

2012


## Admissibility of Non-U.S. Electronic Evidence

Kenneth N. Rashbaum

Matthew F. Knouff

Dominique Murray

Follow this and additional works at: <http://scholarship.richmond.edu/jolt>

 Part of the [Computer Law Commons](#), [Evidence Commons](#), [International Law Commons](#), and the [Internet Law Commons](#)

---

### Recommended Citation

Kenneth N. Rashbaum, Matthew F. Knouff & Dominique Murray, *Admissibility of Non-U.S. Electronic Evidence*, 18 Rich. J.L. & Tech 9 (2012).

Available at: <http://scholarship.richmond.edu/jolt/vol18/iss3/3>

This Article is brought to you for free and open access by UR Scholarship Repository. It has been accepted for inclusion in Richmond Journal of Law and Technology by an authorized administrator of UR Scholarship Repository. For more information, please contact [scholarshiprepository@richmond.edu](mailto:scholarshiprepository@richmond.edu).

## ADMISSIBILITY OF NON-U.S. ELECTRONIC EVIDENCE

By Kenneth N. Rashbaum,<sup>\*</sup> Matthew F. Knouff,<sup>\*\*</sup> and  
Dominique Murray<sup>\*\*\*</sup>

Cite as: Kenneth N. Rashbaum, Matthew F. Knouff & Dominique Murray, *Admissibility of Non-U.S. Electronic Evidence*, XVIII RICH. J. L. & TECH. 9 (2012), <http://jolt.richmond.edu/v18i3/article9.pdf>

---

<sup>\*</sup> Kenneth N. Rashbaum is Principal of Rashbaum Associates, LLC in New York. His practice focuses upon counsel to multinational corporations on privacy, data protection and information governance across borders, litigation, and healthcare compliance. He is a frequent speaker and writer in the area of cross-border discovery and disclosure conflicts and international information governance. Mr. Rashbaum is an active member of The Sedona Conference, and a Vice-Chair of the International Litigation Committee of the American Bar Association. ([www.Rashbaumassociates.com](http://www.Rashbaumassociates.com)).

<sup>\*\*</sup> Matthew F. Knouff is General Counsel and eDiscovery Counsel with Complete Discovery Source, Inc., a global, full-service provider of electronic discovery services and technologies headquartered in New York City. Matthew advises law firms and corporations worldwide on eDiscovery and information governance best practices, cost & risk reduction strategies, and defensible deployment of technology during legal proceedings. He is Chairman of the New York County Lawyers' Association's Cyberspace Law Committee's eDiscovery Sub-Committee, an active member of The Sedona Conference and the New York State Bar Association, and is a frequent CLE instructor, writer, and speaker on issues related to eDiscovery, cross-border litigation, and information governance nationally.

<sup>\*\*\*</sup> Dominique Murray, Associate, Widowski Law Group LLP, New York, New York. J.D., 2005 Brooklyn Law School. Ms. Murray is a litigation attorney with particular experience in complex commercial matters, professional malpractice, product liability and toxic torts defense litigation, and transborder e-discovery.

## I. INTRODUCTION

[1] After two long years collecting hundreds of gigabytes of e-mail, data base reports, and social media posts from countries in Europe, Asia, and South America, such as France, South Korea, Argentina, Canada, Australia, and El Salvador, the day of trial has arrived. The trial team has obtained the data at great cost, in dollars as well as person-hours, but is finally ready for trial. First-chair counsel, second-chair counsel, and four paralegals file into the courtroom, not with bankers boxes full of documents as in earlier times, but with laptops, tablet computers, and a data projector. Following opening statements, the first witness takes the stand. After a few questions about the existence of e-mails written by executives of the defendant multinational corporation, a paralegal moves to the projector, as she rehearsed many times, to flip on the switch that will project the e-mails for the jury. She hears, “Objection!” followed immediately by, “Sustained.” Counsel asks for a sidebar. Instead, the judge asks the court officer to take the jury out. She then notes that these e-mails, the production of which she had ruled upon previously, were created outside the U.S. Who will testify to their authenticity? What was the chain of custody—were they altered in some fashion in the office or between the client’s servers and counsel’s laptop? How, exactly, do the e-mails fit into an exception to the hearsay rule? Business records? What is the “business” of this foreign facility that requires the use of e-mail on a regular basis? Counsel asks for a continuance to respond to those questions. “Denied!” the judge says.

[2] The above cautionary tale describes the next logical step to the cross-border discovery wars that have raged on over the last several years.<sup>1</sup> Studies have shown that over ninety percent of all business

---

<sup>1</sup> See generally SEDONA CONFERENCE, WORKING GRP. SIX, FRAMEWORK FOR ANALYSIS OF CROSS-BORDER DISCOVERY CONFLICTS: A PRACTICAL GUIDE TO NAVIGATING THE COMPETING CURRENTS OF INTERNATIONAL DATA PRIVACY AND DISCOVERY 14-16 (2008) [hereinafter SEDONA FRAMEWORK], available at [http://www.thesedonaconference.org/dltForm?did=WG6\\_Cross\\_Border](http://www.thesedonaconference.org/dltForm?did=WG6_Cross_Border).

correspondence exists in digital form.<sup>2</sup> The pace of global commerce is accelerating, and thus, increasing amounts of documentary evidence needed for U.S. litigation, arbitration, and regulatory proceedings comes from outside the United States.<sup>3</sup> While the law continues to evolve with regard to discovery and disclosure of protected data across borders, it is in a state of relative infancy with regard to admissibility of that information. Furthermore, it would be a disappointing and expensive endeavor indeed if hundreds of thousands of dollars in legal fees were spent to gather and produce discoverable discovery of electronic evidence that is ultimately excluded at trial.<sup>4</sup>

[3] This article will discuss the parameters for the admissibility of electronic information from outside the U.S. in the context of trials as well as motions that require the support of proof in admissible form. It will provide guidance to the practitioner and the court on the admissibility of various types of electronically stored information (“ESI”) that have been created, or are maintained, outside the borders of the United States. Section II will comprise a review of the rules for admission of evidence in U.S. Courts and their application to electronic evidence obtained abroad at various stages of the litigation lifecycle. Section III will discuss challenges to the use of non-U.S. ESI arising from conduct during pretrial

---

<sup>2</sup> See MARY MADDEN & SYDNEY JONES, PEW INTERNET & AMERICAN LIFE PROJECT, NETWORKED WORKERS at ii (2008), available at [http://www.pewinternet.org/~media/Files/Reports/2008/PIP\\_Networked\\_Workers\\_FINAL.pdf](http://www.pewinternet.org/~media/Files/Reports/2008/PIP_Networked_Workers_FINAL.pdf); Maria Perez Crist, *Preserving the Duty to Preserve: The Increasing Vulnerability of Electronic Information*, 58 S.C. L. REV. 7, 8-9 (2006).

<sup>3</sup> See Marissa L. P. Caylor, *Modernizing the Hague Evidence Convention: A Proposed Solution to Cross-Border Discovery Conflicts During Civil and Commercial Litigation*, 28 B.U. INT'L L.J. 341, 342 (2010); Okezie Chukwumerije, *International Judicial Assistance: Revitalizing Section 1782*, 37 GEO. WASH. INT'L L. REV. 649, 650 (2005).

<sup>4</sup> See *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 537-38 (D. Md. 2007). See generally Paul W. Grimm et al. *Back to the Future: Lorraine v. Markel American Insurance Co. and New Findings on the Admissibility of Electronically Stored Information*, 42 AKRON L. REV. 357, 358-61 (2009).

discovery. Section IV will analyze the admissibility of non-U.S. ESI in motion practice. Section V will address authentication of specific categories of ESI encountered in cross-border matters such as e-mails, instant messages and chat logs, social media sites, Internet tracking information, and printouts of the same.

## II. FOUNDATION FOR ADMISSIBILITY OF ELECTRONICALLY STORED INFORMATION

[4] The rules of evidence apply equally to evidence offered in electronic format and on paper.<sup>5</sup> If anything, the rules may apply greater scrutiny to ESI because of concerns about the reliability of electronic evidence. As Chief Magistrate Judge Paul W. Grimm wrote in *Lorraine v. Markel Insurance Co.*, “Computerized data . . . raise[s] unique issues concerning [its] accuracy and authenticity.”<sup>6</sup> Judge Grimm is not alone in his cautious approach to electronic evidence. In *New York v. Microsoft Corp.*, the court posited a fundamental evidentiary inquiry about e-mail, namely, how can one establish that e-mail is what it purports to be.<sup>7</sup> Similarly, Judge Grimm noted in *Lorraine* that whether the offered ESI is a chart entry, business record, or other form of proof, counsel must establish origins and chain of custody.<sup>8</sup>

---

<sup>5</sup> See *Lorraine*, 241 F.R.D. at 538; Jonathan D. Frieden & Leigh M. Murray, *The Admissibility of Electronic Evidence Under the Federal Rules of Evidence*, 17 RICH. J.L. & TECH. 5, ¶ 2 (2010).

<sup>6</sup> *Lorraine*, 241 F.R.D. at 557 n.34.

<sup>7</sup> See *New York v. Microsoft Corp.*, No. CIV A. 98-1233 (CKK), 2002 WL 649951, at \*1 (D.D.C. Apr. 12, 2002). See generally FED. R. EVID. 901 (identifying methods of authentication).

<sup>8</sup> *Lorraine*, 241 F.R.D. 534 at 548. Maintenance of an unbroken chain of custody cannot be stressed enough as a best-practice, although a kink in the chain of custody does not necessarily prevent the admissibility of a piece of evidence. See *United States v. Campbell*, No. 94-30295, 1996 WL 241545, at \*5-6 (9th Cir. May 9, 1996). An audio recording was admitted into evidence based on testimonial evidence regarding characteristics of the defendant’s voice, the content of the recording, and evidence that

[5] These rules for evidence have long existed in the world of paper; however, since paper evidence is commonplace, it often does not require a searching inquiry.<sup>9</sup> Courts assess electronic evidence with greater caution due in part to the fact that courts have far less experience with electronic evidence than with paper.<sup>10</sup> Some judges are unfamiliar with technology, and counsel before them may not have assiduously educated the court on the integrity of the proffered evidence.<sup>11</sup> Non-U.S. evidence presents additional levels of complication. In the country of data creation, what security safeguards exist that can provide indicia of authenticity and reliability? Do the indicia require live testimony or declarations, or are there technological markers and distinctive characteristics that can indicate trustworthiness and reliability? If the data is offered through the business record exception to the hearsay rule, how does one prove the required regularity of business record-keeping practices in, for example, China, where such practices vary sharply from the U.S.? Are there conflicts of law issues regarding privacy and security of data that impact

---

tape was not altered, despite a break in chain-of-custody when a recording was made of the tape. *Id.* The Court went on to say that “[A] defect in the chain of custody goes to the weight, not the admissibility, of the evidence introduced.” *Id.* (citing *United States v. Matta-Ballesteros*, 71 F.3d 754, 768-69 (9th Cir. 1995)). Proof of an unbroken chain of custody, especially with evidence travelling from outside the U.S., will help bolster authenticity and address any claims that foreign ESI has been compromised during its journey to the courtroom. *See* PAUL R. RICE, *ELECTRONIC EVIDENCE LAW AND PRACTICE* 258-59 (2005).

<sup>9</sup> *See* *Rowe Entm't, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 429 (S.D.N.Y. 2002).

<sup>10</sup> *See* *Lorraine*, 241 F.R.D. at 537; SEDONA CONFERENCE, *WORKING GRP. ONE, COMMENTARY ON ESI EVIDENCE & ADMISSIBILITY* 2 (2008). However, “when more judges will have been raised on computers, the suspicion in several judicial quarters surrounding the creation and potential alteration of ESI may diminish, and the requirements for admissibility may be less demanding.” Sheldon M. Finkelstein & Evelyn R. Storch, *Admissibility of Electronically Stored Information: It's Still the Same Old Story*, 23 J. AM. ACAD. MATRIMONIAL LAW. 45, 46 (2010).

<sup>11</sup> *See* Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1, 63 (2009).

discoverability? If so, is the party that has asserted those laws as an objection to discoverability then precluded from offering similar evidence at trial? Finally, what are the standards for proof of the foreign laws and even for resolution of conflicts over language translation?

[6] The rules that govern the admission of documentary evidence require the satisfaction of six criteria: Relevance; Authenticity; Reliability; Non-Hearsay (or coverage under a hearsay exception); Best Evidence/Original Evidence Rule; and Probative Value vs. Prejudicial Effect.<sup>12</sup> These criteria are frequently interrelated; establishment of one requirement may satisfy one or more of the others.<sup>13</sup> In addition, a method exists by which the court may admit foreign ESI through the expediency of the Self-Authenticating Document Rules, which relieve the proponent of the need to obtain extrinsic evidence such as live testimony, declarations, or certifications.<sup>14</sup> Federal Rule of Evidence (“F.R.E.”) 401 admits only that ESI which has a tendency to make some consequential fact to the litigation more or less probable than it would otherwise be.<sup>15</sup> Irrelevant evidence is inadmissible.<sup>16</sup>

---

<sup>12</sup> See *Lorraine*, 241 F.R.D. at 538.

<sup>13</sup> See *United States v. Sliker*, 751 F.2d 477, 499 (2d Cir. 1984); *Lorraine*, 241 F.R.D. at 539; Jonathan L. Moore, *Time for an Upgrade: Amending the Federal Rules of Evidence to Address the Challenges of Electronically Stored Information in Civil Litigation*, 50 JURIMETRICS J. 147, 156 (2010) (suggesting that authenticity is often a subset of relevance: “if evidence is not authentic, it has no relevance to the case”).

<sup>14</sup> See *Lorraine*, 241 F.R.D. at 551; Grimm et. al., *supra* note 4, at 384; Randy Wilson, *Admissibility of Web-Based Data*, 52 THE ADVOC. (TEX.) 31, 31-32 (2010).

<sup>15</sup> FED. R. EVID. 401 (“Evidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence. . . .”).

<sup>16</sup> FED. R. EVID. 402 (“Irrelevant evidence is not admissible.”).

### A. Authenticity

[7] If evidence meets the threshold standard for relevance, it must be shown to be authentic.<sup>17</sup> Authenticity, put simply, requires proof that the item is, in fact, what it purports to be.<sup>18</sup> The court will ask if the item of information is what counsel says it is. For example, for a company e-mail, text message, database report, website, or social media posting from the source the proponent claims, most often the author, an entity can demonstrate the item's authenticity. Evaluating the requirements needed to satisfy the authenticity hurdle is more complex in the world of electronic evidence. The Ninth Circuit held in *In re Vinhee* that “[t]he paperless electronic record involves a difference in the format of the record that presents more complicated variations on the authentication problem than for paper records.”<sup>19</sup> Yet, the court noted, “(u)ltimately. . . it all boils down to the same question of assurance that the record is what it purports to be.”<sup>20</sup> The complexity is found in the provision of such “assurance.” In *In re Vee Vinhnee*, American Express sought to introduce certain electronic account records, but failed to detail the protocols for the computer systems holding those records and the basis of American Express’ assertions that it had preserved the integrity of the data.<sup>21</sup> In sustaining the trial court’s decision, the Circuit court upbraided counsel for assumptions that led to perceived shortcomings in its offer of proof, and, in so doing, provided guidance on laying a proper foundation for ESI:

---

<sup>17</sup> FED. R. EVID. 901(a) requires that evidence be authenticated. This may be accomplished in myriad ways. *See* FED. R. EVID. 901(b).

<sup>18</sup> *See generally* FED. R. EVID. 901(a).

<sup>19</sup> *Am. Express Travel Related Servs. Co. v. Vinhnee (In re Vee Vinhnee)*, 336 B.R. 437, 445 (B.A.P. 9th Cir. 2005).

<sup>20</sup> *Id.*

<sup>21</sup> *See id.* at 442.



The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the question of whether records have been changed since their creation. There is little mystery to this. All of these questions are recognizable as analogous to similar questions that may be asked regarding paper files: policy and procedure for access and for making corrections, as well as the risk of tampering. But the increasing complexity of ever-developing computer technology necessitates more precise focus.<sup>22</sup>

[8] As shown by the *In re Vee Vinhnee* opinion, courts unfamiliar with technology, and even those more sophisticated in the area, may require offers of proof, documents, and hearings to establish that the information being offered as authentic is what counsel says it is.<sup>23</sup> Counsel must ascertain whose policies and procedures govern the creation of the information and determine how to get that person or entity before the court. Courts have been increasingly vigilant about the foundation for ESI, “demanding that proponents of evidence obtained from electronically stored information pay more attention to the foundational requirements than has been customary for introducing evidence not produced from

---

<sup>22</sup> *Id.* at 445.

<sup>23</sup> See generally Cooper Offenbecher, *Admitting Computer Record Evidence after In Re Vinhnee: A Stricter Standard for the Future?*, 4 SHIDLER J. L. COM. & TECH. 6 (2007) (examining the numerous foundation standards that courts have applied to the authentication of electronic records).

electronic sources.”<sup>24</sup> Foundational requirements are particularly important for ESI produced from systems and applications in countries whose information governance protocols may be unfamiliar to U.S. judges, and “[t]he required foundation will vary not only with the particular circumstances but also with the individual judge.”<sup>25</sup> However, it is instructive, as Magistrate Judge Grimm observed in *Lorraine*, that “the inability to get evidence admitted because of a failure to authenticate it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation.”<sup>26</sup>

[9] Authenticity and its corollary reliability may be established by an entity’s information management protocols, the policies, procedures and practices that govern the creation, storage, and transmission of non-U.S. ESI. Moreover, these same protocols will be used by courts in establishing whether ESI satisfies the business records exception to hearsay.<sup>27</sup> Often courts use the same analysis to determine whether electronic information qualifies for the business records exception to the hearsay rule.<sup>28</sup> In other words, the practices of the company in the creation and maintenance of its business information may indicate to a court that the information has the necessary safeguards for the finder of fact to rely upon it.<sup>29</sup> But what if the loci of creation, storage, and transmission are outside the U.S.?

---

<sup>24</sup> *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 543 (D. Md. 2007).

<sup>25</sup> *See id.* at 544.

<sup>26</sup> *Id.* at 542.

<sup>27</sup> *See* FED. R. EVID. 902(11); Frieden & Murray, *supra* note 5, ¶¶ 33-35

<sup>28</sup> *See* FED. R. EVID. 803(6); Frieden & Murray, *supra* note 5, ¶33 (“This method mirrors the requirements of the business records exception to the hearsay rule; therefore, courts often analyze it in conjunction with that exception.”).

<sup>29</sup> *See* *Am. Express Travel Related Servs. Co. v. Vinhnee (In re Vee Vinhnee)*, 336 B.R. 437, 445 (B.A.P. 9th Cir. 2005).

