

# JUDICATURE

*The Scholarly Journal for Judges*

The mass-tort MDL vortex has sucked up 120,000 cases — more than a third of the pending U.S. civil caseload.

1,562 TESTOSTERONE REPLACEMENT THERAPY CASES • IN RE: Zimmer NexGen Knee Implant Products Liability Litigation (MDL No. 2009-0001)

1,041 KNEE IMPLANT CASES • IN RE: Zimmer NexGen Knee Implant Products Liability Litigation (MDL No. 2009-0001)

3,016 DROSPIRENONE CONTRACEPTIVE CASES • IN RE: Biomet M2a Magnum Hip Implant Products Liability Litigation (MDL No. 2009-0001)

1,784 HIP IMPLANT CASES • IN RE: Biomet M2a Magnum Hip Implant Products Liability Litigation (MDL No. 2009-0001)

788 GENETICALLY ENGINEERED CORN CASES • IN RE: Syngenta AG MIR 162 Corn Products Liability Litigation (No. VI) (MDL No. 2009-0001)

1,716 NUVARING CONTRACEPTIVE CASES • IN RE: Nuvaring Contraceptive Cases (MDL No. 2009-0001)

2,138 DEEPATER HORIZON OIL SPILL CASES • IN RE: Horizon Oil Spill Cases (MDL No. 2009-0001)

4,804 ACTOS DIABETES MEDICATION CASES • IN RE: Actos Diabetes Medication Cases (MDL No. 2009-0001)

3,566 GRANUFLO/NATURALANT CONTRACEPTIVE CASES • IN RE: Granuflo/Naturalant Contraceptive Cases (MDL No. 2009-0001)

2,402 HIP IMPLANT CASES • IN RE: Hip Implant Products Liability Litigation (MDL No. 2009-0001)

2,200 MIRENA CONTRACEPTIVE CASES • IN RE: Mirena Contraceptive Cases (MDL No. 2009-0001)

3,068 HIP IMPLANT CASES • IN RE: Hip Implant Products Liability Litigation (MDL No. 2009-0001)

3,041 WATER CONTAMINATION CASES • IN RE: Water Contamination Cases (MDL No. 2009-0001)

1,254 ASBESTOS CASES • IN RE: Asbestos Products Liability Litigation (No. VI) (MDL No. 2009-0001)

10,763 PELVIC MESH PRODUCTS CASES • IN RE: Pelvic Mesh Products Liability Litigation (No. VI) (MDL No. 2009-0001)

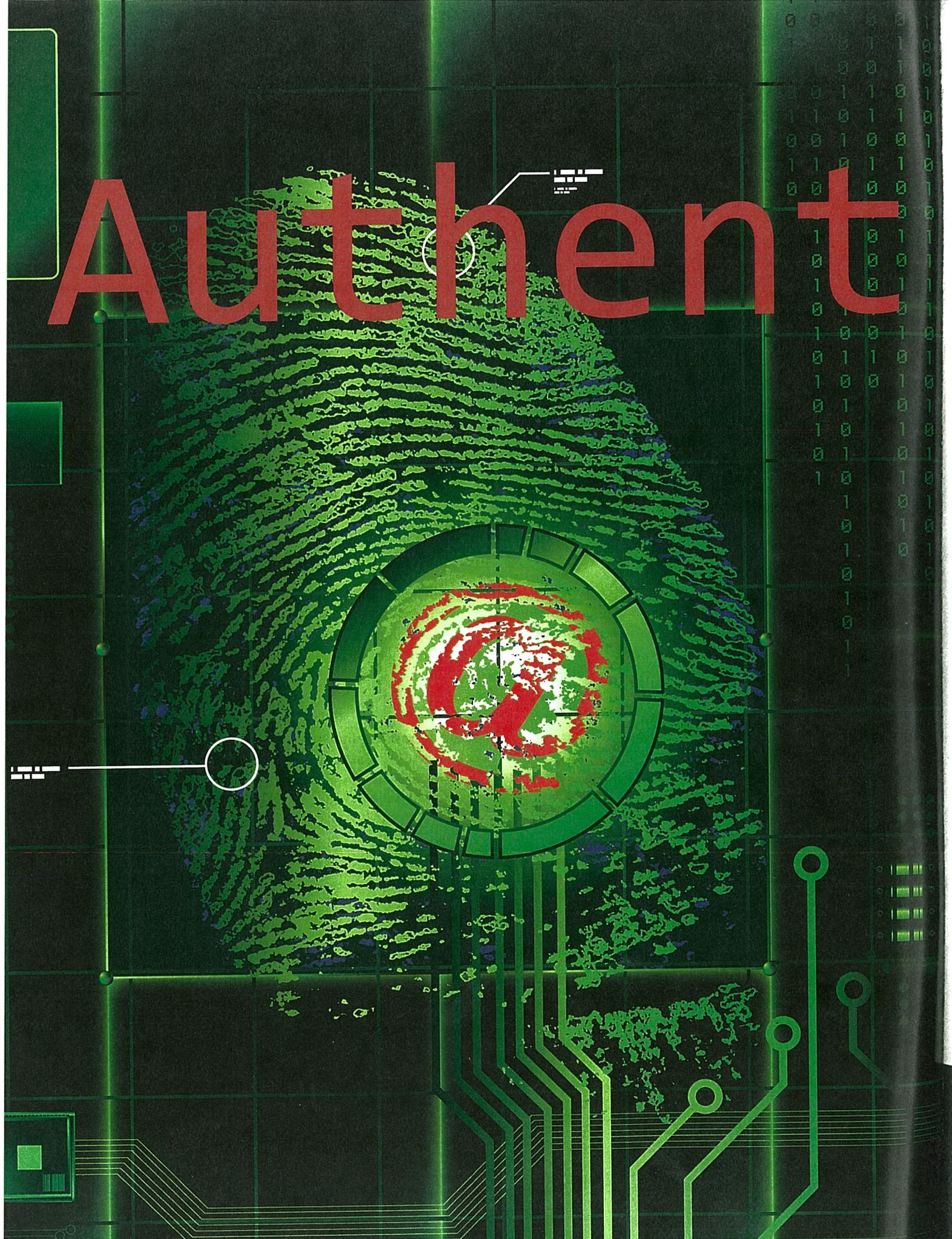
16,425 PELVIC MESH PRODUCTS CASES • IN RE: Pelvic Mesh Products Liability Litigation (No. VI) (MDL No. 2009-0001)

10,778 SKECHERS SHOE CASES • IN RE: Skechers Toning Shoe Products Liability Litigation (No. VI) (MDL No. 2009-0001)

JUSTICE SERVED - OR SUBSUMED?



# Authent



# ication

## What Every Judge and Lawyer Needs to Know About Electronic Evidence

by Gregory P. Joseph

**N**ot long ago, “friend” was a noun, “yelp” meant a shrill bark, “twitter” referred to a chirp, a “tumbler” was a gymnast or a glass, and “facebook,” “youtube,” and “instagram” were gibberish. Cases now rise and fall on the admissibility of Facebook profiles, Yelp reviews, Twitter tweets, YouTube videos, Instagram photos, Tumblr posts, and other social media evidence — and more conventional, but only slightly older, electronic data like text messages, emails, search engine results, and webpages (live or archived).

While the media are new, the applicable evidentiary principles are familiar and have easily adapted to them. The two overarching issues are authentication and hearsay. This article focuses on authentication beginning with the critical, and very distinct, roles of judge

and jury in deciding that question. The article then turns to authentication of website data, moving from conventional webpages to social media pages. It concludes with a discussion of email, text, and social media messages.

### I. JUDGE AS GATEKEEPER, JURY AS DECISION MAKER

The ultimate decision maker on the question of authentication is the finder of fact. The judge is gatekeeper, but this is not *Daubert*-intensive gatekeeping.

