

# Authenticating Digital Evidence from the Cloud

Major Scott A. McDonald\*

*“I’m saying give it to somebody don’t know any better. It’s a fugazy.”<sup>1</sup>*

## I. Introduction

Digital media and communications are a significant part of American life. A 2008 study found that “[s]ome 69% of online Americans use webmail services, store data online, or use software programs such as word processing applications whose functionality is located on the web.”<sup>2</sup> With the surge in popularity of social networking and online storage sites such as Facebook, LinkedIn, Twitter, and Dropbox, that number is substantially larger for 2013.<sup>3</sup>

Perhaps unknowingly, these users all participate in what is now more commonly referred to as “cloud computing” or “the cloud.” Logging in to Gmail, uploading videos to YouTube, or posting a status update to Twitter or Facebook means plugging in to the cloud—“an emerging architecture by which data and applications reside in cyberspace, allowing users to access them through any web-connected device.”<sup>4</sup> In fact, most experts believe that by 2020 virtually

all digital work will be conducted in the cloud.<sup>5</sup>

Cloud architecture, however, has been growing far beyond conventional personal use. For example, Amazon recently launched a free public storage option that gives users the ability to store five gigabytes of media (music, photos, videos, documents) and to access that media from any internet-capable device.<sup>6</sup> With this application, Amazon gives users free storage for up to 2,000 photos.<sup>7</sup>

Equally popular services such as Google Drive and Dropbox provide a folder synchronization option. With these services, though the user’s data may be stored on the cloud, the interface makes it appear as though the digital information is locally stored.<sup>8</sup> These services also offer passive backup of digital data to the cloud, which means users need not take any affirmative action to effect the cloud-based storage of their information.<sup>9</sup>

With this significant increase in the use of cloud architecture, and the attendant increase of available digital evidence, law enforcement has taken notice. Google reports that in 2012 alone, it received 42,327 requests for data from government agencies<sup>10</sup> in relation to criminal matters.<sup>11</sup> Though courts have grown more comfortable and familiar with the introduction of digital evidence in the form of e-mail and web pages,<sup>12</sup> very few reported decisions address the use of digital evidence obtained from the cloud.<sup>13</sup>

---

\* Judge Advocate, U.S. Army. Presently assigned as Special Victim Prosecutor, Europe; J.D. 2006; University of Nevada, Las Vegas, William S. Boyd School of Law; M.A., 2002; Webster University, St. Louis, Missouri; B.A., 1998; California State University, Fullerton. Previous assignments include Chief, Military Justice, Fort Carson, Colorado, 2011–2013; Brigade Judge Advocate, Camp Cropper, Iraq, 2009–2010; Trial Counsel, Fort Leonard Wood, Missouri, 2008–2009; Chief, Client Services, Fort Leonard Wood, Missouri, 2007–2008; Administrative Law Attorney, Fort Leonard Wood, Missouri, 2006–2007; Executive Officer, Hanau, Germany, 2001–2002; Platoon Leader, Hanau, Germany, 2000–2001; Battle Captain, Camp Bondsteel Kosovo, 1999–2000. Member of the bars of the Supreme Court of the United States and the State of Washington. This article was submitted in partial completion of the Master of Laws requirements of the University of Virginia School of Law.

<sup>1</sup> DONNIE BRASCO (1997). Although there is no solid reference for the word “fugazy,” in this scene, Donnie Brasco uses the term “fugazy” to describe a jewel, which appears to be a diamond, as a “fake.”

<sup>2</sup> PEW RESEARCH CTR., USE OF CLOUD COMPUTING APPLICATIONS AND SERVICES 1 (2008) [hereinafter PEW SURVEY], available at [http://www.pewinternet.org/~media/Files/Reports/2008/PIP\\_Cloud.Memo.pdf](http://www.pewinternet.org/~media/Files/Reports/2008/PIP_Cloud.Memo.pdf).

<sup>3</sup> See Cindy Pham, *E-Discovery in the Cloud Era: What’s a Litigant to Do?*, 5 HASTINGS SCI. & TECH. L.J. 139, 139 (2013).

In 2008, the total cloud service revenue was \$46.4 billion, rising to \$58.6 billion by 2009. This amount further increased to \$68.3 billion in 2010. By 2014, the market is expected to be worth \$148.8 billion and it is predicted that people will process more than 50 percent of all computing workloads through cloud computing. Furthermore, it is estimated that, by 2015, cloud usage will grow twelve-fold to represent one-third of Internet traffic.