[10] What if the information crosses several countries? It is not uncommon for employees of multinational corporations to create business documents from laptops, tablets, and smartphones while travelling among multiple countries.<sup>30</sup> A company network housed with a cloud provider may store this information on servers in still more countries and back it up at corporate headquarters in yet another on-site repository.<sup>31</sup> A U.S. court, in exploring the basis for admission of that information, may well ask for proof of routinized practices governing the “life” of that information to be assured of its integrity, and to satisfy the criteria for the business records exception to the hearsay rule.<sup>32</sup>

[11] Frequently, information governance protocols for organizations located outside the U.S. use a language other than English and are drafted

---

<sup>30</sup> See SEDONA CONFERENCE, WORKING GRP. SIX, INTERNATIONAL PRINCIPLES ON DISCOVERY, DISCLOSURE & DATA PROTECTION: BEST PRACTICES, RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING THE PRESERVATION & DISCOVERY OF PROTECTED DATA IN U.S. LITIGATION at v (E.U. ed. Dec. 2011), available at <http://www.thesedonaconference.org/dltForm?did=IntlPrinciples2011.pdf> (“This unprecedented explosion in information owes in large part to ubiquitous, mobile, and easily-replicable nature of ESI. Today, an employee from a Toronto company can conduct business from a cafe [sic] in Paris, while sending electronic messages to customers in Dubai that attach documents from “cloud” servers located in Singapore, Dallas, and Amsterdam.”).

<sup>31</sup> See Alberto G. Araiza, *Electronic Discovery in the Cloud*, 2011 DUKE L. & TECH. REV. 8, ¶7 (“Cloud providers essentially virtualize the same physical resources (such as processors and storage arrays) to service multiple dispersed clients. Cloud providers also divide ‘the tasks of running applications and storing data into small chunks,’ and then allocate the chunks among various distributed resources.” (citation omitted)).

<sup>32</sup> See *In re Vee Vinhnee*, 336 B.R. at 445 (“The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity’s policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the question of whether records have been changed since their creation.”).

and enforced pursuant to the laws of the foreign country in question.<sup>33</sup> While foreign laws governing the security of certain protected data may help establish reliability, parties may dispute the scope and applicability of those laws. Preparation, though, can ease the pain, especially with regard to authentication of non-U.S. ESI.<sup>34</sup>

[12] The evidentiary solution for the admission of foreign ESI may sound daunting, but as the singer Paul Simon wrote, “The answer is easy if you take it logically . . . .”<sup>35</sup> Counsel can achieve that logical solution by taking a step-by-step approach through each of the six foundational requirements and documenting the support for each element. Such support can take the form of pegging the various foundational requirements to support answers found in the entity’s information management procedures and laws of the countries involved in the information creation, maintenance, and transmission. The journey has a few shortcuts. Just as procedures for information governance intertwine security and privacy, the evidentiary components do not reside in silos.<sup>36</sup> Satisfaction of one rule may provide the answer to questions posed by another.

## B. Reliability

[13] After authenticity, the next hurdle to clear for a proponent of foreign ESI is reliability. Reliability exists as an often overlooked, but

---

<sup>33</sup> See *infra* note 63 and accompanying text.

<sup>34</sup> See *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 542 (D. Md. 2007).

<sup>35</sup> PAUL SIMON, *50 Ways to Leave Your Lover*, STILL CRAZY AFTER ALL THESE YEARS (Columbia Records 1975).

<sup>36</sup> See, e.g., Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 (2006) (requiring financial institutions to follow procedures to safeguard the privacy of customer information); *DirecTV, Inc. v. Murray*, 307 F. Supp. 2d 764, 772 (D.S.C. 2004) (analyzing the admissibility of e-mails under Rules 902(11) and 803(6), and explaining that the analyses of authentication and hearsay are intertwined).

critical, subset of authenticity.<sup>37</sup> The *Manual for Complex Litigation* instructs that courts should “consider the accuracy and reliability of computerized evidence” and the “proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy.”<sup>38</sup>

[14] In the United States, reliability can be shown by reference to procedures for transferring ESI, such as documentation showing the policies and security controls for maintaining the integrity of information in storage and in motion—i.e., logged in and out at the recipient’s repository—to establish a chain of custody.<sup>39</sup> Metadata and unique characteristics inherent in a piece of electronic information (i.e. a hash value) may demonstrate that parties have not altered data.<sup>40</sup> Statutory or regulatory compliance may also indicate reliability.<sup>41</sup> Showing that these provisions were followed can help meet the requirement of proof that the proffered evidence remains unaltered and, thus, is reliable (although, of course, this showing is more easily made with documented policies and procedures for sending, receiving, and storing the information in a secure

---

<sup>37</sup> See *Connecticut v. Swinton*, 847 A.2d 921, 942-43 (Conn. 2004) (“In addition to the reliability of the evidence itself, what must be established is the reliability of the procedures involved . . .”).

<sup>38</sup> MANUAL FOR COMPLEX LITIGATION (FOURTH) § 11.446 (2004).

<sup>39</sup> See generally Christy Burke, *Examining E-Discovery Chain of Custody*, LAW.COM (Oct. 23, 2007), <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=900005494089> (explaining the importance of logging the chain of custody of ESI).

<sup>40</sup> See *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 546-48 (D. Md. 2007) (explaining that the use of hash values and the examination of metadata can be used as methods of authenticating electronic evidence).

<sup>41</sup> See, e.g., Steve Apiki, *Sarbanes-Oxley: Driving the Storage Compliance Boom*, ENTERPRISESTORAGEFORUM.COM (Feb. 25, 2005), <http://www.enterprisestorageforum.com/continuity/features/article.php/3485651> (explaining that the Sarbanes-Oxley Act requires that data integrity be maintained over a retention period, which can serve to help in the authentication of stored documents by ensuring they are original).

fashion).<sup>42</sup>

[15] Similarly, data protection statutes, which mandate safeguards for data sent beyond a country's borders, can assist counsel in establishing data integrity.<sup>43</sup> For example, regulations drafted under Israel's Protection of Privacy Act pertaining to personal data in databases protect that information by requiring that the recipient of the database information safeguard it as though it were located in Israel.<sup>44</sup> Israel's Protection of Privacy Act comprises very specific requirements to control entry of data, access to data, and transfers of data from those databases.<sup>45</sup> Argentina's Personal Data Protection Act and regulations promulgated thereunder also provide stringent provisions for the security of personal data in databases and prohibit the transfer of such information unless the recipient can provide similar safeguards.<sup>46</sup> Thus, a showing by the proponent of such evidence of regulatory and statutory requirements preserving the integrity of the data, along with testimony or a certification that the regulations and statutes as pertinent were followed, can satisfy the foundational burden of reliability.<sup>47</sup> The proponents and opponents of such evidence, then, should

---

<sup>42</sup> See *Lorraine*, 241 F.R.D. at 545 ("It is necessary, however, that the authenticating witness 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 . . .").

<sup>43</sup> E.g. Privacy Protection (Transfer of Databases Abroad) Regulations, 2001, KT 5761, 1-2 (Isr.).

<sup>44</sup> *Id.*

<sup>45</sup> Protection of Privacy Law 5741-1981, SH No. 196 p. Chapter 2, Article 1 (Isr.) (such as forbidding possession of a database without registration, and even forbidding use of a database "except for the purposes for which the data base was set up.").

<sup>46</sup> Law No. 25326, Oct. 4, 2000, A.D.L.A. 5426 (Arg.); Decree No. 1558, Dec. 3, 2001, XXIX A.D.L.A. 1558 (Arg.).

<sup>47</sup> See *Lorraine*, 241 F.R.D. at 545; MANUAL FOR COMPLEX LITIGATION (FOURTH) § 11.446 (2004).

familiarize themselves with the applicable non-U.S. data protection provisions.

### C. Hearsay

[16] The criterion that evidence is not hearsay, or falls within an exception to the hearsay rule, requires the court first to determine whether the computerized information in question is indeed hearsay. Hearsay is: (1) an assertive statement; (2) made by a human declarant; (3) offered for the truth of the matter asserted; and (4) not excluded from the definition of hearsay because it is: (a) an opposing party's statement as understood by F.R.E. 801(d)(2); or (b) a prior testimonial statement covered by F.R.E. 801(d)(1).<sup>48</sup> If ESI constitutes hearsay, it is inadmissible unless it falls within one of the recognized exceptions to hearsay statements.<sup>49</sup>

[17] Insofar as ESI is offered to prove the truth of the matter asserted, all ESI is hearsay, provided the data offered is a statement of a declarant and not machine-generated, such as a computerized readout.<sup>50</sup> The exception to the hearsay rule most commonly applicable to ESI is the business records exception.<sup>51</sup> How does one establish the requisite showing of routinized information creation, storage, and maintenance procedures for locations outside the U.S. and what is the level of proof required to get that information before a finder of fact? The initiative breaks down into two categories: (1) enterprise protocols; and (2) laws

---

<sup>48</sup> FED. R. EVID. 801(c) (defining hearsay generally as "a statement that: (1) the declarant does not make while testifying at the current trial or hearing, and (2) a party offers in evidence to prove the truth of the matter asserted in the statement").

<sup>49</sup> See FED. R. EVID. 802.

<sup>50</sup> See Charles Albert Ross, *Evidentiary Issues Regarding Electronically Stored Information*, AVVO (Feb. 10, 2012, 12:01 PM), <http://www.avvo.com/legal-guides/ugc/evidentiary-issues-regarding-electronically-stored-information>.

<sup>51</sup> *Id.*

that may assist in the establishment of the requisite showing. On this latter point, one must also ascertain how to prove the existence of the foreign laws and regulations.

[18] Perhaps the most obvious challenge to foreign ESI falling under the business records exception is an allegation that the information was not created or managed pursuant to reliable business practices. The defense, accordingly, would need to show that the documents were created and managed by sound processes.<sup>52</sup> How does one establish the existence of reliable practices? One of the many struggles that multi-national practitioners face is that courts have inconsistently applied the rules of evidence in this area.<sup>53</sup> This is perhaps due to a lack of effort by counsel to educate the court on the technology at issue and the indicia of reliability of the information (or, in the cases in which courts have admitted the evidence without much analysis, lack thereof). The responsibility, Judge Grimm has noted, is with counsel, in that “they must be the ones to identify reliability/trustworthiness problems with digital business records, develop the facts to challenge them, and argue to the courts why the exception is inapplicable and why the proffered evidence should be excluded.”<sup>54</sup> Of course, the inverse is equally true, significantly so in the case of non-U.S. ESI: the proponent of the evidence must be sufficiently versed in the non-U.S. information management protocols that support the admission of this evidence.<sup>55</sup> Counsel must show that the information offered meets the oft-intertwined criteria of reliability and the business records exception to the hearsay rule.

[19] There exists considerable overlap between the requirements of authenticity and those pertaining to establishment of the ESI as a business

---

<sup>52</sup> See Grimm et al., *supra* note 4, at 376.

<sup>53</sup> See *id.* at 407-09.

<sup>54</sup> See *id.* at 409.

<sup>55</sup> See *infra* Part I.G (discussing non-U.S. management protocols).



record. In *In re Vee Vinhnee*, the court noted that satisfaction of the authenticity requirement calls for, among other things, proof (itself in admissible form) of internal protocols. “[P]olicies and procedures for the use of the equipment, database, and programs are important. How access to the [information] is controlled and, separately, how access to the specific program is controlled are important questions . . . [as well as] audit procedures for *assuring the continuing integrity of the [information]* . . . .”<sup>56</sup> In a similar manner, establishment of evidence as a business record requires a degree of trustworthiness of the electronic information *as* a business record, and that trustworthiness must be proven by business protocols, such as:

evidence to make a clear showing that the digital evidence relates to a regular activity of the business itself, as opposed to the personal use of its creator, and that the business imposed on the employee a requirement to make a digital record of the occurrence, and thereafter to maintain that record for purposes of the future use by the company.<sup>57</sup>

In other words, as the court in *In re Vee Vinhnee* noted, “the authenticity analysis is merged into the business record analysis. . . .”<sup>58</sup>

[20] Cross-border distinctions in business practices can trap the unwary practitioner and perhaps even the court. A question may arise as to cultural distinctions in business practices, in that the information management practices of non-U.S. entities may differ from those typically seen in the U.S.<sup>59</sup> If practices differ, will they meet the level of scrutiny

---

<sup>56</sup> *Am. Express Travel Related Servs. Co. v. Vinhnee (In re Vee Vinhnee)*, 336 B.R. 437, 445 (B.A.P. 9th Cir. 2005) (emphasis added).

<sup>57</sup> Grimm et al., *supra* note 4, at 405.

<sup>58</sup> *See In re Vee Vinhnee*, 336 B.R. at 444.

<sup>59</sup> David O. Stephens, *Putting on a Global Face*, DOCUMENTMEDIA.COM, <http://documentmedia.com/ME2/dirmod.asp?sid=&nm=Content+Library&type=Publishi>

required for a foundation for ESI? If the entity permits its employees to use company computers to send and receive personal communications, does this dilute the business practice with regard to company e-mails and, if so, to what extent? Does the analysis change in light of the fact that permission for occasional personal use of company networks is standard in many U.S. industries (discussed further, *infra*, in Section V)?<sup>60</sup> Opponents of ESI may find it difficult to challenge the practice on the basis that personal use is permitted because, in the case of evidence emanating from an E.U. Member State, local legislation often proscribes the monitoring of employee network use that could reveal extensive personal communications.<sup>61</sup>

[21] Foreign ESI comprising public records may be admissible under the F.R.E. 803(8) hearsay exception for public records and reports.<sup>62</sup> Non-U.S. public records may also be admitted, if meeting all other evidentiary

---

ng&mod=Publications%3A%3AArticle&mid=8F3A7027421841978F18BE895F87F791&tier=4&id=EFF25A90A11C4461B855E0037F5814AE (last visited Feb. 14, 2012).

<sup>60</sup> See Grimm et al., *supra* note 4, at 405 (noting that courts that appreciate this subtlety “are more likely to be inclined to require strict adherence to each element of Rule 803(6)”).

<sup>61</sup> See, e.g., Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Jan. 14, 2003, BUNDESGESETZBLATT, Teil I [BGBL. I] [Federal Law Gazette I] at 66, § 20, as amended, Aug. 14, 2009, BGBL. I at 2814 (Ger.), available at [http://www.bfdi.bund.de/cae/servlet/contentblob/1086936/publicationFile/87545/BDSG\\_idFv01092009.pdf](http://www.bfdi.bund.de/cae/servlet/contentblob/1086936/publicationFile/87545/BDSG_idFv01092009.pdf); Personal Data Protection Code, Decreto Legge 30 giugno 2003, n. 196, Title X, Ch. 1, Sec. 121-23 (It.), available at <http://www.garanteprivacy.it/garante/document?ID=1219452>; [Act on the Protection of Personal Information], Law No. 57 of 2003, art. 27 (Japan), available at <http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf>.

<sup>62</sup> FED. R. EVID. 803(8); see also *Mike’s Train House, Inc. v. Lionel, LLC*, 472 F.3d 398, 412 (6th Cir. 2007) (admitting Korean arrest notices, complaint and investigative reports under FED. R. EVID. 803(8)); *infra* note 114 and accompanying text.

criteria, under the residual hearsay exception of F.R.E. 807.<sup>63</sup> This “catch-all” section provides that a statement that does not fit within the other enumerated exceptions but comprises “circumstantial guarantees of trustworthiness” may be admitted if offered under the following circumstances, “as evidence of a material fact; . . . is more probative on the point for which it is offered than any other evidence that the proponent can obtain through reasonable efforts; and . . . admitting it will best serve the purposes of these rules and the interest of justice.”<sup>64</sup> The proponent must provide advance notice to his or her adversary of the intent to utilize this exception, including the declarant’s name and address.<sup>65</sup> F.R.E. 807 has even been the basis for admission of negative evidence, such as proof that certain information was *not* contained in the records of a foreign government.<sup>66</sup>

#### **D. Preservation and Regularity of Foreign Business Information Generation**

[22] Questions of preservation of foreign ESI may enter into the analysis as well. F.R.E. 803 requires that the information be “*kept* in the course of a regularly conducted activity of a business.”<sup>67</sup> Judge Grimm observed that “it may be difficult to show that the e-mails are ‘kept’ for a ‘business activity’ if they are routinely and automatically deleted without

---

<sup>63</sup> FED. R. EVID. 807 (explaining certain circumstances in which hearsay statements are not excluded, even when not covered by a hearsay exception in FED. R. EVID. 803 or 804).

<sup>64</sup> *Id.*

<sup>65</sup> *Id.*; *see also* United States v. Loalza-Vasquez, 735 F.2d 153, 157 (5th Cir. 1984) (involving an arrangement between U.S. and Panama, which was established through series of teletype messages received by captain of U.S. Coast Guard ship).

<sup>66</sup> *See, e.g.*, United States v. Cahill, No. 85 CR 773, 1988 U.S. Dist. LEXIS 6350, at \*8-9 (N.D. Ill. June 28, 1988).

<sup>67</sup> FED. R. EVID. 803(6) (emphasis added).

being saved to a file where they will continue to be available for business purposes.”<sup>68</sup>

[23] Of course, “keeping,” or “preserving” the information for business purposes may not seem to be an obvious issue, i.e. if counsel have the information available for proffer at trial, they clearly have “kept,” or “preserved” it in some respect.<sup>69</sup> The issue will arise when adversary counsel attempt to challenge the offer of evidence by showing that there is no *established protocol* for such preservation. Counsel can, perhaps, counter this argument with proof that preservation policies outside the U.S. often differ from those of American companies and that local laws and regional directives may be further restrictive.<sup>70</sup> Therefore, showing a lack of an American-style preservation policy may not, without more, sustain an objection to the evidence.

[24] To further complicate matters, preservation in the U.S. sense may, in many parts of the world, actually violate local law. Within the European Union, “personal data” —data that can be traced to an identifiable person—is protected under Privacy Directive 95/46/EC.<sup>71</sup> All E.U. member states have implemented this Directive by local law, as required by the terms of the Directive.<sup>72</sup> Because it is possible to trace e-mail, perhaps the most sought-after form of electronic evidence, to a

---

<sup>68</sup> Grimm et al., *supra* note 4, at 406.

<sup>69</sup> See FED. R. EVID. 803(6).

<sup>70</sup> The conundrum is similar to that for the admissibility standard. See *supra* notes 60-61 and accompanying text; *infra* Section V.

<sup>71</sup> See generally Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, 1995 O.J. (L 281) 31 (EC) [hereinafter Directive] (protecting individuals with regard to the processing of personal data and on the free movement of such data).

<sup>72</sup> Directive, *supra* note 71.

named sender and/or recipient, it thus constitutes “personal data.”<sup>73</sup> The Directive only allows the “processing” of personal data for limited purposes.<sup>74</sup> The Directive defines “processing” broadly, as “*any . . . set of operations . . . [including but not limited to] collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.*”<sup>75</sup> The European Commission Article 29 Working Party on Data Protection has opined that preservation constitutes a form of processing.<sup>76</sup>

[25] Certain countries, including Germany, France, Korea, Japan, and Italy, mandate the deletion of protected data after accomplishing the purpose for which the data was collected.<sup>77</sup> In other jurisdictions, business

---

<sup>73</sup> See EUROPEAN COMMISSION, ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 4/2007 ON THE CONCEPT OF PERSONAL DATA (2007), *available at* [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf).