The principal authentication rule, Rule 901(a), provides that: “To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.” The court makes the initial decision under Rule 104(a) whether the proponent has

offered sufficient proof that a reasonable juror could find in favor of authenticity.<sup>1</sup> If so, then, under Rule 104(b),<sup>2</sup> the jury makes the ultimate determination as to whether the evidence is, in fact, what its proponent claims.<sup>3</sup>

“Importantly,” as the Fourth Circuit has observed, “the burden to authenticate under Rule 901 is not high . . . . [A] district court’s role is to serve as gatekeeper in assessing whether the proponent has offered a satisfactory foundation from which the jury could reasonably find that the evidence is authentic.”<sup>4</sup> “In performing its Rule 104 gate-keeping function, the trial court itself need not be persuaded that the proffered evidence is authentic. The preliminary question for the trial court to decide is simply whether the proponent of the evidence has supplied facts that are sufficient to support a



**GREGORY P. JOSEPH** is past president of the American College of Trial Lawyers; former Chair of the American Bar Association Section of Litigation; president of the Supreme Court Historical Society; a former member of the Advisory Committee on the Federal Rules of Evidence; the author of *Sanctions: The Federal Law of Litigation Abuse* (5th ed. 2013); *Civil RICO: A Definitive Guide* (4th ed. 2015); *Modern Visual Evidence* (Supp. 2015); and a member of the editorial board of *Moore’s Federal Practice* (3d ed. 1995-).

“Note that, while the contents of articles remain subject to hearsay analysis, if an article is more than 20 years old it is not excludable as hearsay because it is an “ancient document” under Rule 803(16), seemingly leading to the conclusion that incredible tabloid articles from the early ‘90s or before are admissible for their truth. Sometimes, common sense must intrude.

reasonable jury determination that the evidence he has proffered is authentic.”<sup>5</sup> At that point, the issue is for the jury.

## II. CONVENTIONAL WEBSITES

### Prima Facie Website Authentication

In applying Rule 901 authentication standards to website evidence, there are three questions that must be answered:

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

It is generally sufficient, in order to make a prima facie showing of authenticity, that a witness testifies — or certifies in compliance with a statute or rule — that:

1. The witness typed in the Internet address reflected on the exhibit on the date and at the time stated;

2. The witness logged onto the website and reviewed its contents; and
3. The exhibit fairly and accurately reflects what the witness perceived.<sup>6</sup>

The exhibit should bear the Internet address and the date and time the webpage was accessed and the contents downloaded.<sup>7</sup>

When evaluating the proffer, the court considers whether the exhibit bears indicia of reliability, such as:

- Distinctive website design, logos, photos, or other images associated with the website or its owner.
- The contents of the webpage are of a type ordinarily posted on that website or websites of similar people or entities.
- The contents of the webpage remain on the website for the court to verify.
- The owner of the website has elsewhere published the same

contents, in whole or in part.

- The contents of the webpage have been republished elsewhere and attributed to the website.
- The contents were posted on the website for some period of time.

The opponent of the evidence is free to challenge it by adducing facts showing that the exhibit does not accurately reflect the contents of a website, or that those contents are not attributable to the ostensible owner of the site. There may be legitimate questions concerning the ownership of the site or attribution of statements contained on the site to the ostensible owner.<sup>8</sup> More by way of authentication may be required of a proponent who is known to be an information technology specialist (that is, a computer geek) and is both able and motivated to modify the proffered website data.<sup>9</sup>

### Self-Authenticating Website Data

Three types of webpage exhibits are self-authenticating.

*Government Websites.* Under Rule 902(5) (*Official Publications*), “[a] book, pamphlet, or other publication purporting to be issued by a public authority” is self-authenticating. Rule 101(b)(6) provides that “a reference to any kind of written material or any other medium includes electronically stored information.” Hence, data on governmental websites are self-authenticating.<sup>10</sup> As discussed below, courts regularly take judicial notice of these websites.

*Newspaper & Periodical Websites.* Under Rule 902(6) (*Newspapers and Periodicals*), “[p]rinted material purporting to be a newspaper or periodical” is self-authenticating. Coupled with Rule 101(b)(6), which expands “printed” to include electronic data, newspaper, and periodical material that appears on the web — whether or not it ever appeared in hard copy — is self-authenticating.<sup>11</sup> As discussed below, courts regularly take judicial notice of these websites. (Note that,

while the contents of articles remain subject to hearsay analysis, if an article is more than 20 years old it is not excludable as hearsay because it is an “ancient document” under Rule 803(16), seemingly leading to the conclusion that incredible tabloid articles from the early '90s or before are admissible for their truth. Sometimes, common sense must intrude.)

*Websites Certified as Business Records.* Rules 902(11) and (12) render self-authenticating business (organizational) records that are certified as satisfying Rule 803(6) by “the custodian or another qualified person.” Exhibits extracted from websites that are maintained by, for, and in the ordinary course of a business or other regularly conducted activity can satisfy this rule.<sup>12</sup>

#### Judicial Notice of Website Evidence

“It is not uncommon for courts to take judicial notice of factual information found on the world wide web.”<sup>13</sup>

*Governmental Websites.* First and foremost among the types of Internet inference that may be judicially noticed is that taken from governmental websites,<sup>14</sup> including:

- Federal, state, and local court websites.<sup>15</sup>
- Federal, state, and local agency, department and other entities’ websites.<sup>16</sup>
- Foreign government websites.<sup>17</sup>
- International organization websites.<sup>18</sup>

Even this rule has exceptions, however. For example, one court found that data posted on the website of a governmental entity, which was a litigant before the court, was in conflict with all other evidence (including evidence before the governmental entity that posted the data) and was insufficiently trustworthy to warrant judicial notice.<sup>19</sup>

*Nongovernmental Websites.* Generally, and with some notable exceptions,

courts are reluctant to take judicial notice of nongovernmental websites because the Internet “contains an unlimited supply of information with varying degrees of reliability, permanence, and accessibility” and “is an open source” permitting anyone to “purchas[e] an Internet address and create a website.”<sup>20</sup>

*Familiar, Frequently Noticed Websites.* Nonetheless, there are many types of nongovernmental websites of which courts routinely take judicial notice, including:

- Internet maps (*e.g.*, Google Maps, MapQuest).<sup>21</sup>
- Calendar information.<sup>22</sup>
- Newspaper and periodical articles.<sup>23</sup>
- Online versions of textbooks, dictionaries, rules, charters.<sup>24</sup>

*Wayback Machine.* Archived versions of websites as displayed on The Wayback Machine ([www.archive.org](http://www.archive.org)) are frequently the subject of judicial notice,<sup>25</sup> but this is not always the case.<sup>26</sup> Note that it is only the contents of the archived pages that may warrant judicial notice — the dates assigned to archived pages may not apply to images linked to them, and more generally, links on archived pages may direct to the live web if the object of the old link is no longer available.<sup>27</sup>

*Corporate Websites.* For certain purposes, even private business websites may warrant judicial notice.<sup>28</sup> Much may turn on the purpose for which judicial notice is taken, the nature or stage of the proceedings, whether any party contests the taking of judicial notice, whether the evidence is in the nature of a party admission, the importance to the outcome of the case of the fact to be noticed, and other variables.<sup>29</sup>

#### III. SOCIAL MEDIA WEBSITES User-Created Pages

Anyone can create a Facebook or other social media page in anyone else’s name — that is, create a false identity, post a

phony social media page, send pseudonymous messages. Law enforcement does this with some regularity.<sup>30</sup> There is even instruction on the Internet in how to create a fake Facebook page.<sup>31</sup>

One person may also gain access to another’s account, which becomes easier and easier as people own more and more devices, each of which can be used to link to their social media accounts.

Courts are, therefore, circumspect in their approach to authentication of social media evidence.

Both the social media page and the particular post must be linked to the purported author.<sup>32</sup> This can be done in a variety of ways, including:

- An admission from the purported author, in or out of court, that he or she created the page or posted the item.
- Testimony of a witness who saw the purported author post the item to the page.
- Testimony of a witness that she often communicated with the alleged creator of the page through that account.
- A forensic review of the Internet history and hard drive of the purported author’s computer or other devices.
- Information from the social media network that links the page or post to the purported author.
- Circumstantial evidence derived from:
  - Witness testimony (Rule 901(a), (b)(1)).
  - Distinctive characteristics of the contents themselves and corroborative circumstances (Rule 901(b)(4)).
  - Descriptions and explanations of the technical process or system that generated the evidence (Rule 901(b)(9)).