*Id.* (citations omitted).

<sup>4</sup> PEW SURVEY, *supra* note 2, at 1.

---

<sup>5</sup> See PEW RESEARCH CTR., THE FUTURE OF CLOUD COMPUTING 2 (2010), available at [http://pewinternet.org/~media/Files/Reports/2010/PIP\\_Future\\_of\\_the\\_Internet\\_cloud\\_computing.pdf](http://pewinternet.org/~media/Files/Reports/2010/PIP_Future_of_the_Internet_cloud_computing.pdf).

<sup>6</sup> AMAZON, [https://www.amazon.com/cloudrive/learnmore/ref=sa\\_menu\\_acd\\_lrn2](https://www.amazon.com/cloudrive/learnmore/ref=sa_menu_acd_lrn2) (last visited May 28, 2014).

<sup>7</sup> *Id.*

<sup>8</sup> For example, Dropbox users can install an application that creates a folder on the user’s desktop, or mobile device, that appears to be located locally, but in actuality is remotely stored. “Dropbox will watch your Dropbox folder and automatically make sure your files are the same no matter where you access them.” DROPBOX, <https://www.dropbox.com/help/4/en> (last visited May 2, 2014).

<sup>9</sup> *Id.*

<sup>10</sup> *User Data Requests*, GOOGLE, <http://www.google.com/transparencyreport/userdatarequests/> (last visited May 28, 2014).

<sup>11</sup> *FAQ*, GOOGLE, <http://www.google.com/transparencyreport/userdatarequests/faq/> (last visited May 28, 2014).

<sup>12</sup> See generally *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007).

<sup>13</sup> As of 2 May 2014, a search of Lexis’s “all federal and state” database for “cloud computing” reveals fifty-seven decisions discussing the matter, fifty-three of which were issued within the last five years.

This article describes the nature of cloud architecture, criminal aspects of cloud storage, and then addresses issues of authenticating evidence obtained from the cloud.<sup>14</sup> Drawing parallels from the approved methods of authentication for e-mail and webpages, this article argues that despite some unique issues associated with data obtained from the cloud, authentication of cloud data should not present an insurmountable obstacle for counsel.

## II. Background

Though the cloud has been available for some time now, an understanding of what the cloud actually is will assist counsel in gathering the information needed to authenticate digital evidence obtained from the cloud.<sup>15</sup> This is particularly true when developments in cloud technology continue to change the definition of cloud architecture.<sup>16</sup> With that foundation in place, a brief examination of the traditional means of authenticating digital evidence will assist counsel in applying the Military Rules of Evidence (MRE) 901<sup>17</sup> to authenticate evidence obtained from the cloud.<sup>18</sup> Much of this article actually references Federal Rules of Evidence (FRE) 901 because the rule is substantially similar to MRE 901, and the body of caselaw regarding authentication of evidence is far better developed for FRE 901.<sup>19</sup>

### A. What Is the Cloud?

The cloud is not a conventional home computer, laptop, or external storage device. Rather, the cloud is comprised of public or private remote servers. Data is stored on these servers and accessed by users through some form of internet facilitated interface.<sup>20</sup> For example, a Missouri resident may access their Gmail via their internet device (computer, laptop, iPad, tablet device, or smart phone), and read their messages, which may be stored on a server in either

California or Virginia. Similarly, an Amazon cloud user may upload their video files from their home in New York, but their data would transfer to a server farm in Northern Virginia.<sup>21</sup> To the end user, the transfer of and access to this data is seamless.

Cloud computing, however, entails additional characteristics that can complicate authentication of the data for evidentiary purposes.<sup>22</sup> First, data may not remain on the original server. The cloud service provider may instead farm the data out to another server run by another service provider. For example, Amazon requires more server capacity during peak shopping season and may farm out personal cloud data storage to another provider like Google.<sup>23</sup> When Amazon does this, a user's data may be farmed out in its entirety, or only a portion of the data may be transferred.<sup>24</sup>

As noted before, for the end user, the process is seamless. However, while the former is akin to transferring an entire file folder from one office to another, the latter is more like transferring pages six, eight, and twenty of a critical report to another office, while leaving the remaining pages in the original office. This was not always the issue before—generally, digital files existed in their entirety on one medium. An entire digital photo file existed on a disc, thumb drive, or hard drive. Now, a portion of that file may exist on one server, and the remainder may exist on another server located thousands of miles away.

