process of cryptography and the specific procedures that were used with respect to the electronic communication at issue.[54]

Social media. Modern cases have increasingly faced the question whether evidence from social media (Facebook, MySpace, Twitter, and others) should be admitted. Authentication issues resemble those found with other forms of electronic communication, but one distinguishing factor is that social media often involve postings that are accessible to large numbers of people, and sometimes to the entire world. It is uncertain whether social media accounts are more easily hacked than email accounts, but obvious concerns about security of social media arise, and it may well be that more people have both motive and access to social media, which heightens concerns over security and possibly malicious and fraudulent postings. The Maryland Supreme Court observed that "authentication concerns attendant to emails, instant messaging, and text messages differ significantly from those involving a MySpace profile and posting printout, because such correspondence is sent directly from one party to an

---

[54]The process requires a public key and a private key. Each is a unique mathematical algorithm maintained by a "certification authority," who is a neutral third party. The signer encrypts the message with a private key, sends it to the recipient, who uses a public key to decode the message. If the document is forged or altered, the keys will not function. Use of digital signature technology is specifically provided for by the Uniform Electronic Transactions Act, which has been adopted by a number of states. See, e.g., Kan. Stat. Ann. § 16-1602.

See generally, Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce, 75 Or. L. Rev. 49 (1996).

intended recipient or recipients, rather than published for all to see."[55]

As with other forms of electronic communication, the challenge is usually not in proving that a particular communication was received or posted, and the concern is rather in learning the identity of the sender or maker. A mere showing that the message was sent from a particular account or posted on a particular web page is not necessarily sufficient to authenticate the message as being from the owner of that account or web page,[56] and more should be shown to establish the identity of the person posting the message, such as evidence that the originating site has security features that tend to assure the identity of the source.[57]

The authentication method most commonly used by proponents of social media evidence is to demonstrate its distinctive characteristics. Under Rule 902(4) the proponent must show that the circumstantial evidence of the case combined with the "appearance, contents, substance, internal patterns, or other distinctive characteristics" of the exhibit are sufficient to prove that the proffered evidence is what it is purported to be. A distinctive characteristic particularly likely to persuade a court that the

---

[55] *Maryland:* Griffin v. Maryland, 19 A.3d 415, 426 n.13 (Md. 2011).

[56] *First Circuit:* Massachusetts v. Williams, 926 N.E.2d 1162, 1172 (Mass. 2010) (while foundational testimony showed that the messages "were sent by someone with access to [defendant's] MySpace Web page, it did not identify the person who actually sent the communication").

Second Circuit: Connecticut v. Eleck, 23 A.3d 818, 824–25 (Conn. App. Ct. 2011) (witness claimed her Facebook account had been hacked, highlighting "the general lack of security of the medium" and raising the question "whether a third party may have sent the messages via [the witness's] account"),

Maryland: Griffin v. State, 19 A.3d 415, 421–422 (Md. 2011) (in homicide trial, error to admit posting on MySpace site; it said "snitches get stitches," and was attributed to defendant's girlfriend; anyone can establish such a site; people can set up fake accounts in the name of another, and possibility of fabrication or tampering "poses significant challenge") (reversing).

New York: State v. Lenihan, 911 N.Y.S.2d 588, 591–592 (N.Y. App. Div. 2010) (MySpace photographs downloaded by defendant's mother and offered to impeach witnesses insufficiently authenticated, given ease of editing photos on a computer).

[57] *First Circuit:* Massachusetts v. Williams, 926 N.E.2d 1162, 1172 (Mass. 2010) (excluding MySpace messages allegedly from defendant; there was no testimony on the security of such a Web Page, or "who can access a MySpace Web page, whether codes are needed for such access," and no expert testimony indicated that only defendant could communicate from that page).

authentication requirement is satisfied is the use of code words known only to the parties.[58]

Circumstantial evidence varies significantly from case to case, and courts apply different levels of scrutiny when determining whether the authentication threshold has been satisfied. Some courts have applied a strict standard[59] and others a more lenient one.[60]

If the proponent calls an authenticating witness to testify how a particular electronic communication is made, such as an expert from the company sponsoring the social media site, that person must be able to "provide factual specificity about the process by which the electronically stored information is created, acquired, maintained, and preserved without alteration or change, or the process by which it is produced if the result of a system or process that does so."[61] Courts have held, however, that it is not es-

---

[58] *Sixth Circuit:* Ohio v. Bell, 882 N.E. 2d 502, 512 (Ohio Ct. Com. Pl. 2008) (MySpace messages contained code words known only to defendant and his alleged victims).

[59] *Second Circuit:* Connecticut v. Eleck, 23 A.3d 818, 824–25 (Conn. App. Ct. 2011) (witness claimed her Facebook account had been hacked, which highlights "the general lack of security of the medium and raises an issue as to whether a third party may have sent the messages via [the witness's] account"),

New York: State v. Lenihan, 911 N.Y.S.2d 588, 591–592 (N.Y. App. Div. 2010) (MySpace photographs downloaded by defendant's mother and offered to impeach witnesses were not authenticated, given ease of editing photos on a computer).

[60] *Third Circuit:* In re F.P., 878 A.2d 91, 95 (Pa. Super. Ct. 2005) (admitting text messages; no need for heightened scrutiny for electronic evidence; "same uncertainties" exist with traditional written documents as they do with electronic evidence; "a signature can be forged; a letter can by typed on another's typewriter; distinct letterhead stationery can be copied or stolen")

Sixth Circuit: Ohio v. Bell, 882 N.E.2d 502, 512 (Ohio Ct. Com. Pl. 2008) (there is a possibility that evidence from a social media site could be incomplete, altered or posted by a third party who hacked into the user's account, but those issues "touch upon concerns regarding the weight of given evidence and not its authenticity").

Texas: Tienda v. State, 358 S.W.3d 633 (Tex. App. 2012) (in homicide trial arising out of shootout, admitting MySpace pages in which defendant presented violent self-image, on basis of testimony describing the creation of MySpace accounts, linking them to defendant through nicknames and photographs and zipcodes and references to events).

[61] *Fourth Circuit:* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 545 (D. Md. 2007).

[62] *Sixth Circuit:* Dockery v. Dockery, 2009 WL 3486662 (Tenn. Ct. App. 2009) (calling "representative from MySpace was not a prerequisite" to admit- ting printouts of exchanged messages).