Among the circumstantial factors that may tip the scales in favor of, or against, putting the issue to the jury for final determination are:

- Whether the purported author knows the password to the account.
- How many others know it as well.
- That the page or post contains:
  - Nonpublic details of the purported author's life.
  - Other items known uniquely to the purported author or a small group including him or her.
  - References or links to, or contact information about, loved ones, relatives, co-workers, others close to the purported author.
  - Photos, videos.
  - Cell numbers.
  - Nicknames.
  - Biographical information.
  - The structure or style of comments.
  - That the purported author acts in accordance with the contents of the page or post.<sup>33</sup>

### Social Media Conversations and Website Chats

Evidence of social media conversations or more conventional website chats may be of interest only to the extent that the person who left a salient posting can be identified. Simply to show that a posting appears on a particular user's webpage is insufficient to authenticate the post as one written by the account holder.<sup>34</sup> Third-party posts, too, must be authenticated by more than the names of the purported authors reflected on the posts.<sup>35</sup> Evidence sufficient to attribute a social media or chat room posting to a particular individual may include, for example:

- Testimony from a witness who identifies the social media account as that of the alleged author and one on which the witness on other occasions communicated with the account holder.<sup>36</sup>
- Testimony from a participant in the conversation based on firsthand knowledge that the transcript fairly and accurately captures the conversation.<sup>37</sup>

- Evidence that the purported author used the same screen name on other occasions.<sup>38</sup>
- Evidence that the purported author acted in accordance with the posting (e.g., when a meeting with that person was arranged, he or she attended).<sup>39</sup>
- Evidence that the purported author identified him- or herself as the individual using the screen name.
- An admission that the social media account containing the chat is that of the alleged author.<sup>40</sup>
- Use in the conversation of the customary signature, nickname, or emoticon associated with the individual.<sup>41</sup>
- Disclosure in the conversation of particularized information that is either unique to the purported author or known only to a small group including the individual.<sup>42</sup>
- Evidence that the individual had in his or her possession information given to the person using the screen name.
- Evidence from the hard drive of the purported author's computer reflecting that a user of the computer used the screen name in question.<sup>43</sup>
- Evidence that the chat appears on the computer or other device of the account owner and purported author.<sup>44</sup>
- Evidence that the purported author elsewhere discussed the same subject matter.<sup>45</sup>

### YouTube and Other Online Videos

The first step in authenticating an online video is to satisfy the three-part test for website evidence generally. That requires evidence that a witness accessed a particular page on a particular site (we will use YouTube as the paradigm) and reviewed what was on the page, and that a proffered video fairly and accurately reflects what the witness saw. *See* § II(A), *supra*.

A YouTube video can be authenticated circumstantially with evidence identifying the individual and items depicted, and establishing where and roughly when the video was recorded, without evidence from YouTube (Google) personnel.<sup>46</sup>

A YouTube video can be rendered self-authenticating by obtaining and proffering a Rule 902(11) or (12) certification from a Google custodian of records that the video was captured and maintained on the company's servers in the ordinary course of business at or near the time that users post them.<sup>47</sup> If the YouTube video is posted on a Facebook page, that certification should be accompanied by a similar Rule 902(11) certification from a Facebook custodian of records that the page was captured and maintained on Facebook servers in the ordinary course of business.<sup>48</sup>

### Yelp and Other Online Reviews

The first step in authenticating an online review is to satisfy the three-part test for website evidence generally, which is set forth in § II(A), *supra*. In addition to proving that the review was posted on the site, it is often essential that it identify the author. Identification can be established circumstantially — for example, by:

- The review's similarity to the alleged author's other writings.
- The reviewer's use of a pseudonym or screen name used elsewhere by the alleged author.
- The reviewer's use of pseudonyms that share the alleged author's actual initials.
- The alleged author repeating the substance of the review elsewhere.
- The alleged author's failure affirmatively to deny authorship.<sup>49</sup>

### Instagram and Other Online Photo Sites

The first step in authenticating an Instagram photo is to satisfy the three-part test for website evidence generally, which is set forth in § II(A),

*supra*. Testimony from a witness that the witness downloaded a photo from Instagram and that the exhibit fairly and accurately reflects it may suffice to authenticate it.<sup>50</sup>

#### IV. EMAIL AND TEXT MESSAGES

##### Conventional Emails and Texts

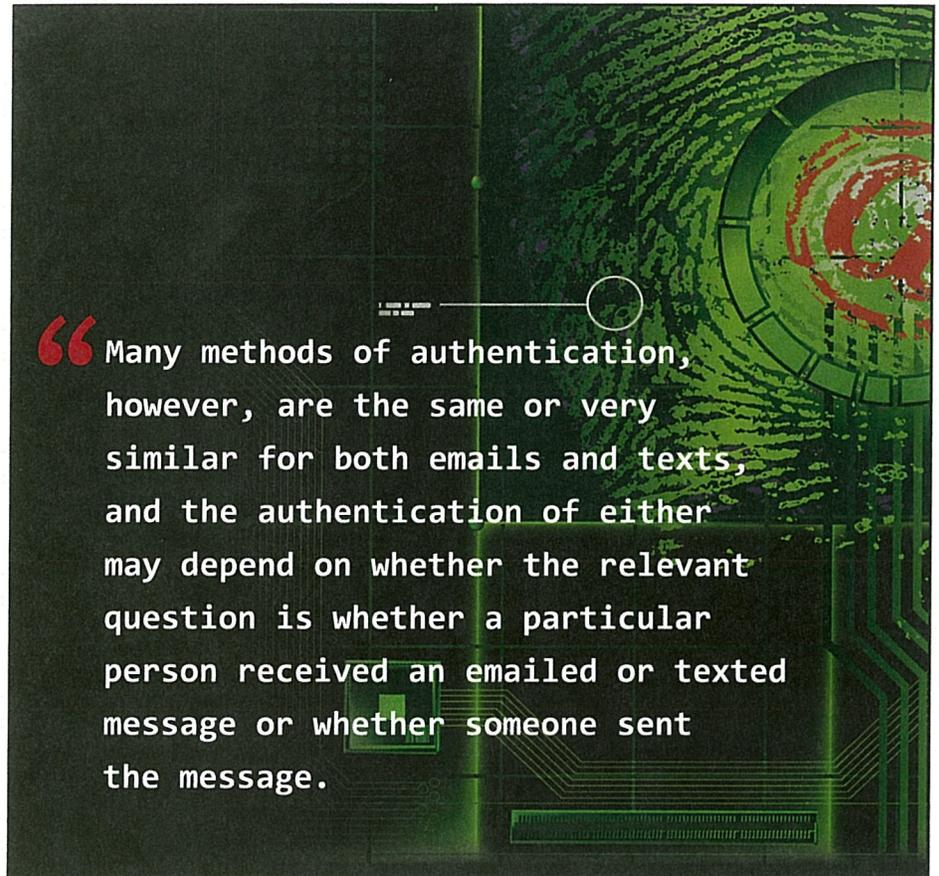
The mere fact that an email purports to come from someone's email address or a text emanates from a person's cell phone or other device typically is insufficient to authenticate a message as coming from a particular individual.<sup>51</sup>

Some methods of authenticating emails and texts are unique to the medium. For example, the "@" designation of origin in an email address has been held sufficient to self-authenticate the email as having been sent by the organization.<sup>52</sup>

Many methods of authentication, however, are the same or very similar for both emails and texts, and the authentication of either may depend on whether the relevant question is whether a particular person *received* an emailed or texted message or whether someone *sent* the message.

*Whether a Particular Person Received a Message.* Receipt of an email or text may be proved circumstantially with evidence that the message was sent to the email address or phone number assigned at the time to the person, and receipt is corroborated by circumstantial evidence, such as:

- A reply to the email was received from the email address or phone number assigned to the person.<sup>53</sup>
- Subsequent communications with the person reflect the person's knowledge of the contents of the message.<sup>54</sup>
- Subsequent conduct of the person reflects the person's knowledge of the contents of the message.<sup>55</sup>
- A participant to an electronic conversation testifies that an exhibit fairly and accurately reflects the messages exchanged with the recipient.<sup>56</sup>



“Many methods of authentication, however, are the same or very similar for both emails and texts, and the authentication of either may depend on whether the relevant question is whether a particular person received an emailed or texted message or whether someone sent the message.”