<sup>74</sup> See Directive, *supra* note 71 (defining “processing” and saying that member states should protect fundamental rights and freedoms, in particular the right to privacy with respect to processing personal data).

<sup>75</sup> *Id.* (emphasis added) (stating that while the United States does not consider certain kinds of personal data storage as processing, Directive 95/46 considers any “retention, preservation, or archiving of data for such purposes” as processing).

<sup>76</sup> European Commission, Data Protection Working Party, *Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation*, at 8 (European Comm’n Working Paper No. 158, 2009) [hereinafter *EU Working Document*], *available at* [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf).

<sup>77</sup> See Loi 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés, [Act No. 78-17 of 6 Jan. 1978 on Information Technology, Data Files, and Civil Liberties], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Jan. 7, 1978, p. 227; Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Jan. 14, 2003, BUNDESGESETZBLATT, Teil I [BGBl. I] [Federal Law Gazette I] at 66, § 20, as amended, Aug. 14, 2009, BGBl. I at 2814 (Ger.), *available at* [http://www.bfdi.bund.de/cae/servlet/contentblob/1086936/publicationFile/87545/BDSG\\_idFv01092009.pdf](http://www.bfdi.bund.de/cae/servlet/contentblob/1086936/publicationFile/87545/BDSG_idFv01092009.pdf); Personal Data Protection Code, Decreto Legge 30 giugno 2003, n. 196 (It.), *available at* <http://www.garanteprivacy.it/garante/document?ID=1219452>; [Act

tradition allows the individual employee to decide whether to retain business data, whereas in the U.S., an enterprise-wide policy may govern retention of important business information.<sup>78</sup>

[26] A comprehensive understanding of what these laws, regulations, and opinions prohibit and permit, with regard to the “keeping” of information, is critical for those who would proffer such evidence, as well as those who would challenge its admission.

### E. Best Evidence/Original Evidence Rule

[27] The best evidence/original evidence rule is the last of the evidentiary hurdles that counsel must clear in order to successfully admit ESI.<sup>79</sup> Under F.R.E. 1002, the original “writing, recording, or

---

on the Protection of Personal Information], Law No. 57 of 2003, art. 27 (Japan), *translated at* <http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf>; Chan-Mo Chung, *Korea's Recent Legislation on Online Data Protection*, 6 PRIVACY L. & POL'Y REP. 38 (1999), *available at* <http://www.austlii.edu.au/au/journals/PLPR/1999/46.html>.

<sup>78</sup> *Compare* Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., 685 F. Supp. 2d 456, 474 (S.D.N.Y. 2010) (holding that Counsel did not meet the standard for a litigation hold, in part, by instructing plaintiffs to be over-, rather than under-, inclusive in collecting and preserving documents since that directive placed “total reliance on the employee to search and select what that employee believed to be responsive records without any supervision from Counsel”), *and* Phillip M. Adams & Assocs., LLC v. Dell, Inc., 621 F. Supp. 2d 1173, 1194 (D. Utah 2009) (holding that defendant had violated its duty to preserve information, in part because the defendant's preservation practices “place operations-level employees in the position of deciding what information is relevant”), *with* Io Group Inc. v. GLBT Ltd., No. C-10-1282 MMC (DMR), 2011 WL 4974337, at \*4 (N.D. Cal. Oct. 19, 2011) (finding an adverse inference charge warranted where the UK defendant admitted deleting e-mails, after receiving several litigation hold notices, on advice of UK counsel that e-mail retention violated the Data Protection Act).

<sup>79</sup> *See generally* FED. R. EVID. 1001-1008 (outlining the requirements for the best evidence rule).

photograph” is required when it is being offered to prove its content.<sup>80</sup> When the original is not available, duplicates are admissible under certain circumstances pursuant to F.R.E. 1003.<sup>81</sup> Thus, provided the printout of a website or other electronic record accurately reflects the original and no impropriety is alleged, such as an incomplete or altered record, an e-mail or database printout should meet the requirements of the original evidence rule.<sup>82</sup> Other exceptions to the original evidence rule include when the original or any duplicates of the electronic document have been lost or destroyed absent bad faith by the proponent, and are unavailable by any judicial process, remain in the possession of an opposing party on notice that it would be a subject of proof, or prove not relevant to a controlling issue.<sup>83</sup> Under these circumstances, a party may submit proof of the contents of the ESI through secondary evidence.<sup>84</sup>

[28] Proof of various laws and regulations, such as Argentina’s aforementioned Personal Data Protection Act and Israel’s Protection of

---

<sup>80</sup> FED. R. EVID. 1002.

<sup>81</sup> *See generally* FED. R. EVID. 1003; *see also* United States v. Bennett, 363 F.3d 947 (9th Cir. 2004) (excluding testimony as to readings of GPS on ground best evidence was a screen shot or printout); Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 576 (D. Md. 2007) (citing People v. Huehn, 53 P.3d 733, 738 (Colo. App. 2002)) (“[Rule 1003] essentially provides that duplicates are co-extensively admissible as originals, unless there is a genuine issue as to the authenticity of the original, or the circumstances indicate that it would be unfair to admit a duplicate in lieu of an original.”).

<sup>82</sup> Recall, however, some courts will approach ESI with skepticism. *See, e.g.*, St. Clair v. Johnny’s Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774 (S.D. Tex. 1999) (“While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation.”). Even so, recently published decisions seem to indicate that the opponent must do more than simply suggest that a document may have been altered. *See* United States v. Safavian, 435 F. Supp. 2d 36, 41 (D.D.C. 2006).

<sup>83</sup> *See* FED. R. EVID. 1004.

<sup>84</sup> *See* FED. R. EVID. 1004 advisory committee’s note.

Privacy Act, may also assist with meeting the evidentiary burdens under the best evidence/original evidence rule.<sup>85</sup> For example, Israeli law may proscribe transfer of the database, in which case counsel may offer a report of the database.<sup>86</sup> Counsel offering the evidence should be familiar with the applicable provisions of non-U.S. law, so that he or she may have a basis for the offer of the report in the absence of the actual database. Of course, practicalities should also enter into the argument; it is difficult to export an entire database and impractical to do so for only a few entries, notwithstanding the fact that juries may not have the patience or wherewithal to review an entire database. It is particularly critical that counsel seeking to challenge such truncated evidence on the ground that it is incomplete or inaccurate, be familiar with the need for, and quantum of, extrinsic evidence, especially since counsel must make an objection based on the original evidence rule at the time or risk waiver.<sup>87</sup> Section V below offers practical steps for offering proof of non-U.S. information protocols, laws, and regulations.

#### F. Self-Authentication: Is the Easier Path Available?

[29] The proponent of electronic evidence can avert a great deal of effort by establishing that the information offered is self-authenticating pursuant to F.R.E. 902, or state law equivalents,<sup>88</sup> which set forth categories of evidence which do not require extrinsic evidence as a condition precedent to admissibility.<sup>89</sup> F.R.E. 902(5) concerns

---

<sup>85</sup> See *supra* Part I.B.

<sup>86</sup> See Privacy Protection (Transfer of Databases Abroad) Regulations, 2001, KT 5761, 1-2 (Isr.).

<sup>87</sup> See *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 579 (D. Md. 2007).

<sup>88</sup> See FED. R. EVID. 902; see, e.g., N.Y. C.P.L.R. 4542(a) (CONSOL. 2011).

<sup>89</sup> See FED. R. EVID. 902.



governmental or public authority records.<sup>90</sup> If the ESI (including website information) contains reliable indicia that it is a public record, it may be admitted without secondary evidence of authenticity unless the nature of the ESI as emanating from a governmental authority faces challenges on other grounds (i.e., relevance, prejudice, hearsay, etc.).<sup>91</sup> Pursuant to F.R.E. 902(4), the ESI may be deemed self-authenticated if appropriately certified by official record, and thus admissible pursuant to Federal Rule of Civil Procedure (“F.R.C.P.”) 44(a)(2).<sup>92</sup> In a like fashion, F.R.E. 902(12) holds that non-U.S. ESI may be self-authenticating if it is shown, by appropriate certification, as the product of regularly conducted foreign business activity.<sup>93</sup>

[30] The Advisory Committee notes to F.R.C.P. 44(a)(2) explicitly reference and reproduce in full a treaty known as the Hague Convention on Abolishing the Requirement for Legalization of Foreign Public Documents (also known as the Hague Legalization Convention or The Apostille Convention).<sup>94</sup> It may provide an expedient for counsel to have official documents covered by the treaty admitted under the public records exception, if a public authority or representative of a public authority in a signatory state has certified the documents.<sup>95</sup> The United States is a

---

<sup>90</sup> FED. R. EVID. 902(5).

<sup>91</sup> See FED. R. EVID. 902 advisory committee’s note.

<sup>92</sup> FED. R. EVID. 902(4); see FED. R. CIV. P. 44(a)(2).

<sup>93</sup> FED. R. EVID. 902(12).

<sup>94</sup> FED. R. CIV. P. 44 advisory committee’s note.

<sup>95</sup> See HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW, OUTLINE HAGUE APOSTILLE CONVENTION (2009) [hereinafter HAGUE OUTLINE], available at [www.hcch.net/upload/outline12e.pdf](http://www.hcch.net/upload/outline12e.pdf).

signatory state.<sup>96</sup> The U.S. State Department notes that “[t]he treaty reduces the burden of the cumbersome ‘chain of authentication’ method of certifying documents which requires a long series of certificates.”<sup>97</sup> The certification, to be appended to the document, is known as an Apostille.<sup>98</sup> It contains ten elements, including country, language, and the capacity of the individual who has certified the document.<sup>99</sup> In this way, the treaty may suffice to deem public documents from a signatory country to fit within the F.R.E. 902(5) provision for self-authentication.<sup>100</sup> Yet the Convention is not the panacea for evidentiary foundation it may at first seem. First, the treaty applies only to public documents, though the definition of a “public document” varies between signatory countries.<sup>101</sup> U.S. counsel, in this regard, would be well-advised to obtain local counsel in the country of origin of the ESI. Second, the Convention dates from 1961, and only provides for Apostilles in paper form, to affix to paper documents.<sup>102</sup> The Hague Conference on Private International Law has recommended the adoption of electronic Apostilles, or “e-Apps,” for use

---

<sup>96</sup> See Hague Convention Abolishing the Requirement of Legalisation for Foreign Public Documents, Oct. 5, 1961, 527 U.N.T.S. 189, available at [http://www.hcch.net/index\\_en.php?act=conventions.status&cid=41](http://www.hcch.net/index_en.php?act=conventions.status&cid=41).

<sup>97</sup> *Judicial Assistance – Notarial and Authentication (Apostille)*, U.S. DEP’T OF STATE [hereinafter *Judicial Assistance*], [http://travel.state.gov/law/judicial/judicial\\_2545.html#3](http://travel.state.gov/law/judicial/judicial_2545.html#3) (last visited Feb. 16, 2012).

<sup>98</sup> *Id.*

<sup>99</sup> See *id.* The Apostille comprises ten elements, including country, name of signer, function of signer, authority of signer, and Apostille registration number. See *Model of Certificate*, HAGUE CONF. ON INT’L L., [hcch.e-vision.nl/upload/apostille.pdf](http://hcch.e-vision.nl/upload/apostille.pdf).

<sup>100</sup> See generally FED. R. EVID. 902(5).

<sup>101</sup> See HAGUE OUTLINE, *supra* note 95; *Judicial Assistance*, *supra* note 97.

<sup>102</sup> See *Judicial Assistance*, *supra* note 97 (noting a variety of methods to affix the Apostille, including “rubber stamp, glue, ribbons, wax seals, impressed seals, self-adhesive stickers, etc.”).

with documents in electronic format and, to that end, has facilitated a Pilot Program for the use of e-Apps.<sup>103</sup> Not all signatory countries have adopted the e-App, however, and therefore the utility of the Convention for foreign ESI is limited to data and electronic documents from participating signatory states.<sup>104</sup>

[31] The inability to obtain an appropriate certification does not necessarily prove fatal to self-authentication of foreign public records. If the parties have been given a reasonable opportunity to investigate the authenticity and accuracy of the records, counsel may offer an attested copy without certification upon an appropriate showing of good cause.<sup>105</sup>

[32] F.R.E. 902(7) provides for self-authentication if the record bears “[A]n inscription, sign, tag or label purporting to have been affixed in the course of business and indicating origin, ownership, or control.”<sup>106</sup> At first glance, this would appear to cover foreign e-mail that bears signature stamps or signature blocks of the corporate entity from which it emanated. Judge Grimm has cautioned, though, that “simply because an individual’s sending address is present on an e-mail does not constitute definitive proof that the person actually sent the e-mail, and authentication of an e-mail could still possibly require testimony from a person with personal knowledge of the transmission or its receipt to ensure its

---

<sup>103</sup> See *Closer and Closer to Reality: The e-Apostille Pilot Program of the HCCH and the NNA*, HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW, 3 (2006), [www.hcch.net/upload/e-app-fnl.pdf](http://www.hcch.net/upload/e-app-fnl.pdf).

<sup>104</sup> *Operational e-Registers by State*, HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW, [http://www.hcch.net/index\\_en.php?act=text.display&tid=146](http://www.hcch.net/index_en.php?act=text.display&tid=146) (last visited Feb. 16, 2012).

<sup>105</sup> See *In re* Letter of Request from Boras Dist. Court, Swed., 153 F.R.D. 31, 35-36 (E.D.N.Y. 1994); see also *United States v. Yousef*, 175 F.R.D. 192, 193-94 (S.D.N.Y. 1997).

<sup>106</sup> FED. R. EVID. 902(7).

trustworthiness.”<sup>107</sup> Indeed, he also notes that as of 2009, “no case since *Lorraine* has discussed the use of [F.R.E.] Rule 902(7) to gauge the authenticity of an e-mail.”<sup>108</sup>

[33] F.R.E. 902(12) may prove the most efficient path to admission, for at least certain types of ESI. F.R.E. 902(12) specifically concerns “Certified Foreign Records of a Regularly Conducted Activity.”<sup>109</sup> By reference to F.R.E. 902(11), this provision requires that the evidence be admissible under F.R.E. 803(6)(A)-(C) (a business records exception for “Records of Regularly Conducted Activity”), *if* accompanied by a declaration certifying:

- (A) the record was made at or near the time by—or from information transmitted by—someone with knowledge;
- (B) the record was kept in the course of a regularly conducted activity of a business . . .; and
- (C) making the record was a regular practice of that activity.<sup>110</sup>

---

<sup>107</sup> Grimm et al., *supra* note 4, at 389.

<sup>108</sup> *Id.* Consider that the absence of supportive case law may not necessarily indicate an unwillingness on the part of the judiciary to allow for the self-authentication of foreign ESI pursuant to F.R.E. 902(7), but rather, that F.R.E. 902(7) foundations may have gone unutilized or unchallenged. Accordingly, counsel should not rule out admission via F.R.E. 902(7), in the absence of better foundational avenues, or as a last resort.

<sup>109</sup> FED. R. EVID. 902(12). Congress amended FED. R. EVID. 902 in 2010 to include subdivisions (11) and (12). As noted by the advisory committee, the rule “sets forth a procedure by which parties can authenticate certain records of regularly conducted activity, other than through the testimony of a foundation witness,” and 902(12) serves as the civil analog to 18 USC § 3505, enacted in 1984, which provides a means for certifying foreign records of regularly conducted activity in criminal cases. FED R. EVID. 902 advisory committee’s note; *see* United States v. Laurent, No. 04-4745, 2006 U.S. App. LEXIS 6023, at \*4 (4th Cir. Mar. 10, 2006).

<sup>110</sup> FED. R. EVID 803(6).

[34] Furthermore, “[t]he declaration must be signed in a manner that, if falsely made, would subject the maker to a criminal penalty in the country where the certification is signed.”<sup>111</sup> In *St. Paul Mercury Ins. Co. v. FDIC*, the U.S. District Court for the Southern District of Florida admitted bank records from a bank in El Salvador, after affording the FDIC an opportunity to obtain proper certification of a declaration that had appropriately demonstrated the above-mentioned four elements.<sup>112</sup> The court took judicial notice of a Salvadoran law that banking institutions in El Salvador must provide data and information regarding their operations and activities when requested by the Financial System of El Salvador (SSF).<sup>113</sup> The court found that the person certifying the records was “qualified” because his position and experience demonstrated sufficient familiarity with the records such that he could attest to the reliability of the banking records:

[He] has been the superintendent and president of the board of directors of the SSF, the SSF oversees and regulates El Salvador's financial system; under Salvadoran law, banking institutions, such as Banco Cuscatlán, are required to provide data and information regarding their operations and activities when requested by the SSF. Based on these criteria, the Court . . . determined that [the certifying declarant's] position and experience demonstrate[d] . . . sufficient familiarity with these types of records such that he is qualified to attest to the reliability of the records at issue here.<sup>114</sup>

---

<sup>111</sup> FED. R. EVID. 902(12).

<sup>112</sup> See *St. Paul Mercury Ins. Co. v. FDIC*, No. 08-21192-CIV-GARBER, 2011 U.S. Dist. LEXIS 62604, at \*6 (S.D. Fla. June 10, 2011). See generally *St. Paul Mercury Ins. Co. v. FDIC*, No. 08-21192-CIV-GARBER, 2011 U.S. Dist. LEXIS 103135, at \*6 (S.D. Fla. Sept. 13, 2011).

<sup>113</sup> See *St. Paul Mercury Ins. Co.*, 2011 U.S. Dist. LEXIS 62604, at \*4.

<sup>114</sup> *St. Paul Mercury Ins. Co.*, 2011 U.S. Dist. LEXIS 10315, at \*7.

The court also concluded that in meeting the four elements of F.R.E. 902(12), the proponent had satisfied the requirements of the business records exception to the hearsay rule.<sup>115</sup> Similarly, in *United States v. Laurent*, a matter concerning a fraudulent visa application, the trial court apparently permitted the government to admit a visa application from Estonia with the condition that the government ultimately produce a certification to authenticate the document (which it did not have at that time), or else the court would “back [the document] out” of evidence.<sup>116</sup>

[35] Meeting all the elements necessary to demonstrate the trustworthiness of a document frequently takes on heightened significance when the source of the evidence comes from beyond U.S. borders. For example, in *Escriba v. Foster Poultry Farms*, medical evidence from Guatemala, which consisted of testimony from an attending physician and medical notes, did not meet the requirements of F.R.E. 902(12), as the documents were neither an original nor duplicate of certified foreign records of regularly conducted activity admissible under F.R.E. 803(6).<sup>117</sup> Yet, in *United States v. Parker*, involving cases of Dewars Scotch lifted from a foreign carrier shipment, a United Kingdom certificate for exports to the U.S. was admitted as an exception to the hearsay rule under F.R.E. 803(6) because “circumstantial evidence and testimony suggested trustworthiness.”<sup>118</sup> While the document was not authenticated under F.R.E. 902(12) (i.e., it was not self-authenticated via certification), the court found the testimony of the sole U.S. importer for Dewar's Scotch amply demonstrated the trustworthiness of the document and showed the document was a business record.<sup>119</sup> Here, the nature of the document

---

<sup>115</sup> *Id.* at \*11.