The second complicating characteristic of cloud computing is redundancy. Because servers always carry the risk of catastrophic failure, “[a] cloud computing system must make a copy of all its clients’ information and store it on other devices.”<sup>25</sup> Thus, a user of Dropbox may upload one copy of a photo they took on vacation and never realize that the photo has been duplicated and potentially stored on any one of many servers located throughout the world. As a result, cloud content gathered pursuant to a law enforcement investigation may not be the original content stored by the user.<sup>26</sup>

---

<sup>14</sup> This article limits its focus to an examination of the means and methods of authenticating digital evidence under Military Rules of Evidence (MRE) 901 (Requirement of authentication or identification). Recognizing that some digital evidence may be self-authenticating under MRE 902 (Self-Authentication), such a discussion is beyond the scope of this paper.

<sup>15</sup> See *infra* Part II.A.

<sup>16</sup> See *infra* Part II.B.

<sup>17</sup> Requirement of authentication or identification.

<sup>18</sup> See *infra* Part II.C.

<sup>19</sup> See also *United States v. Blanchard*, 48 M.J. 306, 309 (C.A.A.F. 1998) (noting MRE 901 is the same as FRE 901, and going on to cite federal cases in support of the decision). “It suffices to say that these same principles are applicable at courts-martial and, accordingly, federal court of appeals decisions applying these principles would be most helpful.” *Id.* at 309–10.

<sup>20</sup> “[T]he data or software applications are not stored on the user’s computer, but rather are accessed through the web from any device at any location a person can get web access.” PEW SURVEY, *supra* note 2, at 4.

---

<sup>21</sup> Amazon maintains nine regional server farms worldwide for its cloud service. AMAZON, <http://aws.amazon.com/ec2/> (last visited May 28, 2014).

<sup>22</sup> See *infra* Part III.C.

<sup>23</sup> See David Navetta, *Legal Implications of Cloud Computing—Part One (the Basics and Framing the Issues)*, INFORMATION LAW GROUP (Aug. 18, 2009), <http://www.infolawgroup.com/2009/08/tags/security/legal-implications-of-cloud-computing-part-one-the-basics-and-framing-the-issues/>.

<sup>24</sup> *Id.*

<sup>25</sup> Jonathan Strickland, *How Cloud Computing Works*, HOW STUFF WORKS, <http://computer.howstuffworks.com/cloud-computing1.htm> (last visited May 28, 2014).

<sup>26</sup> Though this necessarily implicates MRE 1001–08, the “best evidence rule,” which is beyond the scope of this article, it remains an important consideration for counsel attempting to clear the hurdle of authentication. The fact that digital content is constantly replicated may not, in the end, be very problematic. See, e.g., *State v. Bellar*, 217 P.3d 1094, 1110 (Or. Ct.

These characteristics distinguish digital evidence obtained from the cloud from traditional forms of digital evidence, such as e-mail and webpages. However, at one time, courts were forced to analogize webpages and e-mail to similar non-digital evidence to facilitate authentication and admission.<sup>27</sup> Thus, while it is important to recognize the differences between cloud-based evidence and traditional digital evidence, cloud-based evidence shares similar characteristics.

## B. New Developments in Cloud Computing

Technology is ever evolving. Likewise, the nature of cloud computing continues to evolve. Notably, a new technique for cloud computing was recently developed wherein users do not store data on remote server farms, but instead store data on the devices of other users.<sup>28</sup> The new system, dubbed Seattle, “connects devices directly to one another in a decentralized network, relaying information more quickly than it could through a single, often distant exchange point.”<sup>29</sup> Currently, the developers of Seattle are working to expand the system in order to enable similar sharing and storage across portable devices, such as smartphones.<sup>30</sup>

Thus, as cloud computing architecture evolves and continues to grow more amorphous, the attendant challenge of authenticating that data will also evolve.<sup>31</sup> This is because, unlike the previous analogies of file folders being transferred between offices,<sup>32</sup> the Seattle system is akin to one hundred different people having a single page of a critical report, all of whom have to come together to view the report in its entirety.