- The person produced the message in the action.<sup>57</sup>

*Whether a Particular Person Sent a Message.* That a particular person sent a specific email or text may be proved circumstantially with evidence that the message was received from the email address or phone number assigned at the time to the person and receipt is corroborated by circumstantial evidence, such as:

- The message contained the type-written name, nickname, or initials of the recipient or the sender,<sup>58</sup> or reflected the sender's customary use of emoji or emoticons.
- If an email, the message contained the signature block or electronic signature of the person.<sup>59</sup>
- If a text, the sender's cell phone number or name as displayed on the cell phone or other device of the recipient.<sup>60</sup>
- The contents of the message would

normally be known only to the person or to a discrete number or category of people including the person.<sup>61</sup>

- Subsequent or contemporaneous communications with the person reflect the person's knowledge of the contents of the message.<sup>62</sup>
- Subsequent conduct of the person reflects the person's knowledge of the contents of the message.<sup>63</sup>
- The recipient had previously communicated with the sender at the same cell number or email address.<sup>64</sup>
- The sender told the recipient that he would email or text her, and she soon received a text from an account she knew was his.<sup>65</sup>
- The sender alone (or among a small group) had the motive to send the message.<sup>66</sup>
- The absence of evidence that anyone had the motive or opportunity to impersonate the sender in sending the message.<sup>67</sup>

- The alleged sender or recipient knows the password to the computer, cell phone, or other device from which the message was sent.<sup>68</sup>
- Evidence that the message was sent from the computer or other device of the purported author.<sup>69</sup>
- External corroboration that statements made by the alleged sender in the message concerning his or her whereabouts are accurate.<sup>70</sup>
- The tone, syntax, appearance, and other characteristics of the message are consistent with that of other communications from the alleged sender.<sup>71</sup>
- The person produced the message in the action.<sup>72</sup>

### Social Media Messages

Authentication of messages sent over a social network is, at the outset, the same as authentication of other messages. Because anyone can create a social media identity in anyone else's name, "the fact that an electronic communication on its face purports to originate from a certain person's social networking account is generally insufficient standing alone to authenticate that person as the author of the communication."<sup>73</sup> Consequently, "[t]here must be some 'confirming' circumstances' sufficient for a reasonable jury to find by a preponderance of the evidence that the [purported author in fact] authored the e-mails."<sup>74</sup> "So long as the authenticity of the proffered evidence was at least 'within

the zone of reasonable disagreement,' the jury [i]s entitled to weigh the credibility of the [witnesses] and decide who was telling the truth."<sup>75</sup>

Circumstantial indicia of authorship or receipt parallels those used for email and text messages, coupled with the indicia for social media conversations, all as discussed above.

### Conclusion

To borrow from the Second Circuit, speaking in another context: "[A]ttempting to apply established [evidence] law in the fast-developing world of the Internet is somewhat like trying to board a moving bus."<sup>76</sup> So far, however, the Rules and the courts have been fully up to the challenge.

<sup>1</sup> FED. R. EVID. 104(a) provides: "The court must decide any preliminary question about whether a witness is qualified, a privilege exists, or evidence is admissible. In so deciding, the court is not bound by evidence rules, except those on privilege."

<sup>2</sup> FED. R. EVID. 104(b) provides: "When the relevance of evidence depends on whether a fact exists, proof must be introduced sufficient to support a finding that the fact does exist. The court may admit the proposed evidence on the condition that the proof be introduced later."

<sup>3</sup> See generally *United States v. Vayner*, 769 F.3d 125, 129–31 (2d Cir. 2014); *United States v. Mebriatu*, 543 F. App'x 137, 140–41 (3d Cir. 2013); *Sublet v. State*, No. 42, 2015 Md. LEXIS 289, at \*44–45, 52–53 (Md. Ct. App. Apr. 23, 2015); *Parker v. State*, 85 A.3d 682, 688 (Del. 2014); *Tienda v. State*, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012); *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 539–40 (D. Md. 2007).

<sup>4</sup> *United States v. Hassan*, 742 F.3d 104, 133 (4th Cir. 2014).

<sup>5</sup> *Tienda v. State*, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012).

<sup>6</sup> See, e.g., *O'Connor v. Newport Hosp.*, No. 2012–

87, 2015 R.I. LEXIS 35 (R.I. Sup. Ct. Mar. 17, 2015) ("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."); *Estate of Konell v. Allied Prop. & Cas. Ins. Co.*, No. 3:10-cv-955-ST, 2014 U.S. Dist. LEXIS 10183 (D. Or. Jan. 28, 2014) ("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."); *Smoot v. State*, 729 S.E.2d 416 (Ga. Ct. App. 2012) ("[T]o authenticate a printout from a web page, the proponent must present evidence from a percipient witness stating that the printout accurately reflects the content of the page and the image of the page on the computer at which the printout was made."), quoting *Nightlight Sys. v. Nighlites Franchise Sys.*, No. 1:04-CV-2112-CAP, 2007 U.S. Dist. LEXIS 95538, at \*16 (N.D. Ga. May 11, 2007).

<sup>7</sup> See, e.g., *Foreword Magazine, Inc. v. OverDrive Inc.*, No. 1:10-cv-1144, 2011 WL 5169384, at \*4 (W.D. Mich. Oct. 31, 2011) (admitting screenshots from websites, accompanied only by the sworn affidavit of an attorney, given "other indicia of reliability (such as the

Internet domain address and the date of print-out)"); *accord Lebewobl v. Heart Attack Grill, LLC*, 890 F. Supp. 2d 278 (S.D.N.Y. 2012); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1154 (C.D. Cal. 2002).

<sup>8</sup> See, e.g., *Boim v. Holy Land Found.*, 511 F.3d 707 (7th Cir. 2007) ("Where, as here, the expert appears to be relying to a great extent on web postings to establish a particular fact, and where as a result the factfinder would be unable to evaluate the soundness of his conclusion without hearing the evidence he relied on, we believe the expert must lay out, in greater detail than [plaintiff's expert] did, the basis for his conclusion that these websites are in fact controlled by Hamas and that the postings he cites can reasonably and reliably be attributed to Hamas.")

<sup>9</sup> See, e.g., *United States v. Jackson*, 208 F.3d 633, 637 (7th Cir. 2000) ("Jackson needed to show that the web postings in which the white supremacist groups took responsibility for the racist mailing actually were posted by the groups, as opposed to being slipped onto the groups' web sites by Jackson herself, who was a skilled computer user.")

<sup>10</sup> See, e.g., *Williams v. Long*, 585 F. Supp.2d 679, 686–88 & n. 4 (D. Md. 2008) (collecting cases indicating that postings on government websites are inherently authentic or self-authenticating).

<sup>11</sup> See, e.g., *White v. City of Birmingham*, No. 2:13-cv-00099-KOB, 2015 U.S. Dist. LEXIS 39187 (N.D. Ala. Mar. 27, 2015) (noting sua sponte that news articles from Huntsville

Times website (AL.com) "could be found self-authenticating at trial").