<sup>116</sup> *See* *United States v. Laurent*, No. 04-4745, 2006 U.S. App. LEXIS 6023, at \*5 (4th Cir. Mar. 10, 2006).

<sup>117</sup> *See* *Escriba v. Foster Poultry Farms*, 793 F. Supp. 2d 1147, 1156–57 (E.D. Cal. 2011).

<sup>118</sup> *United States v. Parker*, 749 F.2d 628, 633 (11th Cir. 1984).

<sup>119</sup> *Id.*

indicated to the court its reliability and authenticity and justified its admission as an exception to the hearsay rule.<sup>120</sup>

[36] The declaration requirement sounds very much like the foundation requirements for admission under the business records hearsay exception, described above, but the comparison's ease may be deceptive. One may not always have success in obtaining such a declaration, due to the information management practices of the entity in question or recalcitrance of the entity to submit such a declaration.<sup>121</sup> Non-e-mail communications, such as text messages, Instant Messages, and blog and social media posts, may not rise to the "regular activity" requirement of F.R.E. 902(12) or, for that matter, F.R.E. 803(6).<sup>122</sup> The "regular activity" criterion, along with temporal requirements ("made at or near the time of the occurrence"), and the F.R.E. 803(6) criterion that the evidence be created by a person "with knowledge" and pursuant to a "business activity," may provide grounds for challenge, but it is important to keep in mind that these terms and categories may have entirely different meanings and uses outside the U.S. due to linguistic issues, business practices, and cultural distinctions.<sup>123</sup>

### **G. Proof of Non-U.S. Information Protocols, Laws and Regulations and Language Translation**

[37] Where extrinsic evidence is required to authenticate foreign ESI,

---

<sup>120</sup> *See id.* The witness specifically testified that "[the] document was a customs certificate of the United Kingdom representing proof that the Scotch had been imported and thus the purchaser could avoid taxation in the United Kingdom for the cases of Scotch listed on the certificate." *Id.* *But see* discussion of admissibility under the F.R.E. 807(b) residual exception to the hearsay rule, *supra* notes 62-66 and accompanying text.

<sup>121</sup> *Compare* FED. R. EVID. 902(12), *with* FED. R. EVID. 803(6).

<sup>122</sup> *See* FED. R. EVID. 803(6); FED. R. EVID. 902(12).

<sup>123</sup> *See* FED. R. EVID. 803(6); FED. R. EVID. 902(12); *supra* Part I.B.

what form should it take? How does one go about proving foreign law and regulations? The first practical suggestion is for the parties to agree on translation of the *language(s)* used by the authors of the evidence, for both the evidence itself as well as the extrinsic matters offered in support of the evidence. If no agreement exists, the court may order the translators' documents, or a hearing for the conflicting versions pursuant to F.R.E. 702.<sup>124</sup>

1. The Declaration has been discussed above with regard to the certification of the need to *dispense* with extrinsic evidence, but a declaration of a different sort may serve to provide the necessary evidence of the computer and information management protocols that demonstrate indicia of reliability, as well as the regularity of the particular electronic activity in order to fit the evidence under one of the hearsay exceptions.<sup>125</sup> The practitioner should pay careful attention to the court's rules as to how far in advance of the trial, if at all, such declarations must be served upon the other parties, and whether the declarant may be subject to deposition.
2. A Witness with Knowledge of the Facts is often the most compelling support of the offer of proof. The witness can testify to a host of subjects, such as authenticity by virtue of the witness's knowledge of the information (i.e., he or she sent or received it), computer systems and information governance policies and procedures, identifying characteristics of the data, or business regularity with which the proffered types of data are created or received.<sup>126</sup>
3. Testimony of an Expert is particularly useful where one challenges, or must defend a challenge to, the reliability of the

---

<sup>124</sup> FED. R. EVID. 702.

<sup>125</sup> See generally *supra* Part I.F.

<sup>126</sup> See RICE, *supra* note 8, at 229-230, 232, 251. See generally FED. R. EVID. 901(B)(1).



system or applications that created the proffered data or the chain of custody for the data. Among other subjects appropriate for expert testimony are (i) the distinctive characteristics of the proffered evidence (hash values, metadata, replies to e-mails, etc.) (these may not require expert testimony, depending upon prior rulings and the style of the case),<sup>127</sup> (ii) the system's capacity to produce reliable information by virtue of its architecture, configuration, and maintenance, and (iii) the training of both the IT staff tasked with maintaining target systems as well as the end-users of those systems. However, the expert may be subject to the requirement for preparation and service of a report and for deposition pursuant to F.R.C.P. 26 or 30(b)(6).<sup>128</sup> The expert's potential testimony may also be subject to challenge under F.R.E. 702-704 and pursuant (depending upon the state) to preclusion motions and hearings pursuant to *Daubert v. Merrell Dow Pharmaceuticals*<sup>129</sup> or *Frye v. United States*.<sup>130</sup>

4. Certifications of Non-U.S. Counsel may be warranted to prove non-U.S. law. These may be challenged pursuant to F.R.E. 702, particularly if there are conflicting schools of thought on the scope of the particular law or regulations. The court may (and most often will) research the law on its own.<sup>131</sup> Instructive on this point in this regard is the case of *In re Rivastigmine Patent Litigation*,<sup>132</sup> in which the court, faced

---

<sup>127</sup> See Grimm et al., *supra* note 4, at 392.

<sup>128</sup> See *id.* at 377. See generally FED. R. CIV. P. 26.

<sup>129</sup> 509 U.S. 579, 597 (1993).

<sup>130</sup> 293 F. 1013, 1014 (D.C. Cir. 1923).

<sup>131</sup> See FED. R. EVID. 702.

<sup>132</sup> 237 F.R.D. 69 (S.D.N.Y. 2006).

with voluminous privilege logs comprising objections to data produced from nearly forty countries, ruled upon the quantum and quality of proof of privilege in the subject countries.<sup>133</sup>

Where there was no support from an affidavit of counsel from the subject country, or the affidavit did not provide sufficient information for the court to assess the assertion of privilege, the court ordered production of the disputed data.<sup>134</sup>

5. Translations should be the subject of agreement between counsel but, in litigation, the most obvious subjects for cooperation between counsel may become contentious and lengthy battles. While there is no requirement that non-U.S. data created in another language be translated in English for production in discovery,<sup>135</sup> the information cannot be offered into evidence unless translated into English. An inability to reach agreement on translation, such as may occur with regard to dialects in Chinese or Hindi, may result in a F.R.E. 702 hearing on the correct English iteration of the evidence.<sup>136</sup> Discussion of these issues early in the litigation may result in agreement that can avoid the time and expense of such hearings.

[38] Even after counsel has undergone the often arduous task of retrieving foreign-based ESI and clearing all of the aforementioned admissibility hurdles, courts may nonetheless exclude relevant ESI on one

---

<sup>133</sup> See *id.* at 87-88.

<sup>134</sup> See *id.* at 84.

<sup>135</sup> See *In re P.R. Elec. Power Auth.*, 687 F.2d 501, 509 n.3 (1st Cir. 1982) (“Congress could perhaps impose such a rule if it so desired, but the present Federal Rules provide no authority for such an extraordinary burden on foreign parties.”).

<sup>136</sup> See *Kumho Tire Co., Ltd. v. Carmichael*, 526 U.S. 137, 147 (1999) (holding that the trial judge’s gatekeeping function to determine reliability of evidence applies to *all* expert testimony). See *generally* FED. R. EVID. 702.

or more of the grounds articulated in F.R.E. 403 (i.e., unfair prejudice, confusion of the issues, undue delay, etc.).<sup>137</sup>

### III. CHALLENGES TO ADMISSIBILITY BASED ON PRETRIAL DISCOVERY CONDUCT

[39] Circumstances in which counsel may be precluded from using otherwise admissible non-U.S. information include the failure to comply with discovery orders, or to comply with notice requirements.<sup>138</sup> While such compliance is not a strictly evidentiary criterion, from a practical standpoint, litigation counsel should remain cognizant of the consequences of such omissions and other activities during discovery.<sup>139</sup> For example, pursuant to F.R.C.P. 26(a)(1)(A)(ii), provided the lawsuit is not an action described in F.R.C.P. 26(a)(1)(B), or unless otherwise ordered or stipulated:

[A] party must, without awaiting a discovery request, provide to the other parties... a copy—or a description by category and location—of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use

---

<sup>137</sup> See generally FED. R. EVID. 403 (precluding evidence in ESI cases, which may arise where there are confusing voluminous records, biased record summaries, computer animations that portray a matter unfairly, or electronic or text messages that contain highly offensive or derogatory language). This article will not focus on prejudice, but the reader is instructed to note that, as with paper documents, the proponent of any ESI must be prepared to argue not only relevance, but that the evidence's relevance preponderates over any unfair prejudice (as well as any other applicable exclusionary F.R.E. 403 factors).

<sup>138</sup> See FED. R. CIV. P. 37(b)(2)(A), (c)(1).

<sup>139</sup> See, e.g., *Adams v. Teck Cominco Alaska, Inc.*, 231 F.R.D. 578, 581 (D. Alaska 2005) (noting that the burden is on the disclosing party to ensure disclosure is complete and excluding documents not properly disclosed).

to support its claims or defenses, unless the use would be solely for impeachment.<sup>140</sup>

[40] Under F.R.C.P. 26(a)(1)(E), failing to fully investigate the case, challenging the sufficiency of another party's disclosures, or the other party's failure to make its initial disclosures, will not excuse a party from making its F.R.C.P. 26(a)(1) disclosures and may result in sanctions, including but not limited to, preclusion of certain evidence.<sup>141</sup> Moreover, F.R.C.P. 37 allows the court to impose broad sanctions for discovery-related abuses, and in the case of bad faith, the court may impose sanctions based on its "inherent power to manage its own affairs."<sup>142</sup> F.R.C.P. 37(c)(1) specifically provides that evidence will be excluded for failure to comply with F.R.C.P. 26(a) under certain conditions:

If a party fails to provide information or identify a witness as required by *Rule 26(a)* or *(e)*, the party is not allowed to use that information or witness to supply evidence on a motion, at a hearing, or at a trial, unless the failure was substantially justified or was harmless.<sup>143</sup>

[41] Thus, F.R.C.P. 37 sanctions give yet another reason for counsel to identify the documents they intend to rely upon, as well as the witnesses likely to have discoverable information, early on in litigation, in compliance with F.R.C.P. 26(a)(1).<sup>144</sup> Should a party fail to disclose copies, or even a description by category and location, of electronically stored information, there is a palpable risk that the court will exclude such

---

<sup>140</sup> FED. R. CIV. P. 26(a)(1)(A).

<sup>141</sup> FED. R. CIV. P. 26(a)(1)(E).

<sup>142</sup> *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 106-07 (2d Cir. 2002).

<sup>143</sup> FED. R. CIV. P. 37(c)(1).

<sup>144</sup> *See* FED. R. CIV. P. 37(c)(1); FED. R. CIV. P. 26(a)(1).

ESI when it is submitted in support of a motion or trial.<sup>145</sup> A certification pursuant to F.R.C.P. 26(g) made without the required diligence and investigation—i.e., a certification that all documents demanded have been disclosed when, in fact, certain documents have not been produced—may also subject counsel to sanctions.<sup>146</sup>

[42] Disclosure can become a nettlesome issue for a proponent of non-U.S. ESI because of the collision between U.S. discovery rules and non-U.S. privacy and data protection laws.<sup>147</sup> A party that declines to provide certain information during discovery on the grounds that doing so would violate the laws of the host country and, perhaps, subject the litigant to civil or criminal proceedings, may well find itself precluded from offering like kind evidence at trial, and may be subject to other sanctions as well.<sup>148</sup> In *Reino de Espana v. American Bureau of Shipping*, the government of Spain propounded discovery requests but resisted discovery demands served upon it on the ground that compliance would violate Spanish privacy law.<sup>149</sup> The court ordered the Spanish government to comply with the discovery demands, holding that Spain, which chose a U.S. venue for its suit, was bound to comply with U.S. discovery rules.<sup>150</sup>

---

<sup>145</sup> See, e.g., *Forbes v. 21st Century Ins. Co.*, 258 F.R.D. 335, 338 (D. Ariz. 2009) (prohibiting use of materials that were improperly disclosed under F.R.C.P. 26(a)(1)(A)(ii)); *Adams v. Teck Cominco Alaska, Inc.*, 231 F.R.D. 578, 581 (D. Alaska 2005).

<sup>146</sup> See FED. R. CIV. P. 26(g)(3).

<sup>147</sup> See *Reino de Espana v. Am. Bureau of Shipping*, No. 03 Civ. 3573 LTS/RLE, 2006 U.S. Dist. LEXIS 81415, at \*19 (S.D.N.Y. Nov. 3, 2006).

<sup>148</sup> Fed. R. Civ. P. 37(c)(1)(A)-(C) (providing that, if a party fails to disclose information “the party is not allowed to use that information... at a trial, unless the failure was substantially justified or is harmless,” and the party may also be subject to other sanctions).

<sup>149</sup> See *Reino De Espana*, 2007 U.S. Dist. LEXIS 41498, at \*3-4.

<sup>150</sup> See *id.* at \*26. Ultimately, Spain narrowly escaped an adverse inference charge, even though the court found it negligently failed to implement a timely litigation hold, because

[43] The national oil company of Venezuela found itself in a similar situation in *Lynodell-Citgo Refining P.P. v. Petroleos de Venezuela, S.A.*<sup>151</sup> The defendant was served with a discovery demand for minutes of its board of directors.<sup>152</sup> Compliance with the demand, which would have of necessity divulged the identity of the directors and placed them at a particular location on a certain date, would have violated Venezuela's Special Law Against Information Systems Crimes and subjected the defendant to potential criminal prosecution.<sup>153</sup> Because the defendant declined to comply with a court order directing provision of the minutes, the court sanctioned the defendant with an adverse inference jury instruction.<sup>154</sup> While not specifically addressed in the decision, there is little doubt that Petroleos de Venezuela, having raised an objection to producing the minutes because of the requirements of local law, would have been precluded from offering similar evidence at trial.<sup>155</sup> Counsel, then, should carefully weigh its position and the relative risks when considering whether to bring applications to quash subpoenas or motions for Protective Orders on the basis of local privacy or data protection laws.

---

pplaintiff could not demonstrate that the missing evidence was relevant. *See id.* at \*21-24. *But cf.* *IO Group Inc. v. GLBT LTD.*, No. C 10 1282 MMC (DMR), 2011 U.S. Dist. LEXIS 120815, at \*8 (N.D. Cal. Oct. 19, 2011) (granting pplaintiff's motion for an adverse inference charge against ddefendant).

<sup>151</sup> *See* *Lyondell-Citgo Refining, LP v. Petroleos De Venezuela, S.A.*, No. 02 Civ. 0795(CBM), 2005 WL 356808, at \*1 (S.D.N.Y. Feb. 15, 2005).

<sup>152</sup> *Id.*

<sup>153</sup> *See id.*

<sup>154</sup> *See id.* at \*1-2, 4. An adverse inference jury instruction advises the jury that the producing party had a legal duty to produce the subject information but did not do so, and that the jury may presume, though it is not required to do so, that the subject information would have been adverse to the position of the jury at trial. *Zubulake v. UBS Warburg, L.L.C.*, 229 F.R.D. 422, 430 (S.D.N.Y. 2004).

<sup>155</sup> *Cf. Reino De Espana*, 2007 U.S. Dist. LEXIS 41498, at \*26; notes 149-50 and accompanying text.

A long view toward trial is often advisable in formulating discovery strategy.

#### IV. ADMISSIBILITY OF NON-U.S. ESI IN MOTION PRACTICE

[44] The rules that govern the admission of documentary evidence at trial apply with equal force to dispositive and *in limine* motions that require support by proof in admissible form; however, recent changes in procedural rules have altered the logistics and burdens for demonstrating admissibility of supporting documents for such motions.<sup>156</sup>

[45] F.R.C.P. 56 governs summary judgment practice.<sup>157</sup> Until very recently, the rule clearly stated that unauthenticated documents may not be considered on a motion for summary judgment.<sup>158</sup> Under F.R.C.P. 56, parties were required to present documentary proof in *admissible* form in support of summary judgment papers.<sup>159</sup> Accordingly, counsel was essentially required to lay the foundation for every piece of documentary evidence appended to their summary judgment motions. Failure to comply with this requirement would preclude the court from considering the evidence, sometimes resulting in summary judgment decisions in which the judiciary would lambast counsel for foundational omissions.<sup>160</sup> *Bowers v. Rector and Visitors of the University of Virginia* provides a cautionary tale as the evidence takes on the additional layer of complexity, such as those encountered with ESI from other countries.<sup>161</sup> In *Bowers*,

---

<sup>156</sup> See, e.g., FED. R. CIV. P. 56 (Supp. IV 2010).

<sup>157</sup> See generally FED. R. CIV. P. 56.

<sup>158</sup> See FED. R. CIV. P. 56 (Supp. III 2009).

<sup>159</sup> FED. R. CIV. P. 56(e)(1) (Supp. III 2009).

<sup>160</sup> See *infra* notes 161-64 and accompanying text.

<sup>161</sup> *Bowers v. Rector & Visitors of the Univ. of Virginia*, No. 3:06cv00041, 2007 WL 2963818, at \*1 (W.D. Va. Oct. 9, 2007); accord Grimm et al., *supra* note 4, at 369-70.

an employment matter alleging improper termination, counsel appended 600 pages of e-mails and website printouts.<sup>162</sup> Her foundation for authentication comprised mostly counsel's own affidavit averring the information's authenticity because "the e-mails had been obtained from the defendants during the course of discovery and the web pages were taken from 'published' internet web sites."<sup>163</sup> The court, in granting the defendants' motion for sanctions pursuant to F.R.C.P. 56(g), excoriated counsel as follows:

[T]he submission by plaintiff's counsel of . . . more than fifty unauthenticated copies of e-mails convincingly demonstrates both a recklessness and an absence of preparation on the part of plaintiff's counsel. Equally so, her resort to use of her own affidavit in a misguided quick-and-easy attempt to fix significant evidentiary deficiencies, demonstrates a recklessness in preparation and a failure to exercise legal judgment abject.<sup>164</sup>

[46] In 2010, the Supreme Court introduced a new subdivision of F.R.C.P. 56, Subdivision (c), which "establishes a common procedure for several aspects of summary-judgment motions . . ." <sup>165</sup> Subdivision (c), entitled "Procedures," provides in relevant part:

- (1) A party asserting that a fact cannot be or is genuinely disputed must support the assertion by:
  - (A) citing to particular parts of materials in the record, including depositions, documents, *electronically stored information*, affidavits or declarations, stipulations

---

<sup>162</sup> *Bowers*, 2007 WL 2963818, at \*1.

<sup>163</sup> *Id.* at \*2.

<sup>164</sup> *Id.* at \*7.

<sup>165</sup> FED. R. CIV. P. 56(c) advisory committee's notes (Supp. IV 2010).



(including those made for purposes of the motion only),  
admissions, interrogatory answers, or other materials; or

•••

(2) A party may object that the material cited to support or dispute a fact cannot be presented in a form that would be admissible in evidence.<sup>166</sup>

[47] Subdivision (c)(2) sets out a new procedure for submitting documentary proof in support of summary judgment motions.<sup>167</sup> The advisory committee summarized this procedure as follows:

[A] party may object that material cited to support or dispute a fact cannot be presented in a form that would be admissible in evidence. The objection functions much as an objection at trial, adjusted for the pretrial setting. The burden is on the proponent to show that the material is admissible as presented or to explain the admissible form that is anticipated. There is no need to make a separate motion to strike. If the case goes to trial, failure to challenge admissibility at the summary-judgment stage does not forfeit the right to challenge admissibility at trial.<sup>168</sup>

---

<sup>166</sup> FED. R. CIV. P. 56(c)(1)(A)-(2) (Supp. IV 2010) (emphasis added).

<sup>167</sup> FED. R. CIV. P. 56(c)(2) (Supp. IV 2010). In addition to motions for summary judgment, the admissibility issue may arise as early as pre-answer motion practice. Pursuant to F.R.C.P. 12(d): “If, on a motion under Rule 12(b)(6) or 12(c), matters outside the pleadings are presented to and not excluded by the court, the motion must be treated as one for summary judgment under Rule 56. All parties must be given a reasonable opportunity to present all the material that is pertinent to the motion.” FED. R. CIV. P. 12(d).

<sup>168</sup> FED. R. CIV. P. 56 (c)(2) committee notes on rules (Supp. IV 2010).

[48] Ostensibly, Subdivision (c) may obviate the need for counsel to provide the basis for a document's admissibility. The language is ambiguous, and with the exception of *Foreword Magazine v. Overdrive*, the courts have yet to weigh in on whether unchallenged evidence, for which counsel has laid no foundation, will be considered on summary judgment.<sup>169</sup> Indeed, the new F.R.C.P. 56(c) creates more questions than it answers. For example, does the new rule suggest that only after objection does the burden shift to the proponent to demonstrate admissibility?<sup>170</sup> For this reason alone, the wording of the subdivision should give counsel pause because it does not speak on whether a court may exclude evidence on a *sua sponte* basis, especially in light of case law under the former F.R.C.P. 56, which, by and large, holds that "[a] trial court can only consider admissible evidence in ruling on a motion for summary judgment."<sup>171</sup> One must question whether this holding is consistent with the procedure articulated in the new subdivision and, if so, how.

[49] In *Foreword Magazine*, the U.S. District Court for the Western District of Michigan explained that the new subdivision had replaced former F.R.C.P. 56(2), which had unequivocally mandated authentication for documents presented in summary judgment motions.<sup>172</sup> But, the court warned, as a result of the 2010 amendments to F.R.C.P. 56, parties must

---

<sup>169</sup> *Foreword Magazine, Inc. v. Overdrive, Inc.*, No. 1:10-cv-1144, 2011 U.S. Dist. LEXIS 125373, at \*3-6 (W.D. Mich. Oct. 31, 2011) ("Thus, the amendment replaces a clear, bright-line rule ('all documents must be authenticated') with a multi-step process by which a proponent may submit evidence, subject to objection by the opponent and an opportunity for the proponent to either authenticate the document or propose a method to doing so at trial.").

<sup>170</sup> See 11 JAMES WM. ET AL., *MOORE'S FEDERAL PRACTICE* § 56.91[7] (3d ed. 2011) ("If a party fails to object to the inadmissibility of evidence submitted by its opponent in the summary judgment proceedings, the court may consider the evidence.").

<sup>171</sup> *Orr v. Bank of America, NT & SA*, 285 F.3d 764, 773 (9th Cir. 2002).

<sup>172</sup> See *Foreword Magazine*, 2011 U.S. Dist. LEXIS 125373, at \*3-4.

not disregard the prevailing authorities but, in fact, should read them very carefully.<sup>173</sup> The *Foreword Magazine* court found that the “unequivocal requirement” of authentication for documents submitted in support of summary judgment papers was effectively eliminated.<sup>174</sup> According to the *Foreword Magazine* court, the opponent must now object to the admissibility of evidence, demonstrating a paradigm shift from objection that the item “has not” been submitted in admissible form to objection that it “cannot” be.<sup>175</sup> The court interpreted the comments to the 2010 amendments to mean that “the drafters intended to make summary judgment practice conform to procedure at trial.”<sup>176</sup>

[50] *Foreword Magazine* is one of very few published decisions interpreting the significance of the new F.R.C.P. 56(c); in contrast, some other decisions cite to earlier versions of the statute, indicating that some litigators and judiciary may rely on the old rule in support of their briefs and decisions.<sup>177</sup> This presents a conundrum for practitioners making dispositive motions. If they submit materials in support of their summary judgment motion without laying any evidentiary foundation whatsoever, in reliance on the new F.R.C.P. 56(c), will they be penalized for the omission as though the old rule were still in effect? This risk may be heightened when citing to foreign ESI in support of or opposition to dispositive motions, as authenticity issues may loom large in the mind of the judge considering the motion. In this regard, it is helpful to recall that the court, even if it is well aware of the new procedure, may exclude the

---

<sup>173</sup> *Id.* at \*4.

<sup>174</sup> *Id.*

<sup>175</sup> *Id.* at \*5.

<sup>176</sup> *Id.*

<sup>177</sup> *See, e.g.,* Arroyo-Perez v. Demir Grp. Int’l, 762 F. Supp. 2d 374, 376 (Dist. P.R. 2011).

evidence *sua sponte* or, as the court stated in *Foreword*, hold the proponent of the evidence to trial standards of authentication.<sup>178</sup>

[51] Thus, the practitioner who plans to rely on Subdivision (c) by appending ESI proof to a dispositive motion without providing the evidentiary basis for its admissibility would be well advised to assess the risk of exclusion or disregard of the evidence by the court. To make this assessment, counsel should be knowledgeable about local rules,<sup>179</sup> any prior decisions of the motion court with regard to the new procedure, and how the court has considered ESI proof generally as well as ESI from outside the U.S.

[52] An opposing party's level of cooperation may also influence counsel's course of action. For example, in the case of a foreign party unfamiliar with U.S. litigation, from a jurisdiction in which privacy and/or data protection laws may give such party pause when it comes to fully complying with the discovery process, any delay or impairment of counsel's ability to ascertain all the information necessary to overcoming evidentiary hurdles may make submitting documents in accordance with Subdivision (c)'s new procedure very attractive, provided the court follows the logic articulated in the *Foreword* decision. The case arguably affords counsel the opportunity to seek the disposition of a matter without

---

<sup>178</sup> See *Foreword Magazine*, 2011 U.S. Dist. LEXIS 125373, at \*5.

<sup>179</sup> Some U.S. District Court local rules mirror the new F.R.C.P. subdivision. See, e.g., U.S. DIST. CT. FOR THE DIST. OF OR. LOCAL R. CIV. P. 56-1(b) (2011), available at <http://www.ord.uscourts.gov/en/local-rules-of-civil-procedure/lr-56-summary-judgment>. Others resemble the old version of F.R.C.P. 56. See, e.g., LOCAL RULES OF THE U.S. DIST. COURTS FOR THE SOUTHERN AND EASTERN DIST. OF NEW YORK, LOCAL RULE 56.1 (2011), available at <http://www.nyed.uscourts.gov/pub/docs/localrules.pdf>; see also LOCAL RULES OF THE U.S. DIST. COURTS FOR THE SOUTHERN AND EASTERN DIST. OF NEW YORK, LOCAL RULE 56.1, advisory committee's note (2011), available at <http://www.nyed.uscourts.gov/pub/docs/localrules.pdf> ("the Committee believes that the language adopted in 2004 sets forth these requirements clearly, and does not recommend any changes in that language.").

being forced to submit evidence in admissible form when, under the circumstances, such evidence is not easily authenticated.

[53] The pretrial discovery phase of litigation also offers other opportunities to tackle thorny evidentiary issues involving foreign ESI. Under F.R.C.P. 36, for example, a party may request that his or her adversary admit to the “genuineness of a document,”<sup>180</sup> which may be of mutual benefit in matters where both parties are multinational entities. Litigants should raise these issues, and others regarding foreign ESI authentication issues, at the earliest opportunities, including discovery conferences pursuant to F.R.C.P. 26(f) and 16.<sup>181</sup>

[54] Motions *in limine* present another key opportunity to address the exclusion or admission of evidence in advance of trial. The purpose of a motion *in limine* is typically to limit or exclude certain evidence or testimony, but it may also be used by a proponent seeking to admit evidence.<sup>182</sup> The motion is generally made at the commencement of trial,<sup>183</sup> and the judge hears it outside the presence of the jury. Motions *in limine* can be an important tool for trial counsel and can accordingly reduce the number of disruptions (e.g., side-bar conferences and objections) during trial.<sup>184</sup> More important, a motion *in limine* permits the court to rule on the relevance and admissibility of evidence before counsel

---

<sup>180</sup> FED. R. CIV. P. 36(a)(3) (“A matter is admitted unless, within 30 days after being served, the party to whom the request is directed serves on the requesting party a written answer or objection addressed to the matter and signed by the party or its attorney.”).

<sup>181</sup> See FED. R. CIV. P. 16; FED. R. CIV. P. 26(f).

<sup>182</sup> See FED. R. EVID. 104; BLACK’S LAW DICTIONARY 1109 (9th ed. 2009).

<sup>183</sup> See BLACK’S LAW DICTIONARY 1109 (9th ed. 2009).

<sup>184</sup> See *Bastilla v. The Village of Cahokia*, No. 06-CV-0150-MJR, 2010 U.S. Dist. LEXIS 1939, at \*2 (S.D. Ill. Jan. 11, 2010) (citing *Palmieri v. Defaria*, 88 F.3d 136, 141 (2d Cir. 1996)) (explaining that motions *in limine* can speed up the trial process by avoiding interruptions and lengthy arguments at trial).

offers it at trial, thus reducing time spent in hearings outside the presence of the jury.<sup>185</sup>

[55] In the case of foreign ESI, a motion *in limine* hearing may serve as an opportunity for counsel to fully educate the court on the source, creation, and maintenance of the proffered data or documents.<sup>186</sup> This, in turn, may well trigger the judge to initiate a F.R.E. 104(a) examination of the evidence.<sup>187</sup> F.R.E. 104(a) provides that: “the court must decide any preliminary question about whether a witness is qualified, a privilege exists, or evidence is admissible.”<sup>188</sup> Generally, the proponent will carry the burden of persuasion by a preponderance of evidence on preliminary questions concerning admissibility.<sup>189</sup> Conversely, under F.R.E. 104(b), the court does not employ the same standard as under F.R.E. 104(a) when

---

<sup>185</sup> *See id.* Hearings on admissibility during state court trials, known as *voir dire*, are conducted outside the hearing of the jury.

<sup>186</sup> *See generally* 21 FED. PRAC. & PROC. EVID. § 5037.10 (2d ed. 2011) (explaining that motions *in limine* “[allow] the parties to more thoroughly brief the law and the court to consider the arguments more thoroughly than would be possible in the heat of trial”); G. Michael Fenner, *The Daubert Handbook: The Case, Its Essential Dilemma, and Its Progeny*, 29 CREIGHTON L. REV. 939, 957 (1996) (explaining that early 104(a) rulings help to educate judges about special vocabulary before evidence begins to come in).

<sup>187</sup> *See Bastilla*, 2010 U.S. Dist. LEXIS 1939 at \*1-2 (both parties’ motions *in limine* caused the judge to conduct F.R.E. 104 analysis). Also note that, under F.R.E. 104(c), there is no guarantee that once trial is underway, a hearing on admissibility will be conducted outside the presence of the jury, unless the court is ruling on the admissibility of a confession; the interests of justice require it; or it is at the request of a witness, and that witness is the accused. FED. R. EVID. 104(c).

<sup>188</sup> FED. R. EVID. 104(a) (stating that a court ruling on the admissibility of evidence is “not bound by the rules of evidence except those on privilege”).

<sup>189</sup> *See, e.g.,* *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579, 592 n.10 (1993); *Bourjaily v. United States*, 483 U.S. 171, 175 (1987); *Miller v. Keating*, 754 F.2d 507, 511 (3d Cir. 1985).

deciding questions of conditional relevancy.<sup>190</sup> Instead, the standard is effectively a *prima facie* standard, as the trial court only determines whether the proponent presented sufficient evidence to support a finding of the fulfillment of the condition.<sup>191</sup> The distinction, in practice, is subtle.<sup>192</sup>

[56] Discovery conferences pursuant to F.R.C.P. 16, and other pre-trial conferences, provide additional opportunities to preliminarily address admissibility.<sup>193</sup> For example, F.R.C.P. 16(c)(2) not only permits counsel to request that the adversary stipulate to the authenticity of documents, including ESI, but also allows the court the chance to assess the evidentiary issues and take appropriate action to address any such applications.<sup>194</sup> Thus, an opposing counsel's refusal of the request could prompt a F.R.E. 104(a) examination of the foundational grounds for the document's admissibility, at which time, depending on the evidentiary rules at issue, counsel could make a *prima facie* showing of authenticity to the court.<sup>195</sup>

---

<sup>190</sup> See FED. R. EVID. 104(b) ("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>191</sup> *Id.*

<sup>192</sup> See, e.g., *Nat'l Union Fire Ins. Co. of Pittsburgh v. L.E. Myers Co. Grp.*, 937 F. Supp. 276, 287 (S.D.N.Y. 1996) (illustrating that when the court "lacks the necessary specificity with respect to the evidence to be excluded," the motion can be denied). Moreover, the court may in its discretion alter an *in limine* ruling at trial. *Luce v. United States*, 469 U.S. 38, 41-42 (1984).

<sup>193</sup> See generally FED. R. CIV. P. 16.

<sup>194</sup> See FED. R. CIV. P. 16(c)(2).

<sup>195</sup> See FED. R. EVID. 104(a) (authorizing the court to determine preliminary admissibility matters including whether the proponent of evidence has laid down a sufficient foundation, from which the jury could find the evidence is authentic).

## V. AUTHENTICATION OF SPECIFIC CATEGORIES OF ESI ENCOUNTERED IN CROSS BORDER MATTERS

[57] Historically, as technological innovations have given rise to new types of evidence, judges have initially met such offerings with a significant level of skepticism, especially with regard to evidence collected from the Internet.<sup>196</sup> However, the approach of U.S. courts toward authenticating electronic evidence has evolved. Some courts still may suggest that “the complex nature of computer storage calls for a more comprehensive foundation,”<sup>197</sup> but others hold that discovery of new types of ESI “requires the application of basic discovery principles in a novel context.”<sup>198</sup> While ESI authentication occurs in the same manner as any other type of evidence, different forms of ESI have distinct characteristics and qualities that impact admissibility. In a world where paper documents compare to electronic information as the horse and buggy compares to the

---

<sup>196</sup> See *St. Clair v. Johnny’s Oyster & Shrimp, Inc.*, 76 F. Supp. 2d 773, 774-75 (S.D. Tex. 1999). In holding the plaintiff’s proffered data from the US Coast Guard’s online vessel database insufficient, U.S. District Judge Samuel Kent stated “[w]hile some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation.” *Id.* Judge Kent went on to state:

[a]nyone can put anything on the Internet. No web-site is monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on any web-site from any location at any time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules. . . .

*Id.*

<sup>197</sup> *United States v. Scholle*, 553 F.2d 1109, 1125 (8th Cir. 1976).

<sup>198</sup> *Equal Emp’t Opportunity Comm’n v. Simply Storage Mgmt.*, 270 F.R.D. 430, 434 (S.D. Ind. 2010) (in reference to social networking sites).



automobile and where online interaction is the daily norm, the Federal Rules of Civil Procedure have been amended to explicitly cover the discovery of “electronically stored information,”<sup>199</sup> and courts have begun to apply the rules of admissibility to the realities of the Digital Age. This section will address the issues associated with the admissibility of types of ESI frequently encountered during disputes between multinational entities, namely e-mails, text messages, instant messages, electronic chat logs, web pages, archived Internet content, social media, Internet tracking information, and log files.

### A. E-mail

[58] As attractive markets abroad entice U.S. companies to expand overseas and the Internet continues to erode traditional barriers between foreign companies and U.S. consumers, more subsidiaries and affiliates of U.S. companies and foreign companies doing business in the U.S. will find themselves subject to the long arm of U.S. jurisdiction.<sup>200</sup> E-mail serves as a primary bridge to facilitate the communication that makes this global interconnectivity possible.<sup>201</sup> The more we e-mail, the more e-mail will be potentially relevant to U.S. legal proceedings.

[59] When offering e-mail into evidence, counsel must show that the information is self-authenticating under F.R.E. 902<sup>202</sup> or meet the

---

<sup>199</sup> FED. R. CIV. P. 26(a)(1)(A)(ii).

<sup>200</sup> See generally 4 CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 1068 (3d ed.) (discussing how long-arm statutes have expanded over time to allow for jurisdiction over foreign companies performing significant business in the United States, either at the state or national level).

<sup>201</sup> See SEDONA FRAMEWORK, *supra* note 1 at 1.

<sup>202</sup> Courts most often deem e-mail evidence to be self-authenticating under FED. R. EVID. 902(7) (Trade Inscriptions and the Like), and FED. R. EVID. 902(11) (Certified Domestic Records of a Regularly Conducted Activity).

standards for authentication under F.R.E. 901.<sup>203</sup> Where a proponent makes no attempt to authenticate e-mail evidence by offering any explanation as to its origin, the court will likely rule that the document is unauthenticated and thus inadmissible.<sup>204</sup> As with any other evidence, counsel must take steps to show that the e-mail is what it purports to be. Testimony from one with personal knowledge of the e-mail in question is a widely accepted method for showing an e-mail's authenticity.<sup>205</sup> Furthermore, many courts have held that live testimony of a witness with personal knowledge may not be necessary if an affidavit of such a witness, combined with non-hearsay evidence of identifying characteristics (such as the URL address, date of the exchange, print date, profile names of the messengers, identity of the sender and recipient, etc.), is available to show authenticity:

The lower [federal] courts generally hold that an affidavit of a witness, when viewed in combination with circumstantial indicia of authenticity (such as the existence of the URL, date of printing, or other identifying

---

<sup>203</sup> See FED. R. EVID. 901; *United States v. Safavian*, 435 F. Supp. 2d 36, 40-41 (discussing how e-mail may be authenticated under the Federal Rules of Evidence). It is important to note that in many courts, parties must address authentications and other admissibility issues with regards to each individual e-mail comprising a chain or thread. See, e.g., *New York v. Microsoft Corp.*, No. CIV A. 98-1233, 2002 WL 649951 at \*5 (D.D.C. 2002) (holding that the individual e-mail messages did not overcome the hearsay requirements to be admitted).