- <sup>12</sup> See, e.g., *United States v. Hassan*, 742 F.3d 104, 132–34 (4th Cir. 2014) (Facebook posts, including YouTube videos, accompanied by certificates from Facebook and Google custodians "verifying that the Facebook pages and YouTube videos had been maintained as business records in the course of regularly conducted business activities" were self-authenticating under Rules 803(6) and 902(11)).
- <sup>13</sup> *O'Toole v. Northrop Grumman Corp.*, 499 F.3d 1218, 1224 (10th Cir. 2007), quoted with approval in many cases, including, e.g., *Juniper Networks, Inc. v. Shipley*, 394 F. App'x 713, 713 (Fed. Cir. 2010), and *Jeandron v. Bd. of Regents of Univ. Sys. of Md.*, 510 F. App'x 223, 227 (4th Cir. 2013).
- <sup>14</sup> See, e.g., *United States v. Head*, No. 08-CR-116, 2013 U.S. Dist. LEXIS 151805, at \*7 n.2 (E.D. Cal. Oct. 22, 2013) ("The court may take judicial notice of information posted on government websites as it can be 'accurately and readily determined from sources whose accuracy cannot reasonably be questioned.'"); *In re MTBE Prods. Liab. Litig.*, No. 1:00-1898, 2013 U.S. Dist. LEXIS 181837, at \*16 (S.D.N.Y. Dec. 30 2013) ("Courts routinely take judicial notice of data on government websites because it is presumed authentic and reliable.").
- <sup>15</sup> See, e.g., *Feingold v. Graff*, 516 F. App'x 223, 226 (3d Cir. 2013); *Whittington v. Isgrig*, No. 2:13CV16DDN, 2013 U.S. Dist. LEXIS 127297, at \*2–3 n.1 (E.D. Mo. Sept. 6, 2013); *Ceras v. Janda*, No. CV 14-09177, 2014 U.S. Dist. LEXIS 175586 (C.D. Cal. Dec. 18, 2014); *Mortensen v. Mortg. Elec. Registration Sys.*, No. CV10-234-S-EJL, 2012 U.S. Dist. LEXIS 140923, at \*5, \*8–9 n.5 (D. Idaho Sept. 26, 2012).
- <sup>16</sup> See, e.g., *Lawrence v. Fed. Home Loan Mortg. Corp.*, No. A-13-CV-913, 2015 U.S. Dist. LEXIS 40012 (W.D. Tex. Mar. 30, 2015) (federal government's agreement with national bank as posted on government website); *Flores v. City of Baldwin Park*, No. 14-9290-MWF, 2015 U.S. Dist. LEXIS 22149 (C.D. Cal. Feb. 23, 2015) (municipal police department website); *United States v. Washington*, No. 70-9213, 2013 U.S. Dist. LEXIS 48850, at \*58 & n.26 (W.D. Wash. 2013) (state DOT's website); *Golden v. Absolute Collection Servs.*, No. 1:12CV956, 2013 U.S. Dist. LEXIS 77998, at \*2 (M.D.N.C. June 4, 2013) (state secretary of state website); *Taylor v. Shore*, No. 8:11-CV-2137-T-17TBM, 2013 U.S. Dist. LEXIS 90603, at \*3 (M.D. Fla. June 27, 2013) (county website); *Casterline v. OneWest Bank, FSB*, No. C-12-150, 2012 U.S. Dist. LEXIS 163222 (S.D. Tex. Oct. 10, 2012) (records on FDIC website); *Daniels-Hall v. Nat'l Educ. Ass'n.*, 629 F.3d 992, 998–99 (9th Cir. 2010) (school district websites); *In re Amgen Inc. Sec. Litig.*, 544 F. Supp. 2d 1009, 1023–24 (C.D. Cal. 2008) (FDA website).
- <sup>17</sup> See, e.g., *United States v. Broxmeyer*, 699 F.3d 265, 296 (2d Cir. 2012) (websites of governments of Vietnam and Brazil).
- <sup>18</sup> See, e.g., *Kirtsang v. John Wiley & Sons, Inc.*, 133 S. Ct. 1351, 1367 (2013) (World Bank website).
- <sup>19</sup> *Spokane Cnty. v. E. Wash. Growth Mgmt. Hearings Bd.*, No. 31941-5-III, 2015 Wash. App. LEXIS 755 (Wash. Ct. App. Apr. 9, 2015).
- <sup>20</sup> *United States v. Kane*, No. 2:13-cr-250-JAD-VCF, 2013 U.S. Dist. LEXIS 154248 (D. Nev. Oct. 28, 2013) (citing *Pickett v. Sheridan Health Care Ctr.*, 664 F.3d 632, 648 (7th Cir. 2011)). See also *Victaulic Co. v. Tieman*, 499 F.3d 227, 236 (3d Cir. 2007) ("First, . . . [a]nyone may purchase an Internet address, and so . . . it is premature to assume that a webpage is owned by a company merely because its trade name appears in the uniform resource locator. . . . Second, a company's website is a marketing tool. . . . Thus courts should be wary of finding judicially noticeable facts amongst all the fluff.").
- <sup>21</sup> See, e.g., *United States v. Brooks*, 715 F.3d 1069, 1078 (8th Cir. 2013); *Pabls v. Thomas*, 718 F.3d 1210, 1216 n.1 (10th Cir. 2013); *United States v. Schultz*, 537 F. App'x. 702, 703–04 (9th Cir. 2013); *Xtreme Caged Combat v. ECC Fitness*, No. 12-cv-3855, 2013 U.S. Dist. LEXIS 162055, at \*6 n.4 (E.D. Pa. Nov. 12, 2013); *Miller v. Bennett*, No. 12-cv-02063-MSK-CBS, 2013 U.S. Dist. LEXIS 129011 (D. Colo. Aug. 12, 2013).
- <sup>22</sup> See, e.g., *Tyler v. United States*, No. 1:08-CR-165-CC-JSA, 2012 U.S. Dist. LEXIS 184007, at \*9–10 n.6 (N.D. Ga. Dec. 6, 2012); *Local 282, Int'l Bhd. of Teamsters v. Pile Found. Constr. Co.*, No. 09-cv-4535(KAM)(LB), 2011 U.S. Dist. LEXIS 86644, at \*17–18 n.5 (E.D.N.Y. Aug. 5, 2011).
- <sup>23</sup> See, e.g., *Ford v. Artiga*, No. 2:12-CV-02370, 2013 U.S. Dist. LEXIS 106805, at \*19 n.5 (E.D. Cal. July 30, 2013); *HB v. Monroe Woodbury Cent. Sch. Dist.*, No. 11-CV-5881, 2012 U.S. Dist. LEXIS 141252 (S.D.N.Y. Sept. 27, 2012).
- <sup>24</sup> See, e.g., *United States v. Mosley*, 672 F.3d 586, 591 (8th Cir. 2012) (Physicians' Desk Reference); *Shuler v. Garrett*, 743 F.3d 170 (6th Cir. 2014) (Oxford English Dictionary); *Dealer Computer Servs. v. Monarch Ford*, No. 1:12-CV-01970-LJO-SKO, 2013 U.S. Dist. LEXIS 11237, at \*11 & n.3 (E.D. Cal. Jan. 25, 2013) (American Arbitration Association rules); *Morgan Stanley Smith Barney LLC v. Monaco*, No. 14-cv-00275-RM-MJW, 2014 U.S. Dist. LEXIS 149419 (D. Colo. Aug. 26, 2014) (FINRA rules); *Famous Music Corp. v. 716 Elmwood, Inc.*, No. 05-CV-0885A(M), 2007 U.S. Dist. LEXIS 96789, at \*12–13 n.7 (W.D.N.Y. Dec. 28, 2007) (Articles of Association of ASCAP).
- <sup>25</sup> See, e.g., *Under a Foot Plant Co. v. Exterior Design, Inc.*, No. 6:14-cv-01371-AA, 2015 U.S. Dist. LEXIS 37596 (D. Md. Mar. 24, 2015) ("District courts have routinely taken judicial notice of content from The Internet Archive."); *Tompkins v. 23andMe, Inc.*, No. 5:13-CV-05682-LHK, 2014 U.S. Dist. LEXIS 88068 (N.D. Cal. June 25, 2014); *The Pond Gray, Inc. v. Aquascape Designs, Inc.*, No. 13-13229, 2014 U.S. Dist. LEXIS 85504 (E.D. Mich. June 24, 2014); *Martins v. 3PD, Inc.*, No. 11-11313-DPW, 2013 U.S. Dist. LEXIS 45753, at \*16 n.8 (D. Mass. Mar. 28, 2013); *In re MTBE Prods. Liab. Litig.*, No. 1:00-1898, 2013 U.S. Dist. LEXIS 181837, at \*16–18 n. 65 (S.D.N.Y. Dec. 30, 2013).
- <sup>26</sup> See, e.g., *Open Text S.A. v. Box, Inc.*, No. 13-cv-04910-JD, 2015 U.S. Dist. LEXIS 11312 (N.D. Cal. Jan. 30, 2015) (proffered Wayback Machine printouts not authenticated absent certification from representative of archive.org).
- <sup>27</sup> See *United States ex rel. Oliver v. Philip Morris USA, Inc.*, No. 08-0034, 2015 U.S. Dist. LEXIS 56655 (D.D.C. Apr. 30, 2015).
- <sup>28</sup> See, e.g., *Capitol Records, LLC v. Escape Media Grp., Inc.*, No. 12-CV-6646, 2015 U.S. Dist. LEXIS 38007 (S.D.N.Y. Mar. 25, 2015) (judicial notice of corporate website for the purpose of ascertaining the service it offered); *Frankfort GGNSC Frankfort, LLC v. Tracy*, No. 14-30-GFVT, 2015 U.S. Dist. LEXIS 41466 (E.D. Ky. Mar. 31, 2015) (judicial notice of private business's website for its discussion of methods of payment accepted); *Smith v. United States Cong.*, No. 3:12CV45, 2015 U.S. Dist. LEXIS 27818 (E.D. Va. Mar. 6, 2015) (judicial notice of products available for sale); *Allphin v. Peter K. Fitness, LLC*, No. 13-cv-01338-BLF, 2014 U.S. Dist. LEXIS 171711 (N.D. Cal. Dec. 11, 2014) (judicial notice of parties' websites to determine personal jurisdiction (collecting cases)); *Saint Laurie Ltd. v. Yves Saint Laurent Am., Inc.*, No. 13-V-6857, 2015 U.S. Dist. LEXIS 42621 (S.D.N.Y. Mar. 26, 2015) (judicial notice of corporate website for fact of trademarks displayed); *In re Reynolds*, No. 9:14-bk-10690-PC, 2015 Bankr. LEXIS 732 (Bankr. C.D. Cal. Mar. 9, 2015) (judicial notice of website of firm seeking attorney's fees for lawyers' biographical data to assess reasonableness of hourly rates sought).