<sup>204</sup> See *Boyd v. Toyobo Am., Inc. (In re Second Chance Body Armor, Inc.)*, 434 B.R. 502, 505 (Bankr. W.D. Mich. 2010) (holding that e-mail was not properly authenticated where it bore no indicia of authenticity and the e-mail was an internal communication between employees of a non-party company, and the proponent's witness was not an employee of that company, was not listed as a recipient of the e-mail, and testified that he had never seen the e-mail).

<sup>205</sup> See *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 545 (D. Md. 2007).

information) would support a reasonable juror in the belief that the documents are what the proponent says they are.<sup>206</sup>

[60] Despite the fact that e-mails present numerous metadata fields and other characteristics that can be used as indicia of authenticity, F.R.E. 901 sets a relatively low bar for clearing the authenticity hurdle since the proponent must only “produce evidence to support a finding that the item is what the proponent claims.”<sup>207</sup> In other words, judges may leave questions of origin, business practices, etc. to the jury to attach such importance as they deem appropriate. Furthermore, the court need not make a determination that the evidence is what the proponent claims, rather, it should determine whether there is evidence sufficient for a reasonable jury to make that determination.<sup>208</sup> Once meeting this “minimal authentication requirement,” arguments concerning the accuracy of the printouts go only to weight, not admissibility.<sup>209</sup>

[61] In the case of e-mail collected from foreign sources, obtaining evidence supporting authenticity in the form of live testimony from the sender or recipient of an e-mail, or the controller of a server where the e-

---

<sup>206</sup> *Foreword Magazine v. OverDrive, Inc.*, No. 1:10-CV-1144, 2011 WL 5169384 at \*3 (W.D. Mich. 2011).

<sup>207</sup> FED. R. EVID. 901(a).

<sup>208</sup> *See Safavian*, 435 F. Supp. 2d at 38 (“The threshold for the Court’s determination of authenticity is not high... The Court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so.” (citations omitted)).

<sup>209</sup> *See United States v. Meienberg*, 263 F.3d 1177, 1181 (10th Cir. 2001). Computer printouts of records maintained by the Colorado Bureau of Investigation were deemed authenticated through testimony by a government witness that the printouts reflected the Bureau’s record of information about the defendant’s business. *Id.* The court went on to note that such public records can be authenticated by showing custody and nothing more. *Id.* (citing FED. R. EVID. 901, advisory committee notes, 1972 Proposed Rules).

mail is held, may not be possible or practical.<sup>210</sup> For example, if the witness is in a foreign country, he or she may be beyond subpoena power, or may not be willing to travel to the U.S. If so, is the witness willing to provide oral testimony, an affidavit, sworn declaration, or unsworn declaration as permitted by 28 U.S.C. §1746? It may be that the applicable laws of the foreign country (such as blocking statutes that proscribe testimony or evidence provided for a foreign judicial proceeding),<sup>211</sup> company culture, or local customs may preclude a witness from testifying in the litigation.<sup>212</sup>

[62] If authenticating direct testimony, whether oral or written, should prove impractical, and assuming that such e-mails are not self-authenticating under F.R.E. 902 or other provisions, counsel must look to other modes of authentication through more circumstantial evidence such as (i) expert testimony, (ii) comparison of the e-mail to another communication that has already been authenticated, (iii) distinctive characteristics and other circumstances indicating reliability, or (iv) some other method sufficient to clear the authenticity hurdle.<sup>213</sup> It behooves counsel to gather all identifying and circumstantial evidence surrounding

---

<sup>210</sup> See generally SEDONA FRAMEWORK, *supra* note 2 at 10 (giving an example of how the location of a server can hinder the discovery process and how the law must be adopted to deal with such issues).

<sup>211</sup> See *id.* at 18.

<sup>212</sup> Cf. Karen McVeigh and Amelia Hill, *Bill Limiting Sharia Law is Motivated by 'Concern for Muslim Women,'* THE GUARDIAN, Jun. 8, 2011, <http://www.guardian.co.uk/law/2011/jun/08/sharia-bill-lords-muslim-women> (The practice under Sharia law of ascribing testimony from a female witness half the weight of that from a man, for example, could ultimately have some impact on gathering testimony from such a witness for use in a U.S. Court.).

<sup>213</sup> See *U.S. Info. Sys. Inc. v. Int'l Bhd.*, No. 00 Civ 4763 RMB JCF, 2006 WL 2136249 at \*7 (S.D.N.Y. Aug. 1, 2006) (highlighting that under some circumstances, the mere fact that documents were produced pursuant to discovery or a subpoena is sufficient for authentication).

e-mail early in the litigation to help support authenticity in the context of foreign e-mail. Such evidence may include descriptions of contemporaneous events and opinions, references to certain circumstances specifically known by the sender, a time stamp prior to litigation,<sup>214</sup> certain unique uses of language, or circumstantial evidence associated with whether e-mail services are provided through an ISP, an employer, or via a web-based service (i.e., web-based services will have a unique URL that can go towards authentication; evidence of the authentication and access controls used to secure an employer-provided e-mail system may be used to address concerns regarding hacking or fraudulent use).<sup>215</sup>

### **B. Text Messages, Instant Messages, and Electronic Chat Logs**

[63] Text messages, instant messages, and electronic chat logs present the same types of challenges to authenticity as e-mail; namely that anyone with access to the sending device could feasibly author a particular message and that—as with e-mail—“while an electronic message can be traced to a particular computer, it can rarely be connected to a specific author with any certainty.”<sup>216</sup> However, counsel can overcome these challenges, and the purported text, instant message or electronic chat log can be authenticated in the same manner as any other document: through the introduction of evidence that the text, instant message or chat log is what the proponent says.<sup>217</sup> This authenticating evidence can take the

---

<sup>214</sup> *See id.* at \*6.

<sup>215</sup> *See generally Lorraine* 241 F.R.D. at 551-52 (discussing how employer company e-mail can help identify the source of the e-mail).

<sup>216</sup> *In re F.P.*, 878 A.2d 92, 95 (Pa. Super. Ct. 2005) (quoting appellant’s argument).

<sup>217</sup> *Id.* at 96 (“We see no justification for constructing unique rules for admissibility of electronic communications such as instant messages; they are to be evaluated on a case-by-case basis as any other document to determine whether or not there has been an adequate foundational showing of their relevance and authenticity.”).

form of testimony from a witness who participated in the communication,<sup>218</sup> expert testimony or comparison with a previously authenticated message, or evidence of distinctive characteristics and corroborating circumstances. Counsel must remain cognizant, though, of language translation issues, as discussed *supra*.

[64] The testimony of any participant in the conversation can authenticate a text, message, or chat log, thereby evening the playing field for practitioners who may not be able to access foreign participants' live testimony. Thus, a text message can be authenticated even in situations where the witness did not print out or save the message<sup>219</sup> or there is no testimony from an Internet Service Provider or other expert.<sup>220</sup>

---

<sup>218</sup> See *United States v. Barlow*, 568 F.3d 217, 220 (5th Cir. 2009) (upholding a sex crimes conviction by finding that chat log transcripts were properly authenticated through testimony from a woman posing as a minor child who participated in online chats with the defendant, and that the transcripts fully and fairly reproduced the chats between her and the defendant). The *Barlow* Court went on to note that the issue of authenticating online chat log transcripts through testimony of the other participant had been addressed previously. *But see United States v. Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007) (finding sufficient authentication from testimony by a federal agent and a federal informant who engaged in the chat in question); *United States v. Tank*, 200 F.3d 629, 630-31 (9th Cir. 2000) (finding the testimony of another chat room user that he recorded the chats and printed them out, and that the printouts appeared to accurately represent the chats, was sufficient to establish prima facie showing of authenticity); *United States v. Simpson*, 152 F.3d 1243, 1250 (10th Cir. 1998) (holding that a combination of identifying information given by the user in the chat and corroborating evidence found in defendant's home near his computer was sufficient to authenticate the chat log).

<sup>219</sup> *People v. Pierre*, 41 A.D.3d 290, 291 (N.Y. App. Div. 2007) (holding that an instant message was properly authenticated through testimony from defendant's close friend that the screen name associated with the message was the defendant's, that the witness sent a message to that screen name and received a reply, and that the content of the message would have only made sense if it was sent by defendant).

<sup>220</sup> *In re F.P.*, 878 A.2d at 94-95.

### C. Website Content and Archived Web Pages

[65] The judiciary has typically viewed the Internet—arguably the most revolutionary communications development of modern times and giving rise to an unprecedented level of global interaction—in a dubious light due to its public access and the ease by which content can be manipulated, even prompting one court to opine that “any evidence procured off the Internet is adequate for almost nothing.”<sup>221</sup> At first glance, this skepticism seems valid when one looks at examples such as Wikipedia.com, a multi-lingual, free encyclopedia with the tag line “the free encyclopedia that anyone can edit.”<sup>222</sup> However, Wikipedia serves as an excellent microcosm for the lack of uniformity with which the judiciary approaches the Internet in general. At least one state court has specifically called Wikipedia “a malleable source of information [that] is inherently unreliable,”<sup>223</sup> but other courts at the federal level have been skeptics of this position.<sup>224</sup> Wikipedia does not make any guarantee of validity with

---

<sup>221</sup> *St. Clair v. Johnny’s Oyster & Shrimp, Inc.*, 76 F. Supp. 2d 773, 775 (S.D. Tex. 1999); *see supra* note 196.

<sup>222</sup> WIKIPEDIA, [http://en.wikipedia.org/wiki/Main\\_Page](http://en.wikipedia.org/wiki/Main_Page) (last visited Feb. 9, 2012).

<sup>223</sup> *Palisades Collection, L.L.C. v. Graubard*, No. A-1338-07T3, 2009 N.J. Super. Unpub. LEXIS 1025, at \*7 (N.J. Super. Ct. App. Div. Apr. 17, 2009) (reversing the trial court’s decision after finding that the court erred in admitting a print out from Wikipedia and taking judicial notice of content from the Wikipedia page). In support of its holding, the court stated that the “trial court’s acceptance of Wikipedia was also contrary to the principle that judicial notice must be based upon ‘sources whose accuracy cannot be reasonably questioned.’” *Id.*

<sup>224</sup> *E.g. Verkuilen v. MediaBank, LLC*, 646 F.3d 979, 982 (7th Cir. 2011) (citing to Wikipedia for background information on “Media Buying”); *Alfa Corp. v. OAO Alfa Bank*, 475 F. Supp. 2d 357, 361-62, No. 04 Cv 8968 (KMW) (JCF), 2007 U.S. Dist. LEXIS 12771, at \*12-13 (S.D.N.Y. Feb. 21, 2007) (rejecting the argument that expert testimony should be excluded because the expert relied, in part, on a Wikipedia page); *see also Chapman v. San Francisco Newspaper Agency*, No. C01-02305 CRB, 2002 U.S. Dist. LEXIS 18012, at \*5 (N.D. Cal. Sept. 20, 2002) (finding that a computer printout of page from U.S. Postal Service Web site was sufficiently reliable to constitute an admissible public record).

regard to content and disclaims any liability, telling users to post and utilize information at their own risk.<sup>225</sup> In this sense, Wikipedia reflects a concern highlighted by Judge Grimm, that a website may display information not posted by or officially endorsed by the site owner.<sup>226</sup>

[66] As with all electronic evidence, the court, in authenticating a web page, must find enough support that would “warrant a reasonable person in determining that the evidence is what it purports to be,”<sup>227</sup> and can do so through witness testimony, expert opinion, public records evidence supporting F.R.E. 901(7), process or system evidence supporting F.R.E. 901(9), or evidence deemed to be self-authenticating as an official publication under F.R.E. 902(5). In *Lorraine*, Judge Grimm suggests additional factors that counsel should consider when authenticating content from web pages, including length of time that the data was on the site and whether the owner of the data has republished it elsewhere.<sup>228</sup>

[67] The Internet gives counsel involved in cross-border matters a unique ability to gather information otherwise difficult to retrieve. Information about foreign business, individuals, government entities, and other organizations is often readily available from any U.S.-based office with an Internet browser.<sup>229</sup> While some courts have deemed website

---

<sup>225</sup> *Wikipedia: General Disclaimer*, WIKIPEDIA (last visited Feb. 9, 2012), [http://en.wikipedia.org/wiki/Wikipedia:General\\_disclaimer](http://en.wikipedia.org/wiki/Wikipedia:General_disclaimer) (“...all information read here is without any implied warranty of fitness for any purpose or use whatsoever.”).

<sup>226</sup> *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534, 555 (D. Md. 2007).

<sup>227</sup> *United States v. Cameron*, 762 F. Supp. 2d 152, 158, No. 1:09-cr-00024-JAW, 2011 U.S. Dist. LEXIS 4721, at \*11 (D. Me. Jan. 18, 2011) (citing *United States v. Holmquist*, 36 F.3d 154, 167 (1st Cir. 1994)).

<sup>228</sup> *Lorraine*, 241 F.R.D. at 555-56 (internal citations omitted).

<sup>229</sup> *See How to Track Down Anyone Online*, LIFE HACKER, <http://lifelifehacker.com/329033/how-to-track-down-anyone-online> (last visited Feb. 10, 2012) (explaining how Internet users can easily search for people using the various



content authenticated simply because the offered printout contains the website URL and the date of printing,<sup>230</sup> counsel should use caution in relying on this method in cross-border matters. Instead counsel should “present evidence from a witness with personal knowledge of the website . . . stating that the printout accurately reflects the content of the website and the image of the page on the computer at which the printout was made.”<sup>231</sup> The individual performing the actual search and review, if available, may serve as an ideal source of testimony. Counsel can help support authentication by obtaining the testimony of an expert well-versed in the use of hash values,<sup>232</sup> who can speak the language displayed on the target website, collect web postings and other such content, and provide

---

services and search engines available online); LEXISNEXIS INFO PRO, <http://law.lexisnexis.com/infopro/zimmermans/disp.aspx?z=1313> (last visited Feb. 10, 2012) (listing online resources for finding information about companies); *Tax Information for Government Entities*, IRS, <http://www.irs.gov/govt/index.html> (last visited Feb. 10, 2012) (providing links to tax information about federal, state, and local government agencies).

<sup>230</sup> U.S. Equal Emp’t Opportunity Comm’n v. E.I. DuPont De Nemours & Co., No. 03-1605, 2004 U.S. Dist. LEXIS 20753, at \*5 (E.D. La. Oct. 18, 2004).

<sup>231</sup> Toytrackerz, LLC v. Koehler, No. 08-2297-GLR, 2009 U.S. Dist. LEXIS 74484, at \*24 (D. Kan. Aug. 21, 2009); *see also* Nightlight Sys., Inc. v. Nitelites Franchise Sys., Inc., No. 1:04-CV-2112-CAP, 2007 U.S. Dist. LEXIS 95538, at \*16 (N.D. Ga. May 11, 2007) (“In addition to a witness with personal knowledge of the web page at issue, to 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.”).

<sup>232</sup> As a practical strategy to support authentication, counsel should use hash values whenever possible. A hash is defined as “a mathematical algorithm that represents a unique value for a given set of data, similar to a digital fingerprint.” THE SEDONA CONFERENCE, E-DISCOVERY & DIGITAL INFORMATION MANAGEMENT 25 (Sherry B. Harris ed., 3rd ed. 2010), *available at* [http://www.thesedonaconference.org/dltForm?did=TSCGlossary\\_12\\_07.pdf](http://www.thesedonaconference.org/dltForm?did=TSCGlossary_12_07.pdf); *see also* Lorraine, 241 F.R.D. at 547 (“Hash values can be inserted into original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication under Rule 901(b)(4).”).

testimony or prepare an affidavit or declaration describing how and when these efforts were performed.

[68] U.S. Courts have differed in the level of inquiry used to authenticate evidence collected from the Internet Archive.<sup>233</sup> In *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, the U.S. District Court for the Northern District of Illinois held that the defendant adequately authenticated printouts from the Internet Archive by submitting a declaration from a representative of the Internet Archive, who stated that the copies retrieved came from the website as it appeared on the dates in question.<sup>234</sup> The court went on to note that the party opposing the printouts presented no evidence of the Internet Archive's unreliability or that the exhibits themselves were untrustworthy.<sup>235</sup>

[69] In granting a Canadian defendant's motion to strike various printouts from the Wayback Machine,<sup>236</sup> the U.S. District Court for the Eastern District of New York relied, in part, on the absence of the type of personal knowledge present in *Telewizja*. The court noted that the plaintiff lacked personal knowledge about how the web content appeared at the earlier time and did not proffer testimony or sworn statements from

---

<sup>233</sup> See generally Deborah R. Eltgroth, *Best Evidence and the Wayback Machine: Toward a Workable Authentication Standard for Archived Internet Evidence*, 78 FORDHAM L. REV. 182 (2009) (discussing differing judicial opinions and orders that have commented on the admissibility of Internet Archive evidence).

<sup>234</sup> *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, No. 02 C 3293, 2004 WL 2367740, at \*6 (N.D. Ill. Oct. 15, 2004).

<sup>235</sup> *Id.*

<sup>236</sup> The Wayback Machine is a free service offered by the Internet Archive, a non-profit organization formed for the purpose of provided access to "historical collections that exist in digital format." *About the Internet Archive*, INTERNET ARCHIVE, <http://www.archive.org/about/about.php> (last visited Feb. 10, 2012). The Wayback Machine allows users to search for and retrieve archived versions of web sites. *The Wayback Machine*, INTERNET ARCHIVE, [http://www.archive.org/about/faqs.php#The\\_Wayback\\_Machine](http://www.archive.org/about/faqs.php#The_Wayback_Machine) (last visited Feb. 10, 2012).

any employees from the companies hosting the sites from which the pages were printed.<sup>237</sup> Taken together, these two opinions show the importance of having an appropriately qualified person perform the archive collection, consider any translation issues, and provide oral or written testimony as to the archived copies' appearance in comparison to the website as it appeared at the time in question.<sup>238</sup>

#### D. Social Media

[70] Social media and social networking sites have facilitated an unprecedented amount of interconnectivity among citizens from various nations.<sup>239</sup> On Facebook alone, for example, there are more than 800 million active users; of those users, approximately 80% of them live outside the U.S.<sup>240</sup> The micro-blogging site Twitter is very popular all over the world, with some statistics indicating that users across the world

---

<sup>237</sup> *Novak v. Tucows, Inc.*, No. 06CV1909(JFB)(ARL), 2007 WL 922306, at \*5 (E.D.N.Y. Mar. 26, 2007).

<sup>238</sup> As a practical consideration, counsel should also be aware of the technological limitations of collecting archived web site content, including the fact that an archived page may not include all the content as it originally appeared since content may have since been deleted, may require communication with another host for certain content, or may contain broken or re-directed links. When dealing with evidence collected from the Internet Archive, counsel would be wise to consider a forensic or other expert that can provide testimony regarding these issues.

<sup>239</sup> See *About - Twitter*, <http://twitter.com/about#about> (last visited Feb. 4, 2012) (indicating that Twitter is "used by people in nearly every country in the world"); *Facebook Newsroom - Fact Sheet*, FACEBOOK, <http://newsroom.fb.com/content/default.aspx?NewsAreaId=22> (last visited Feb. 4, 2012) (highlighting that "Facebook's mission is to make the world more open and connected.").

<sup>240</sup> *Facebook Newsroom - Fact Sheet*, FACEBOOK, <http://newsroom.fb.com/content/default.aspx?NewsAreaId=22> (last visited Feb. 4, 2012).

send over 1 billion “tweets” each week.<sup>241</sup> Although Facebook and Twitter are the poster children for the explosion in the use of online social networks, millions of users subscribe to a multitude of different social media sites.<sup>242</sup> The international market for social media is extremely robust, with many local sites dominating larger social media outlets, like Facebook, in their respective regions and offering competitive alternatives to U.S.-based social media and networking sites.<sup>243</sup> For example, StudiVZ is the largest social network in Germany;<sup>244</sup> Xing is a competitor to LinkedIn that is popular in Spain, France, and Italy;<sup>245</sup> and in China, where Facebook is blocked by government censors, networks like QZone, RenRen, and Pengyou compete for users.<sup>246</sup>

[71] A few years ago, social media and networking sites would not have registered on the average practitioner’s radar.<sup>247</sup> However, potential

---

<sup>241</sup> Anna Gervai, *Twitter Statistics - Updated stats for 2011*, MARKETING GUM, <http://www.marketinggum.com/twitter-statistics-2011-updated-stats> (last visited Feb. 4, 2012).

<sup>242</sup> See *Facebook Newsroom - Fact Sheet*, FACEBOOK, <http://newsroom.fb.com/content/default.aspx?NewsAreaId=22> (last visited Feb. 4, 2012) (highlighting that, on Facebook alone, more than 50% of users log on to the site every day).

<sup>243</sup> See Sarov Jain, *40 Most Popular Social Networking Sites of the World*, SOCIALMEDIATODAY, <http://socialmediatoday.com/soravjain/195917/40-most-popular-social-networking-sites-world> (last visited Feb. 4, 2012).

<sup>244</sup> *Id.*

<sup>245</sup> *Id.*

<sup>246</sup> Kai Lukoff, *Coming Soon: Tencent’s “International” Social Network*, TECHRICE, <http://techrice.com/2011/01/17/coming-soon-tencents-international-social-network/> (last visited Feb. 4, 2012).

<sup>247</sup> See Evan E. North, Comment, *Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites*, 58 KAN. L. REV. 1279, 1286 (2010).

evidence from such sites must be preserved if relevant,<sup>248</sup> and at least one U.S. Court has now held that counsel's failure to investigate and introduce evidence from such social networking sites could constitute ineffective assistance of counsel.<sup>249</sup> Social media falls within the purview of F.R.C.P. 26 and it, too, must jump through the hoops of admissibility.<sup>250</sup> The unique challenges that practitioners face when admitting electronic information into evidence become very apparent when social media is at issue, particularly where the site is hosted outside the U.S.<sup>251</sup>

[72] Despite social media and networking sites falling under the same traditional admissibility rubric as all electronic documents and data, social media evidence has occasionally engendered heightened judicial skepticism due to concerns about susceptibility of social media and networking sites to fraud.<sup>252</sup> In *Griffin v. State*, the Maryland Court of

---

<sup>248</sup> See *Katiroll Co. v. Kati Roll & Platters, Inc.*, 2011 U.S. Dist. LEXIS 85212, at \*11 (D.N.J. Aug. 3, 2011) (describing how defendant spoliated evidence, albeit unintentionally, in changing his Facebook profile picture while litigation was pending).

<sup>249</sup> See *Cannedy v. Adams*, No. ED CV 08-1230-CJC(E), 2009 WL 3711958, at \*280-29 (C.D. Cal. Nov. 4, 2009). The court deemed counsel rendered ineffective assistance in failing to investigate an Internet posting via an AOL Instant Messenger "Buddy" profile purporting to be the victim's recantation of allegations that the Petitioner had molested her. *Id.*

<sup>250</sup> See Beth C. Boggs & Misty L. Edwards, *Does What Happens on Facebook Stay on Facebook? Discovery, Admissibility, Ethics, and Social Media*, 98 ILL. B.J. 366, 369 (2010).

<sup>251</sup> See David J. Goldstone & Daniel B. Reagan, *Social Networking, Mobile Devices, and the Cloud: The Newest Frontiers of Privacy Law*, 55 B.B.J. 17 (2011) (presenting recent developments in using social media as evidence).

<sup>252</sup> See *United States v. Jackson*, 208 F.3d 633 (7th Cir. 2000) (finding that website postings on a white supremacist's site were ruled unauthenticated where proponent could not show that they were posted by the actual group maintaining the site as opposed to the proponent herself, who was knowledgeable in the use of computers); *Commonwealth v. Williams*, 926 N.E.2d 1162 (Mass. 2010) (ruling MySpace messages unauthenticated because proponent did not offer evidence of others who had access to the page and who could have authored the messages); *People v. Lenihan*, 30 Misc. 3d 289, 911 N.Y.S. 2d

Appeals reversed and remanded the matter of the defendant's conviction based on the State's failure to properly authenticate printouts taken from a MySpace profile that contained threatening statements allegedly made by the Petitioner's girlfriend directed towards the State's witness.<sup>253</sup> The State attempted to authenticate printouts by using the lead investigator's testimony that he knew it was the Petitioner's girlfriend's profile because it contained a photograph of her and the Petitioner, her birth date, references to the Petitioner, and other details.<sup>254</sup> The State never questioned the Petitioner's girlfriend about the subject profile.<sup>255</sup> In holding that the MySpace printouts were not properly authenticated, the *Griffin* Court highlighted the fact that social networking sites can mask the true end-user,<sup>256</sup> and that the factors highlighted by the State did not constitute sufficient distinctive characteristics<sup>257</sup> because of the possibility

---

588 (N.Y. Sup. Ct. 2010) (finding that photographs taken from a MySpace profile could not be authenticated because they could be edited using certain computer software).

<sup>253</sup> *Griffin v. State*, 419 Md. 343, 347-48 (Md. 2011).

<sup>254</sup> *Id.* at 348. The MySpace profile also contained the message: "FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!" *Id.* "Boozy" was the alleged nickname of the defendant and the following comment was argued to be consistent with threats the Petitioner's girlfriend allegedly made to a witness. *Id.*

<sup>255</sup> *Id.*

<sup>256</sup> *Id.* at 353-54 (citing Samantha A. Millier, Note, *The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet*, 97 KY. L.J. 541, 542-43 (2009)) (highlighting Sophos, a Boston-based Internet security company, that created a profile for a toy frog named "Freddie Staur," and nearly 200 Facebook users chose to add the frog as a friend"); *Id.* at 354 (citing *United States v. Drew*, 259 F.R.D. 449 (D.C.D. Cal 2009)) (discussing the case in which a girl committed suicide after being harassed by Lori Drew, the mother of a former friend of her daughter's, using a fictitious MySpace profile).

<sup>257</sup> *Id.* at 357-58. The ability of a proponent of evidence to support authentication using "distinctive characteristics" under Maryland Rule 5-901 mirrors that of the Federal Rules of Evidence 901(b)(4). *Id.* at 355-56.

for fraud.<sup>258</sup> The *Griffin* court went on to suggest methods which counsel could use to properly authenticate printouts from social media sites, including:

- (1) gathering deposition testimony from the alleged owner of the subject profile about whether they created the profile and posted the content at issue,
- (2) investigating any subject hardware to uncover any evidentiary link between such devices and the profile and/or any online content, and
- (3) contact service providers directly to gather user-account and profile information.<sup>259</sup>

[73] The Appellate Court of Connecticut further echoed the *Griffin* Court's concerns regarding the potential for fraud in the world of social media in *State v. Eleck*.<sup>260</sup> The Petitioner in *Eleck* argued that the trial court's refusal to admit a message, allegedly sent by a prosecution witness that he printed from his Facebook account, was an abuse of discretion.<sup>261</sup> Defense counsel attempted to use the Facebook message to contradict testimony from a State's witness that she did not communicate with the Petitioner following a stabbing.<sup>262</sup> In response to the State's objection to

---

<sup>258</sup> *Id.* at 352 (citing Nathan Petrashek, Comment, *The Fourth Amendment and the Brave New World of Online Social Networking*, 93 MARQ. L. REV. 1495, 1499 n.16 (2010)) (highlighting that the "identity of who generated the profile may be confound[ed], because 'a person observing the online profile of a user with whom the observer is unacquainted has no idea whether the profile is legitimate'"). *But see id.* at 367 (Harrell, J., dissenting) ("The technological heebie-jeebies discussed in the Majority Opinion go, in my opinion, however, not to the admissibility of the print-outs under Rule 5-901, but rather to the weight to be given the evidence by the trier of fact.").

<sup>259</sup> *See Griffin*, 419 Md. at 363-64.

<sup>260</sup> *State v. Eleck*, 23 A.3d 818 (Conn. App. Ct. 2011).

<sup>261</sup> *Id.* at 820.

<sup>262</sup> *Id.*

the Facebook printout, the defense attempted to authenticate the document through testimony from the Petitioner: (1) that he printed the message from his personal computer; (2) that he recognized the witness' profile name; (3) that the profile contained photographs identifying the witness as the profile owner; (4) and that the witness had deleted the Petitioner as a friend the day after her testimony in court.<sup>263</sup> The witness admitted that the messages came from her account but denied authorship and testified that her account had been "hacked."<sup>264</sup> Although the court gave the hacking claims little weight, the court stated that such testimony highlights the security concerns with social media and supported the notion that, although the messages came from the witness' Facebook account, this did not conclude that the messages came from the witness herself.<sup>265</sup> The Court upheld the conviction, in part, on the grounds that the Facebook printout had not been properly authenticated.<sup>266</sup>

[74] Despite the anonymity offered by social networking sites that may support concerns about fraud, some courts have held that the ease of altering electronic communications should not be the sole basis for their exclusion as unauthenticated.<sup>267</sup> Social media presents many of the same

---

<sup>263</sup> *Id.* at 820-21.

<sup>264</sup> *Id.* at 820.

<sup>265</sup> *Eleck*, 23 A.3d 818, 822. (citing *Williams*, 926 N.E.2d 1162, 1172 (Mass. 2010)).

<sup>266</sup> *Id.* at 825. The court also rejected the defendant's argument that the Facebook messages could be authenticated using the "reply letter" doctrine, which states that "letter B is authenticated merely by reference to its content and circumstances suggesting it was in reply to earlier letter A and sent by addressee of letter A . . . ." CONN. CODE EVID. § 9-1 (a), commentary (4). The *Eleck* court held that there were no circumstances which tied the reply message to the alleged sender and the fact that a message was sent and a reply received does not, by itself, authenticate the reply. *Eleck*, 23 A.3d at 825.

<sup>267</sup> See *United States v. Safavian*, 435 F. Supp. 2d 36, 41 (D.D.C. 2006); *Simon v. State*, 632 S.E.2d 723, 726 (Ga. 2006); *Commonwealth v. Purdy*, 945 N.E.2d 372, 381 (Mass. 2011); *Commonwealth v. Williams*, 926 N.E.2d 1162, 1172-73 (Mass. 2010).



challenges as paper records. In the same manner that a profile on Facebook may allow a user to hijack another's identity, "[a] signature can be forged, a letter can be typed on another's typewriter; distinct letter head stationary can be copied or stolen."<sup>268</sup> In determining how to verify an author's identity, practitioners need look no further than the current rules.<sup>269</sup>

[75] Though both *Griffin* and *Eleck* highlighted the potential for fraud in their rulings, deeming certain social media evidence inadmissible, the important lesson learned from these opinions is that a proponent of foreign social media evidence should potentially offer more than just a profile name, photograph, and a few statements about a party to lay a proper foundation. The *Eleck* court noted that practitioners attempting to authenticate social media evidence can do so using traditional methods such as obtaining "direct testimony of the purported author or circumstantial evidence of 'distinctive characteristics' in the document that identify the author."<sup>270</sup> In these situations, a party must turn to other foundational support. As can be extrapolated from *Griffin*, counsel could build such support through obtaining hardware or devices where posts may have originated for evidence to support distinctive characteristics, collecting affidavits from service providers describing any unique functionality of a social media site that may provide some indicia of

---

<sup>268</sup> *Eleck*, 23 A.3d at 823 (citing *In re F.P.*, 878 A.2d 91, 95 (Pa. Super. Ct. 2005)).

<sup>269</sup> *Id.*; see also JOHN BROWNING, THE LAWYER'S GUIDE TO SOCIAL NETWORKING: UNDERSTANDING SOCIAL MEDIA'S IMPACT ON THE LAW (Aspatore 2010) at 111 (highlighting the reluctance that courts have shown in crafting rules specifically applicable to the authentication of electronic data).

<sup>270</sup> *Eleck*, 23 A.3d at 823. Examples of distinctive characteristics and corroborating circumstances that support authentication include a message sent from a known sender's e-mail address including factual details known to the sender corroborated by a phone call, an author of chat room messages showing up at an arranged meeting, instant messages authenticated by author's reference to his own name, surrounding circumstances, and threats corroborated by later actions. *Id.* at 824-25.

authenticity, or gathering testimony from other witnesses who may have personal knowledge of a target profile.<sup>271</sup>

[76] When counsel cannot obtain direct testimony, the process of authentication becomes a very fact based inquiry with the proponent gathering evidence of “distinctive characteristics” for the court to evaluate considering “all the circumstances.”<sup>272</sup> When relying on circumstantial evidence to authenticate social media evidence, counsel must do her due diligence to investigate the media and hardware involved, the applications used to generate content and the indicia of reliability in the content itself. At least one U.S. Magistrate Judge, with regard to downloaded documents generally, stated he “would expect the proponent of downloaded document[s] to provide, at a minimum, the web address and path where the document was located, the date and title of the document, the date the document was accessed/downloaded, and a sworn statement that the content of the copy submitted to the court was not altered from the content appearing on the website.”<sup>273</sup> The circumstances surrounding the creation and/or delivery of a piece of social media evidence can go a long way towards meeting the authentication burden. Additional circumstantial evidence to support authorship could include (i) expert testimony regarding the security controls of a particular website<sup>274</sup> as well as the

---

<sup>271</sup> Griffin v. State, 419 Md. 343, 364-65 (Md. 2011).

<sup>272</sup> FED. R. EVID. 901(b)(4).

<sup>273</sup> State ex rel. Leslie v. Ohio Hous. Fin. Agency, 2003 Ohio 6560, 24 (Ohio Ct. App. Dec. 9, 2003). Magistrate Judge Lazarus went on to note that “although the legal requirements for admissibility of downloaded documents may not be well established, a party’s statement that ‘I downloaded these pages from the internet’ is probably not sufficient to authenticate a downloaded document.” *Id.*; see BROWNING, *supra* note 269 at 113 (suggesting that evidence showing that a purported web page author actually wrote the content could take the form of “...an admission by the author, a stipulation entered into by the parties, the testimony of a witness who assisted in or observed the creation of the web page, or content on the web page itself that connects it to the author.”).

<sup>274</sup> Commonwealth v. Williams, 926 N.E.2d 1162, 1172-73 (Mass. 2010).

relative ease or difficulty with which the site could be hacked (particularly critical in the case of non-U.S. or non-E.U. social media, where security controls may be lax),<sup>275</sup> (ii) content of the message itself or any attachments (i.e. photographs of the purported author, descriptions of unique circumstances known only to the sender and the recipient such as nicknames or shared experiences, indications that the message or post shows an awareness of certain facts in issue),<sup>276</sup> and (iii) similar

---

<sup>275</sup> *Commonwealth v. Purdy*, 945 N.E.2d 372, 381-82 (Mass. 2011). The court found adequate “confirming circumstances” to authenticate e-mails of a defendant where the e-mails originated from an account bearing the defendant's name which the defendant acknowledged he used, and the e-mails were found on the hard drive of the computer that the defendant acknowledged he owned, and to which he supplied all necessary passwords. *Id.* The court went on to say that this was sufficient evidence to authenticate the e-mails absent persuasive evidence of fraud, tampering, or “hacking.” *Id.* Although the court further held that “the defendant's uncorroborated testimony that others used his computer regularly and that he did not author the e-mails was relevant to the weight, not the admissibility, of these messages” it nevertheless behooves counsel objecting to the admissibility of certain electronic evidence by arguing fraudulent authorship to present expert testimony on the ability to hack a particular website as well as other circumstances that may support fraud. *Id.*; see *People v. Pierre*, 41 A.D.3d 289, 291 (N.Y. App. Div. 2007) (in holding that an instant message was properly authenticated through circumstantial evidence the court noted that “there was no evidence that anyone had a motive, or opportunity, to impersonate defendant using his screen name.”). The court in *Purdy* went on to find that the defendant's uncorroborated testimony that others used his computer regularly and that he did not author the e-mails was relevant to the weight, not the admissibility, of these messages. *Purdy* at 382. (citing to *Com. v. Mahoney*, 510 N.E.2d 759, 762 (Mass. 1987); *Chartrand v. Registrar of Motor Vehicles*, 187 N.E.2d 135, 137 (Mass. 1963).); The court goes on to state, “Evidence of authorship would not necessarily have been a precondition of admissibility if the prosecution had offered the e-mails, which the defendant acknowledged having read, as evidence of the defendant's knowledge of the nature of the massage business in the salon. If offered for this purpose, the prosecution would not need to show authorship of the e-mails, but would need only to authenticate the communications as accurate reproductions of the messages that were received and sent from the defendant's computer and e-mail address.” (internal citations omitted).

<sup>276</sup> In *Tienda v. State*, 05-09-00553-CR, 2010 WL 5129722 (Tex. App. Dec. 17, 2010), petition for discretionary review granted (May 4, 2011), *aff'd*, PD-0312-11, 2012 WL 385381 (Tex. Crim. App. Feb. 8, 2012). The Texas Court of Appeals, Fifth District, upheld a murder conviction after finding that the trial court did not err in admitting

characteristics between unauthenticated messages or online content and those definitively authored by the party in question.<sup>277</sup>

[77] Counsel can help establish the reliability of certain online communications and content by giving “due attention to the nature of the site at the time relevant to the case.”<sup>278</sup> This is particularly germane to

---

certain evidence taken from MySpace. The appellant argued that there was no proof that the MySpace pages were owned and maintained by him. However, at trial the court introduced evidence that the profile owner identified himself as “Smiley” or “Ron Tienda” from “Dallas” or “D-town” as well as photos of the appellant, references to the murder of the complainant, and comments mentioning the arrest of the appellant, his electronic monitoring device, the fact that multiple parties were involved in the shooting, and individuals that gave statements to the police the night of the murder. The Tienda court noted that “the inherent nature of social networking websites encourages members who choose to use pseudonyms to identify themselves by posting profile pictures or descriptions of their physical appearances, personal backgrounds, and lifestyle. This type of individualization is significant in authenticating a particular profile page as having been created by the person depicted in it.”