- <sup>29</sup> If you are not yet tired of the topic, see Gregory P. Joseph, *Judicial Notice of Internet Evidence*, U.S. LAW WEEK, Vol. 82, No. 34 (Mar. 11, 2014).
- <sup>30</sup> See, e.g., *United States v. Gatson*, No. 13-705, 2014 U.S. Dist. LEXIS 173588 (D.N.J. Dec. 15, 2014) (“[L]aw enforcement officers used an undercover account to become Instagram ‘friends’ with Gatson. Gatson accepted the request to become friends. As a result, law enforcement officers were able to view photos and other information Gatson posted to his Instagram account. No search warrant is required for the consensual sharing of this type of information.”). See also Sari Horwitz, *Justice Dept. Will Review Practice of Creating Fake Facebook Profiles*, WASH. POST (Oct. 7, 2014), available at [http://www.washingtonpost.com/world/national-security/justice-dept-will-review-practice-of-creating-fake-facebook-profiles/2014/10/07/3f9a2fe8-4e57-11e4-aa5e-7153e466a02d\\_story.html](http://www.washingtonpost.com/world/national-security/justice-dept-will-review-practice-of-creating-fake-facebook-profiles/2014/10/07/3f9a2fe8-4e57-11e4-aa5e-7153e466a02d_story.html).
- <sup>31</sup> See, e.g., *How to Make a Fake Facebook Page Seem Real*, <http://www.wikihow.com/Make-a-Fake-Facebook-Page-Seem-Real> (last visited May 19, 2015) (stating that as of this date this “page . . . has been read 80,838 times”).
- <sup>32</sup> See, e.g., *People v. Glover*, No. 13CA0098, 2015 Colo. App. LEXIS 295 (Colo. Ct. App. Feb. 26, 2015).
- <sup>33</sup> See generally *United States v. Vayner*, 769 F.3d 125 (2d Cir. 2014); *Parker v. State*, 85 A.3d 682 (Del. 2014); *Sublet v. State*, No. 42, 2015 Md. LEXIS 289 (Md. Ct. App. Apr. 23, 2015); *Moore v. State*, 763 S.E.2d 670 (Ga. 2014); *Smith v. State*, 136 So. 3d 424 (Miss. 2014); *State v. Gibson*, No. L-13-1222, 2015 Ohio App. LEXIS 1614 (Ohio Ct. App. May 1, 2015); *Wilson v. State*, No. 45A03-1409-CR-317, 2015 Ind. App. LEXIS 378 (Ind. Ct. App. Apr. 30, 2015); *People v. Glover*, No. 13CA0098, 2015 Colo. App. LEXIS 295 (Colo. Ct. App. Feb. 26, 2015); *State v. Jones*, 318 P.3d 1020 (Kan. Ct. App. 2014).
- <sup>34</sup> See, e.g., *Glover*, 2015 Colo. App. LEXIS 295; *Sublet*, 2015 Md. LEXIS 289.
- <sup>35</sup> See, e.g., *Dering v. State*, No. 11-13-00076-CR, 2015 Tex. App. LEXIS 2899 (Tex. Ct. App. Mar. 26, 2015).
- <sup>36</sup> See, e.g., *Glover*, 2015 Colo. App. LEXIS 295.
- <sup>37</sup> See, e.g., *United States v. Lebowitz*, 676 F.3d 1000 (11th Cir. 2012) (Internet chat authenticated by credible testimony of one participant); *United States v. Lundy*, 676 F.3d 444 (5th Cir. 2012) (testimony by one party to chat “that the chats are as he recorded them is enough to meet the low threshold for authentication”); *United States v. Barlow*, 568 F.3d 215 (5th Cir. 2009) (“English, as the other participant in the year-long ‘relationship,’ had direct knowledge of the chats. Her testimony could sufficiently authenticate the chat log presented at trial.”).
- <sup>38</sup> See, e.g., *State v. Koch*, 334 P.3d 280 (Idaho 2014).
- <sup>39</sup> See, e.g., *Sublet v. State*, 2015 Md. LEXIS 289.
- <sup>40</sup> See, e.g., *State v. Burns*, No. M2014-00357-CCA-R3-CD, 2015 Tenn. Crim. App. LEXIS 325 (Tenn. Ct. App. May 5, 2015).
- <sup>41</sup> See, e.g., *Moore v. State*, 763 S.E.2d 670 (Ga. 2014).
- <sup>42</sup> See, e.g., *State v. Snow*, 437 S.W.3d 396, 403 (Mo. Ct. App. 2014); *Moore*, 763 S.E.2d at 670.
- <sup>43</sup> See, e.g., *United States v. Manning*, 738 F.3d 937 (8th Cir. 2014); *United States v. Barlow*, 568 F.3d 215 (5th Cir. 2009); *United States v. Gagliardi*, 506 F.3d 140 (2d Cir. 2007); *United States v. Burt*, 495 F.3d 733, 738–39 (7th Cir. 2007); *United States v. Tank*, 200 F.3d 627, 630–31 (9th Cir. 2000); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1154 (C.D. Cal. 2002); *United States v. Simpson*, 152 F.3d 1241, 1249–50 (10th Cir. 1998).
- <sup>44</sup> See, e.g., *Burns*, 2015 Tenn. Crim. App. LEXIS 325.
- <sup>45</sup> See, e.g., *Sublet*, 2015 Md. LEXIS 289.
- <sup>46</sup> See, e.g., *United States v. Broomfield*, 591 F. App’x 847 (11th Cir. 2014).
- <sup>47</sup> See, e.g., *United States v. Hassan*, 742 F.3d 104, 132–33 (4th Cir. 2014); *Randazza v. Cox*, No. 2:12-cv-2040-JAD-PAL, 2014 U.S. Dist. LEXIS 49762 (D. Nev. Apr. 10, 2014).
- <sup>48</sup> See, e.g., *Hassan*, 742 F.3d at 132–33.
- <sup>49</sup> See generally *Judge v. Randell*, No. A138481, 2014 Cal. App. Unpub. LEXIS 4767 (Cal. Ct. App. July 7, 2014); *Pham v. Lee*, No. H039184, 2014 Cal. App. Unpub. LEXIS 8812 (Cal. Ct. App. Dec. 11, 2014).
- <sup>50</sup> See, e.g., *Camowraps, LLC v. Quantum Digital Ventures LLC*, No. 13-6808, 2015 U.S. Dist. LEXIS 16091 (E.D. La. Feb. 10, 2015) (“Defendants have submitted affidavits of the individuals who accessed the [Instagram] web pages which, in combination with information available on the face of the printouts themselves, suffice to establish that the printouts are what defendants claim them to be as required by Rule 901(a) of the Federal Rules of Evidence.”) (citing *Foreword Magazine, Inc. v. OverDrive, Inc.*, No. 1:10-cv-1144, 2011 WL 5169384, at \*3 (W.D. Mich. Oct. 31, 2011) (finding “screen shots of Internet websites” authenticated on the basis of affidavits “along with other indicia of reliability (such as the Internet domain address and the date of printout)”)); see also *In re D.H.*, 2015 Cal. App. Unpub. LEXIS 867 (Cal. Ct. App. Feb. 6, 2015).
- <sup>51</sup> See, e.g., *People v. Glover*, No. 13CA0098, 2015 Colo. App. LEXIS 295 (Colo. Ct. App. Feb. 26, 2015); *Tienda v. State*, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012).
- <sup>52</sup> FED. R. EVID. 902(7) provides for self-authentication of “Trade inscriptions and the like. Inscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin.” See, e.g., *Superhighway Consulting, Inc. v. Techwave, Inc.*, No. 98CV5502, 1999 U.S. Dist. LEXIS 17910, at \*6 (N.D. Ill. 1999).
- <sup>53</sup> See, e.g., *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.”); *Tienda*, 358 S.W.3d at 641; *Varkonyi v. State*, 276 S.W.3d 27, 35 (Tex. Ct. App.), review denied 2008 Tex. Crim. App. LEXIS 1634 (Tex. Ct. Crim. App. Oct. 29, 2008).
- <sup>54</sup> See, e.g., *Meyer v. Callery Conway Mars HV, Inc.*, No. 2:13-cv-00109, 2015 U.S. Dist. LEXIS 937 (W.D. Pa. Jan. 5, 2015); *Donati v. State*, 215 Md. App. 686 (Md. Ct. Spec. App. 2014), cert denied, 438 Md. 143 (2014); *Shea v. State*, 167 S.W.3d 98, 105 (Tex. Ct. App. 2005), discretionary review denied, 2005 Tex. Crim. App. LEXIS 1951 (Tex. Ct. Crim. App. Nov. 9, 2005); *Bloom v. Commonwealth of Virginia*, 542 S.E.2d 18, 20–21 (Va. Ct. App. 2001); *Dominion Nutrition, Inc. v. Cesta*, No. 04C4902, 2006 U.S. Dist. LEXIS 15515, at \*16 (N.D. Ill. Mar. 2, 2006); (“E-mail communications may be authenticated as being from the purported author based on . . . other communications from the purported author acknowledging the e-mail communication that is being authenticated.”) (quoting *Fenje v. Feld*, 301 F. Supp. 2d, 781 (N.D. Ill. 2003)), *aff’d*, 398 F.3d 620 (7th Cir. 2005)).
- <sup>55</sup> See, e.g., *Commonwealth v. Czubinski*, 26 N.E.3d 753 (Mass. App. Ct. 2015) (author leaves voicemail with substantially the same content); *Commonwealth v. Amaral*, 941 N.E.2d 1143, 1147 (Mass. App. Ct. 2011) (“One e-mail indicated that Jeremy would be at a certain place at a certain time and the defendant appeared at that place and time. In other e-mails, Jeremy provided his telephone number and photograph. When the trooper called that number, the defendant immediately answered his telephone, and the photograph was a picture of the defendant. These actions served to confirm that the author of the e-mails and the defendant were one and the same.”) (citing Mass. G. Evid. § 901(b)(6)). See also *State v. Glass*, 190 P.3d 896, 901 (Idaho Ct. App. 2008) (same re online chat).