<sup>277</sup> United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) (holding that subject e-mails can be authenticated through comparison to other e-mails that have been authenticated).

<sup>278</sup> State v. Altajir, 33 A.3d 193, 197 (Conn. 2012). In this matter, the defendant received a partially suspended prison sentence and probation following her plea of *nolo contendere* after she caused the death of an individual during an auto-accident. She appealed the Connecticut Appellate Court’s affirmation of the trial court’s decision to revoke her probation, arguing that her right to due process was violated when the court admitted undated Facebook photos which influenced the sentencing decision. In its affirmation of the Appellate Court’s decision, the court stated in a footnote that “due to the dynamic nature of Facebook and other such social network sites, these details, as well as basic structural features of the social network, are subject to frequent modification. Care should therefore be taken to assess information relating to social network sites on a case-by-case basis, with due attention to the nature of the site at the time relevant to the case.” In its discussion about where twenty-four of the thirty-six images were located on Facebook (i.e. “posted by other Facebook users to their own profiles”), the Court discussed certain functionality that Facebook allowed at the time of sentencing (i.e. users could “untag” photographs to disassociate them from their personal profile, but a user could not delete images from another profile, the user of which had originally posted the subject photo). It is important to note that the Court stated, “the evidence of reliability

non-U.S. social media sites that may provide different features, layouts, and have developed differently over time. For example, Renren provides an instant messaging service (iRénrénzhuōmiàn or 人人桌面) allegedly more popular than that of Facebook, which U.S. counsel should take into account when collecting evidence to support authentication of Renren pages.<sup>279</sup> The fact that Renren was apparently hacked on April 29, 2011 illustrates how the history of a social media site could impact admitting or objecting to evidence.<sup>280</sup> Counsel could use this knowledge to challenge the authentication of affected profiles on that date or afterwards. The German site StudiVZ offers users the ability to track who most recently visited their profile, a feature that many attorneys familiar with Facebook may not consider.<sup>281</sup> Knowledge of such functionality, as well as language and cultural differences (i.e., social media and non-U.S. text slang) could help counsel uncover additional distinctive characteristics or

---

proffered by the state here is, at best, limited, and certainly would not be sufficient under the rules of evidence at a trial” when, in submitting that the pictures in question were of the defendant while she was on probation, the State represented that the defendant’s hair was darker after she was released from prison, consistent with the Facebook photos, and offered proof of the upload dates of the photos, all of which went unchallenged by the defendant. *See also* A.B. v. State, 885 N.E.2d 1223, 1224 (Ind. 2008). In a juvenile delinquency adjudication proceeding, the Supreme Court of Indiana, in reversing the judgment of the trial court, noted in dicta that “the evidence presented at the fact-finding hearing was extremely sparse, uncertain, and equivocal regarding the operation and use of My Space.com (“MySpace”), which is central to this case.” *Id.* The Court provided information regarding the “use and operation of MySpace” to “facilitate understanding of the facts and application of relevant legal principles. *Id.*

<sup>279</sup> *Facebook*, FACEBOOK, <https://www.facebook.com/pages/Xiaonei/106216539417805> (last visited Feb. 4, 2012). (Ironically posted using a Facebook page).

<sup>280</sup> *Wikipedia*, WIKIPEDIA, [http://en.wikipedia.org/wiki/Renren#Privacy\\_Leakage\\_April\\_2011](http://en.wikipedia.org/wiki/Renren#Privacy_Leakage_April_2011). Subsequent to the attack, all Chinese media coverage of the event were removed. Screenshots of some of the sources survive, with text in the original Chinese. *See* <http://pastebin.com/qKrbvGFF>; <http://page.renren.com/699131345/note/724338594>; <http://i.imgur.com/NCUi5.png>; <http://i.imgur.com/4r3FN.png>.

<sup>281</sup> Facebook does not offer this functionality.

circumstances necessary to authenticate evidence collected from a foreign social media or networking site.<sup>282</sup>

### E. Internet Tracking Information

[78] One of the unique benefits that law enforcement and legal practitioners have in the Information Age is the ability to track online activity through browser caches<sup>283</sup> and “cookies.”<sup>284</sup> Internet browsing history has played a significant role in a number of recent cases.<sup>285</sup>

---

<sup>282</sup> For example, certain sites are not available in English (i.e. RenRen & Qzone); thus, their review will require the use of an experienced translator.

<sup>283</sup> “Caching” is a generic term meaning “to store.” In the context of online activity, “caching” refers to the temporary storage of information for later use. Browser caches are locations where data about websites that a user has previously visited is stored. Instead of a request being serviced by an online web server, information is retrieved from the browser cache allowing for information to be retrieved more quickly. *See* Nat’l Cable & Telecomms. Ass’n v. Brand X Internet Servs., 545 U.S. 967, 999-1000 (2005) (“Cacheing [sic] obviates the need for the end user to download new information from third-party Web sites each time the consumer attempts to access them, thereby increasing the speed of information retrieval.”). A browser cache is also commonly referred to as the “Temporary Internet Files Folder.”

<sup>284</sup> “Cookies” are messages given to web browsers by web servers that are stored locally in a text file format. Cookies are used to track users’ browsing activity. *See* Blumofe v. Pharmatrak, Inc. (In re Pharmatrak, Inc. Privacy Litig.), 329 F.3d 9, 14 (1st Cir. Mass. 2003) (citing M. Enzer, *Glossary of Internet Terms*, MATISEE.NET, <http://www.matissee.net/files/glossary> (last visited Feb, 4, 2012)).

<sup>285</sup> In the quadruple-murder trial of a Montreal couple and their eldest son (dubbed by many in the press as the “Shafia Family Murder”), a police officer testified on October 27, 2011 that searches for “documentaries on murders” and “where to commit a murder” were found on the laptop used by one of the defendants. *Timeline: the Shafia family murder trial*, GLOBAL NEWS AND THE GAZETTE (Feb. 9, 2012, 8:23 AM), <http://www.globalnews.ca/timeline+shafia+murder+trial/6442509727/story.html>. Similarly, in the Casey Anthony murder trial, which caused a media frenzy in the U.S. in 2011, the prosecution offered testimony from technical experts regarding the internet browsing history of the defendant including online searches using terms such as “chloroform,” “neck breaking,” “inhalation,” “head injury” and “making weapons out of household products.” Jones, Keith J., *Casey Anthony Murder Trial, The Computer*

Although browser caches and cookies are technologically distinct, from an evidentiary standpoint, they provide many of the same benefits and pose similar challenges. While there is some support for the notion that certain categories of data, including temporary Internet files, search history, caches files, and cookies are “generally not discoverable in most cases,”<sup>286</sup> it is important to note that the duty to preserve such data may still apply under certain circumstances,<sup>287</sup> especially where the proponent of such information can show “good cause.”<sup>288</sup> Such evidence can also be

---

*Evidence Part #2*, JDA BLOG (June 14, 2011, 12:00), <http://www.jonesdykstra.com/blog/201-caseyanthony-part2>.

<sup>286</sup> SEVENTH CIRCUIT ELEC. DISCOVERY COMM., SEVENTH CIRCUIT ELECTRONIC DISCOVERY PILOT PROGRAM 14 (Oct. 1, 2009). (“The following categories of ESI generally are not discoverable in most cases, and if any party intends to request the preservation or production of these categories, then that intention should be discussed at the meet and confer or as soon thereafter as practicable... (2) random access memory (RAM) or other ephemeral data; (3) on-line access data such as temporary internet files, history, cache, cookies, etc.”).

<sup>287</sup> *Victory Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 524 (D. Md. 2010) (holding that “[t]he general duty to preserve may also include deleted data, data in slack spaces, backup tapes, legacy systems, and metadata.”) (quoting Paul W. Grimm et. al., *Proportionality in the Post-Hoc Analysis of Pre-Litigation Preservation Decisions*, 37 U. BALT. L. REV. 381, 410 (2008)); see *Columbia Pictures v. Bunnell*, No. 2:06-cv-01093 FMC-JCx, 2007 U.S. Dist. LEXIS 96360, at \*20-21 (C.D. Cal. Dec. 13, 2007). In a copyright infringement case filed by several motion pictures studios against the operators of a website with servers located in the Netherlands, the court found that data stored in defendants’ website’s random access memory (RAM) was extremely relevant and ordered that it be preserved. *Id.*

<sup>288</sup> *Tener v. Cremer*, 89 A.D.3d 75, 80 (N.Y. App. Div. 2011). In this defamation action, the Supreme Court of New York, Appellate Division, First Department reversed an order of the New York Supreme Court denying appellant’s civil contempt motion against a non-party for failing to turn over the identities of all persons who accessed the internet at a specific time based on the grounds of technological impracticality. *Id.* The court held that the appellant had shown “good cause” for requesting the cache file potentially present in unallocated space on the target hard drive since the “only chance to confirm the identity of the person who allegedly defamed her may lie with [the non-party in possession of the data].” *Id.* The court remanded the matter to the trial court for a hearing to determine whether the data is in fact “inaccessible.” *Id.*

discoverable by providing foundational support for other admissible evidence (i.e., internet cookies may be used to show a nexus between a user and a specific social media site). As with social media evidence, there is a concern that such Internet tracking information can be hacked, manipulated, or, absent additional information, serve as a dubious indicator of the identity of the actual user.<sup>289</sup> This “modification” argument, although a very common one, usually does not, absent more specific allegations, provide a basis upon which a court will deem cookies and other such data inadmissible.<sup>290</sup> In affirming the conviction of a defendant on various sexual abuse crimes, the Court of Appeals in Utah held that a list of Internet cookies that contained site names suggesting pornographic content was properly authenticated where the party who created the list gave testimony about the operation and regular use of her computer, demonstrated a sophisticated knowledge of the interaction between her computer and the Internet, and testified that the defendant

---

<sup>289</sup> See *United States v. Safavian*, 435 F. Supp. 2d 36, 41 (D.D.C. 2006). The court noted that the possibility of alteration is not limited to e-mail and:

can be true of any piece of documentary evidence, such as a letter, a contract or an invoice. . . . The *possibility* of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course, any more than it can be the rationale for excluding paper documents . . . . The defendant is free to raise this issue with the jury and put on evidence that e-mails are capable of being altered before they are passed on.

*Id.*; see also *United States v. Whitaker*, 127 F.3d 595, 602 (7th Cir. 1997) (affirming admission of computer records where allegation of tampering was “...almost wild-eyed speculation . . . [without] evidence to support such a scenario.”); *United States v. Glasser*, 773 F.2d 1553, 1559 (11th Cir. 1985) (“The existence of an air-tight security system [to prevent tampering] is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records.”).

<sup>290</sup> *Safavian*, 435 F. Supp. 2d at 41.



would have had access to her computer, that she personally viewed many of the subject sites, and that she created the list of cookies herself.<sup>291</sup>

[79] The proponent of such evidence collected from foreign sources faces the same dilemma as with social media or other ESI evidence collected domestically and can take further guidance from *Griffin*:

- (1) Is there a credible source of testimony to authenticate such evidence from the host country?
- (2) Can one acquire the devices in question to further investigate such Internet tracking information?
- (3) Can one gather the information necessary to authenticate such browsing history and other such data (i.e. subpoenaing Google to obtain the IP addresses and user names to ultimately link certain online activity to certain people or devices or subpoenaing Internet Service Providers to link IP address to specific ISP customers, where such subpoenas are permissible pursuant to applicable law)?<sup>292</sup>
- (4) What do Internet browsing history and other cookie data actually prove?<sup>293</sup>

[80] Just as the *Griffin* and *Eleck* courts highlighted the fact that although a social media printout or display will readily show only that *someone* posted a particular piece of content and not necessarily *who* posted it, internet tracking information will show only that someone visited a site, but the who can only be uncovered through the same type of

---

<sup>291</sup> State v. Burke 256 P.3d 1102, 1125 (Utah Ct. App. 2011).

<sup>292</sup> In a defamation lawsuit filed in California, counsel for a Turkish developer subpoenaed Google for user information and IP address log-in history. *Kinay v. TCI Journal*, CITIZEN MEDIA LAW JOURNAL (Sept. 9, 2009), <http://www.citmedialanw.org/threats/kinay-v-tci-journal> (case pending in California state court).

<sup>293</sup> See *supra* note 284.

analysis of distinctive characteristics and corroborating circumstances as other ESI.<sup>294</sup>

## F. An International Case Study

[81] Where testimony from foreign sources is unavailable, distinctive characteristics and other corroborating circumstantial evidence must authenticate foreign ESI. The following case study illuminates these issues. In a 2009 criminal conspiracy case, *United States v. Albert Gonzalez*, three men were indicted on various charges involving the online theft of credit card numbers.<sup>295</sup> The government submitted two pieces of evidence: a computer server where the defendant allegedly stored hacking programs and stolen credit card numbers and files from a laptop seized during the arrest of a co-defendant.<sup>296</sup> The evidence was collected with the help of the state police of Latvia and Turkey.<sup>297</sup> The government submitted Mutual Legal Assistance Treaty requests for the foreign nationals who assisted in the acquisition of the evidence to provide testimony but uncertainty existed over the ability to secure such evidence.<sup>298</sup> Regardless, the government submitted that such testimony

---

<sup>294</sup> See generally *Griffin v. State*, 995 A.2d 791 (Md. 2010), *cert. granted*, 415 Md. 607 (Md. 2010), *rev'd*, 419 Md. 343 (Md. 2011).

<sup>295</sup> Government's Motion *in limine* at 2, *United States v. Albert Gonzalez*, Crim. Docket No. 2:08-cr-00160-SJF-AKT, Aug. 17, 2009, ECF No. 61-1, *available at* [http://www.wired.com/images\\_blogs/threatlevel/2009/08/maksik\\_computer\\_motion.pdf](http://www.wired.com/images_blogs/threatlevel/2009/08/maksik_computer_motion.pdf).

<sup>296</sup> *Id.* (The Government generated forensic images for the both the Latvian server and the seized laptop for evidentiary purposes.).

<sup>297</sup> *Id.* at 3-7; see also Kim Zetter, *In Gonzalez Hacking Case, a High-Stakes Fight Over a Ukrainian's Laptop*, WIRED (Aug. 20, 2009, 4:21 PM), <http://www.wired.com/threatlevel/2009/08/gonzalez-evidence/>.

<sup>298</sup> See Government's Motion *in limine* at 4-7, *Gonzalez*, Crim. Docket No. 2:08-cr-00160-SJF-AKT, Aug. 17, 2009, ECF No. 61-1, *available at* [http://www.wired.com/images\\_blogs/threatlevel/2009/08/maksik\\_computer\\_motion.pdf](http://www.wired.com/images_blogs/threatlevel/2009/08/maksik_computer_motion.pdf). The government expressed this concern in a footnote to its letter brief: "The government . . . has no power to compel foreign citizens to testify in United States court proceedings. It is uncertain at

was not required since a foundation could be properly laid through circumstantial evidence.<sup>299</sup>

[82] In arguing that the “distinctive characteristics” of the server, in combination with various circumstances, provided sufficient evidence for its authentication, the Government submitted that (i) the computer server and the forensic image taken of the server were “substantially identical,”<sup>300</sup> (ii) the IP address provided by a cooperating witness was hosted on the target server, (iii) none of the subject files were altered on the server following the arrest of the cooperating witness and the defendant, and (iv) the examiners were able to open files on the server using the password provided by the cooperating witness.<sup>301</sup>

[83] The Government also submitted a forensic image of the files of the laptop seized prior to the co-defendant’s arrest.<sup>302</sup> The image emerged after the co-defendant was in custody, and, furthermore, counsel showed that: (i) no files were altered between the date of arrest and the date of image creation, (ii) the image displayed the same “Mars” logon screen, which was photographed on the date of arrest, (iii) the image contained

---

this time whether these individuals will agree to travel to the United States for trial in this case, or even to be deposed here or in their home nations.” *Id.* at 1-2, n.1.

<sup>299</sup> *Id.* at 9-11.

<sup>300</sup> *Id.* at 4. During an arrest of an accomplice of the defendant, United States Secret Service tracked an IP address used to mask criminal activities to a server in Riga, Latvia. The government originally acquired a forensic image of the server, but then obtained possession of the server itself to compare to the image. The comparison evidenced that the server had not been altered after the defendant had been arrested. All of the files on the server the government intended to use at trial were identical. The only difference was that the image contained some text strings consistent with a signature or metadata created by the device manufacturer or disk controller. *Id.*

<sup>301</sup> *Id.* at 5.

<sup>302</sup> *Id.* at 4.

chat logs identical to those found on the defendants' computer (seized several months later) as well as chat logs identical to those sent from an undercover agent's computer to co-defendant, and (iv) the image had several factors in common with an image made of the same laptop during a prior search including identical chat logs, logon screen, and file containers with the same password.<sup>303</sup>

[84] Although many circumstances make a criminal matter like *Gonzales* an extreme example of authentication through distinctive characteristics, the case provides counsel with some comfort that circumstantial evidence can authenticate foreign ESI even if foreign witnesses are absent or uncooperative. In *Gonzalez*, the government relied heavily on evidence collected through forensic imaging and analysis of various devices.<sup>304</sup> Although counsel in civil cases may not have the benefit of such devices as a Mutual Legal Assistance Treaty, and the European Union Privacy Directives, member state implementing laws, or national blocking statutes may prevent counsel from acquiring certain information, this case highlights the technological means by which foreign ESI can be collected, investigated, and distinguished for authentication purposes.<sup>305</sup>

## VI. CONCLUSION

[85] The expenditure of thousands of person-hours and, often, hundreds of thousands of dollars, to collect evidence from around the globe can be a very costly Sisyphean effort, if counsel does not have the knowledge and skills to present the evidence before the finder of fact. The Rules of Evidence apply to electronic information with the same force as they do to

---

<sup>303</sup> Government's Motion *in limine* at 6-7, *Gonzalez*, Crim. Docket No. 2:08-cr-00160-SJF-AKT, Aug. 17, 2009, ECF No. 61-1, *available at* [http://www.wired.com/images\\_blogs/threatlevel/2009/08/maksik\\_computer\\_motion.pdf](http://www.wired.com/images_blogs/threatlevel/2009/08/maksik_computer_motion.pdf).

<sup>304</sup> *See generally id.*

<sup>305</sup> *See generally id.*

paper documents.<sup>306</sup> The differences are in the application of those rules to electronic evidence, which many lawyers and judges find to be somewhat daunting.<sup>307</sup> This problem does not have to exist, though. To paraphrase Paul Simon, taking the admissibility of non-electronic evidence logically by anticipating the need for fulfillment of the requisites of the foundation for such evidence, and having documents and witnesses ready to lay the foundation for the evidence or to challenge it, will produce a result that can justify all the time and money spent in obtaining the evidence.<sup>308</sup>

---

<sup>306</sup> See FED. R. EVID. 403; FED R. EVID 901. See generally *supra* Section V.

<sup>307</sup> See *supra* Section V.

<sup>308</sup> See SIMON, *supra* note 35.