- <sup>56</sup> See, e.g., *Peña v. State*, No. 04-14-00177-CR, 2015 Tex. App. LEXIS 3710 (Tex. App. Apr. 15, 2015).
- <sup>57</sup> See, e.g., *Bruno v. AT&T Mobility, LLC*, No. 10-404, 2011 U.S. Dist. LEXIS 59795, at \*5 n.4 (W.D. Pa. June 3, 2011) (“Plaintiff argues that the series of emails between Ms. Menster and Mr. Thomas have not been properly authenticated . . . . ‘A party to litigation that produces documents during discovery in that litigation thereby authenticates the documents it has produced.’”); *Dominion Nutrition, Inc.*, 2006 U.S. Dist. LEXIS 15515, at \*16 (“As to authentication, documents produced by an opponent may be treated as authentic.”); *Superhighway Consulting, Inc. v. Techwave, Inc.*, No. 98CV5502, 1999 U.S. Dist. LEXIS 17910, at \*6 (N.D. Ill. 1999) (“[O]ther courts in this district have held that the production of documents during discovery from the parties’ own files is sufficient to justify a finding of authentication.”); *Wells v. Xpedx*, No. 8:05-CV-2193-T-EAJ, 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*, No. 1:06-CV-0627-JOF, 2007 U.S. Dist. LEXIS 49248 (N.D. Ga. July 6, 2007) (“The e-mails in question were produced by Defendants during the discovery process. Such documents are deemed authentic when offered by a party opponent.”).
- <sup>58</sup> See, e.g., *United States v. Siddiqui*, 235 F.3d 1318, 1322 (11th Cir. 2000) (“[T]he e-mail sent to Yamada and von Gunten referred to the author as ‘Mo.’ Both Yamada and von Gunten recognized this as Siddiqui’s nickname.”); *United States v. Mebrtanu*, 543 F. App’x 137 (3d Cir. 2013) (emails sent to person with defendant’s first name, Promise, and referred to her boyfriend, Marcus); *Culp v. State*, No. CR-13-1039, 2014 Ala. Crim. App. LEXIS 102 (Ala. Crim. App. Nov. 21, 2014) (use of screen name and initials); *Donati v. State*, 84 A.3d 156, 172 (Md. Ct. Spec. App. 2014) (“[A]n e-mail reference to the author with the defendant’s nickname, where the context of the e-mail revealed details that only the defendant would know, and where the defendant called soon after the receipt of the e-mail, making the same requests that were made in the e-mail.”); *Interest of F.P.*, 878 A.2d 91, ¶13 (Pa. Super. Ct. 2005) (“He referred to himself by his first name.”); *Commonwealth v. Capece*, No. 65, 2010 Pa. Dist. & Cnty. Dec. LEXIS 506, 119 (Ct. Common Pl. Oct. 18, 2010) (“The e-mails were often signed ‘Jerry,’ a name to which Defendant answered.”); *Shea v. State*, 167 S.W.3d 98, 105 (Tex. Ct. App. 2005) (“Four of the e-mails were signed ‘Kev.’”).
- <sup>59</sup> See, e.g., *State v. Pullens*, 800 N.W.2d 202, 229 (Neb. 2011) (“There are several ways that the authorship of an e-mail may be shown . . . . The signature or name of the sender or recipient in the body of the e-mail is also relevant to authentication.”) (citing McCormick on Evidence § 227 (4th ed. 1992)); *Sea-Land Service, 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); cf. *In re 4Kids Entm’t, Inc.*, 463 B.R. 610, 693 (Bankr. S.D.N.Y. 2011) (“[T]he emails include signature blocks, which signify an intent to authenticate.”) (addressing effectiveness of modification of written agreement).
- <sup>60</sup> See, e.g., *People v. Sissac*, No. D064910, 2015 Cal. App. Unpub. LEXIS 1504 (Cal. Ct. App. Mar. 3, 2015) (purported sender possessed phone before and after texts were sent; a witness texted that phone number; the witness’s cell ties the number to the sender’s name; the sender acted consistently with earlier texts; the witness called number 6 hours after the texts the purported sender answered); *Butler v. State*, No. PD-0456-14, 2015 Tex. Crim. App. LEXIS 491 (Tex. Ct. Crim. App. Apr. 22, 2015) (cell number known by recipient to be sender’s from prior communications); *State v. Elseman*, 841 N.W.2d 225 (Neb. 2014); *Manuel v. State*, 357 S.W.3d 66 (Tex. Ct. App.), review denied, 2011 Tex. Crim. App. LEXIS 1711 (Tex. Ct. Crim. App. 2011); *State v. Thompson*, 777 N.W.2d 617 (N.D. Sup. Ct. 2010); *Campos v. State*, No. 01-13-00415-CR, 2015 Tex. App. LEXIS 230 (Tex. Ct. App. Jan. 13, 2015).
- <sup>61</sup> See, e.g., *Harsley v. State*, No. 29A02-1409-CR-661, 2015 Ind. App. Unpub. LEXIS 169 (Ind. Ct. App. Feb. 18, 2015) (testimony from recipient that she recognized the phone number as that of sender and that messages contained information only the two of them knew); *Culp v. State*, No. CR-13-1039, 2014 Ala. Crim. App. LEXIS 102 (Ala. Crim. App. Nov. 21, 2014) (use of euphemisms for drugs commonly used by sender and recipient in other emails); *Siddiqui*, 235 F.3d at 1322–23 (“The context of the e-mail . . . shows the author of the e-mail to have been someone who would have known the very details of Siddiqui’s conduct with respect to the Waterman Award and the NSF’s subsequent investigation. In addition, in one e-mail sent to von Gunten, the author makes apologies for cutting short his visit to EAWAG . . . . In his deposition, von Gunten testified that in 1994 Siddiqui had gone to Switzerland to begin a collaboration with EAWAG for three or four months, but had left after only three weeks to take a teaching job.”); *Hardin v. Belmont Textile Mach. Co.*, No. 3:05-CV-492-M, 2010 U.S. Dist. LEXIS 61121, at \*16 (W.D.N.C. June 7, 2010) (“The e-mails also discuss various identifiable matters related to [plaintiff’s] employment . . . which sufficiently authenticate the e-mails as being what its proponent claims.”); *United States v. Safavian*, 435 F.Supp.2d 36, 40 (D.D.C. 2006) (“The 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, such as Mr. Safavian’s work at the General Services Administration (‘GSA’), Mr. Abramoff’s work as a lobbyist, Mr. Abramoff’s restaurant, Signatures, and various other personal and professional matters.”); *State v. Taylor*, 632 S.E.2d 218, 231 (N.C. Ct. App. 2006) (quoting and following *Safavian*); *Pullens*, 800 N.W.2d at 229 (inclusion of sender’s social security and telephone numbers).
- <sup>62</sup> See, e.g., *Butler*, 2015 Tex. Crim. App. LEXIS 491; *Shea v. State*, 167 S.W.3d 98, 105 (Tex. Ct. App. 2005), *discretionary review denied*, 2005 Tex. Crim. App. LEXIS 1951 (Tex. Ct. Crim. App. Nov. 9, 2005); *Bloom v. Commonwealth of Virginia*, 34 Va. App. 364, 370, 542 S.E.2d 18, 20–21 (2001); *Dominion Nutrition, Inc. v. Cesca*, 2006 U.S. Dist. LEXIS 15515, at \*16 (N.D. Ill. Mar. 2, 2006); (“E-mail communications may be authenticated as being from the purported author based on . . . other communications from the purported author acknowledging the e-mail communication that is being authenticated.”) (quoting *Fenje v. Feld*, 301 F.Supp.2d, 781 (N.D. Ill. 2003)), *aff’d*, 398 F.3d 620 (7th Cir. 2005).
- <sup>63</sup> See, e.g., *Commonwealth v. Czubinski*, 26 N.E.3d 753 (Mass. App. Ct. 2015) (author leaves voicemail with substantially the same content); *Cook v. State*, No. 2015 Tex. App. LEXIS 2649 (Tex. Ct. App. Mar. 20, 2015) (recipient testified that she sent to, and received from, the defendant text messages to arrange a meeting and a drug buy; that she sent texts asking him when and where to meet; that she received responsive text messages stating his location; and that she met the defendant at that location); *Commonwealth v. Amaral*, 941 N.E.2d 1143, 1147 (Mass. App. Ct. 2011) (“The actions of the defendant himself served to authenticate the e-mails. One e-mail indicated that Jeremy would be at a certain place at a certain time and the defendant appeared at that place and time. In other e-mails, Jeremy provided his telephone number and photograph. When the trooper called that number, the defendant immediately answered his telephone, and the photograph was a picture of the defendant. These actions served to confirm that the author of the e-mails and the defendant were one and the same.”); *State v. Glass*, 190 P.3d 896, 901 (Idaho Ct. App. 2008) (same re online chat).

- <sup>64</sup> See, e.g., *Pavlovich v. State*, 6 N.E.3d 969 (Ind. Ct. App. 2014); *Butler*, 2015 Tex. Crim. App. LEXIS 491.
- <sup>65</sup> See, e.g., *People v. Harris*, No. A136727, 2014 Cal. App. Unpub. LEXIS 7086 (Cal. Ct. App. Oct. 1, 2014); *Harsley v. State*, No. 29A02-1409-CR-661, 2015 Ind. App. Unpub. LEXIS 169 (Ind. Ct. App. Feb. 18, 2015) (contents known only to sender and recipient).
- <sup>66</sup> See, e.g., *Butler*, 2015 Tex. Crim. App. LEXIS 491.
- <sup>67</sup> See, e.g., *People v. Pierre*, 41 A.D.3d 289, appeal denied, 874 N.E.2d 759 (2007).
- <sup>68</sup> See, e.g., *United States v. Benford*, No. CR-14-321-D, 2015 U.S. Dist. LEXIS 17046 (W.D. Okla. Feb. 12, 2015).
- <sup>69</sup> See, e.g., *State v. Burns*, No. M2014-00357-CCA-R3-CD, 2015 Tenn. Crim. App. LEXIS 325 (Tenn. Ct. App. May 5, 2015).
- <sup>70</sup> See, e.g., *Pavlovich* 6 N.E.3d at 969.
- <sup>71</sup> See, e.g., *Smith v. Smith*, No. 2140028, 2015 Ala. Civ. App. LEXIS 72 (Ala. Ct. Civ. App. Apr. 3, 2015).
- <sup>72</sup> See, e.g., *Bruno v. AT&T Mobility, LLC*, No. 10-404, 2011 U.S. Dist. LEXIS 59795, at \*5 n.4 (W.D. Pa. June 3, 2011) (“Plaintiff argues that the series of emails between Ms. Menster and Mr. Thomas have not been properly authenticated . . . ‘A party to litigation that produces documents during discovery in that litigation thereby authenticates the documents it has produced.’”); *Dominion Nutrition, Inc. v. Cesca*, No. 04C4902, 2006 U.S. Dist. LEXIS 15515, at \*16 (N.D. Ill. Mar. 2, 2006) (“As to authentication, documents produced by an opponent may be treated as authentic.”); *Superhighway Consulting, Inc. v. Techwave, Inc.*, No. 98CV5502, 1999 U.S. Dist. LEXIS 17910, at \*6 (N.D. Ill. 1999) (“[O]ther courts in this district have held that the production of documents during discovery from the parties’ own files is sufficient to justify a finding of authentication.”); *Wells v. Xpedx*, No. 8:05-CV-2193-T-EAJ, 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*, No. 1:06-CV-0627-JOF, 2007 U.S. Dist. LEXIS 49248 (N.D. Ga. July 6, 2007) (“The e-mails in question were produced by Defendants during the discovery process. Such documents are deemed authentic when offered by a party opponent.”).
- <sup>73</sup> *Campbell v. State*, 382 S.W.3d 545 (Tex. App. 2012).
- <sup>74</sup> *Smith v. State*, 136 So. 3d 424 (Miss. 2014); *Commonwealth v. Purdy*, 945 N.E.2d 372 (Mass. 2011); accord *State v. Eleck*, 130 Conn. App. 632, 637 n.4, 821 n.4 (2011), *aff’d on other grounds*, 314 Conn. 123, 100 A.3d 817 (2014).
- <sup>75</sup> *Campbell v. State*, 382 S.W.3d 545 (Tex. App. 2012).
- <sup>76</sup> *Bensusan Restaurant Corp. v. King*, 126 F.3d 25, 27 (2d Cir. 1997).

## 24th National College on Judicial Conduct and Ethics

October 28-30, 2015 – Chicago

### Sessions include:

Compare and Contrast: Judicial Discipline Systems

The 2007 Model Code of Judicial Conduct: Eight Years Later

The Constitutionality of Restrictions on Judges’ Political Conduct

Ex Parte Communications

“Do you know who I am?” The Prestige of Judicial Office

Problem-solving Courts and Judicial Ethics

Robe-itis: Causes and Cures

Determining the Appropriate Sanction



**NCSC**  
NATIONAL CENTER FOR STATE COURTS  
Center for Judicial Ethics

Sponsored by the Center for Judicial Ethics of the National Center for States Courts, the 24th National College on Judicial Conduct and Ethics will provide a forum for judges, judicial conduct commission members and staff, judicial ethics advisory committees, and others to discuss professional standards for judges and current issues in judicial discipline. For more information and registration, visit [www.ncsc.org/cje](http://www.ncsc.org/cje).