---

App. 2009) (Sercombe, J., dissenting) (quoting Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 564 (2005)) (“From a technical perspective, it usually makes no sense to speak of having an ‘original’ set of data. Given this, it would be troublesome and artificial to treat copies as different from originals.”).

<sup>27</sup> See, e.g., *Manuel v. State*, 357 S.W.3d 66, 75 (Tex. App. 2011) (noting that the “reply-letter doctrine” applies to authentication of e-mail). “Another traditional method of authentication permitted by Rule 901 is the ‘reply-letter doctrine.’ Under this doctrine, a letter received in the due course of mail purportedly in answer to another letter is *prima facie* genuine and admissible without further proof of authenticity.” *Id.* (citations omitted).

<sup>28</sup> See *How Justin Cappos Created a New Way to Cloud Compute*, POPULAR SCI., <http://www.popsci.com/science/article/2013-09/justin-cappos> (last visited May 28, 2014).

<sup>29</sup> *Id.*

<sup>30</sup> *Id.*

<sup>31</sup> See PROSPECTIVE ANALYSIS ON TRENDS IN CYBERCRIME FROM 2011 TO 2020, at 21 (2011), available at <http://www.mcafee.com/us/resources/white-papers/wp-trends-in-cybercrime-2011-2020.pdf>. “There is also an opinion that cloud computing architectures blur the boundaries between what is physical and what is digital, to the point where no one knows where the data is stored, nor who manages and uses it, etc.” *Id.*

<sup>32</sup> See *supra* Part II.A.

## C. Traditional Means of Authentication

The requirements for authentication are set out in Military Rules of Evidence (MRE) 901. The rule provides that prior to a particular piece of evidence being admissible, the court must be satisfied that “the matter in question is what its proponent claims.”<sup>33</sup> This is not to say that the proponent must “prove beyond all doubt that the evidence is authentic and has not been altered.”<sup>34</sup> Rather, the proponent must meet only the low threshold established in the rule, with issues of reliability going instead to weight.<sup>35</sup>

The authentication requirement may be satisfied by testimony from a witness with knowledge of the matter, comparison with previously authenticated items, establishment of distinctive characteristics, or a description of the process or system that created the matter in question.<sup>36</sup> The proponent of an exhibit may also authenticate documents with an attestation certificate or testimony from the custodian of records, though this may only be mandatory if required by law.<sup>37</sup> Some evidence, however, is self-authenticating and does not require the foregoing.<sup>38</sup>

If the trial court determines that the proponent of the evidence has satisfied the authenticity requirement, the court should admit the evidence if it comports with any additional relevant rules of evidence.<sup>39</sup> At that point, as noted above, the opponent’s objection to authentication and any reliability issues go to the weight of the evidence rather than admissibility.<sup>40</sup>

### 1. Testimony of a Witness with Knowledge

One of the most basic methods of authentication is proffering testimony from a witness with knowledge of the evidence who can make out a *prima facie* case that the evidence is what it purports to be.<sup>41</sup> For example, when

---

<sup>33</sup> MANUAL FOR COURTS-MARTIAL, UNITED STATES, MIL. R. EVID. 901(a) (2012) [hereinafter MCM].

<sup>34</sup> U.S. ATT’Y MANUAL, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 197 (2009) [hereinafter U.S. ATTY MANUAL] (citation omitted).

<sup>35</sup> See *id.* at 197–98.

<sup>36</sup> MCM, *supra* note 33, MIL. R. EVID. 901(b). “Rule 901(b) is a non-exhaustive list of illustrative examples of authentication techniques.” *Id.* MIL. R. EVID. 901(b) analysis, at A22-60.

<sup>37</sup> *Id.* MIL. R. EVID. 903.

<sup>38</sup> *Id.* MIL. R. EVID. 902.

<sup>39</sup> WEINSTEIN’S EVIDENCE MANUAL § 8.01[1] (citing *United States v. Patterson*, 277 F.3d 713 (4th Cir. 2002)).

<sup>40</sup> *Id.* (citing *Orr v. Bank of Am., NT & SA*, 285 F.3d 764, 773 n.6 (9th Cir. 2002)).

<sup>41</sup> MCM, *supra* note 33, MIL. R. EVID. 901(b)(1); FED. R. EVID. 901(b)(1); see also *United States v. Lanzon*, 639 F.3d 1293, 1301 (11th Cir. 2011) (citing *United States v. Caldwell*, 776 F.2d 989, 1002 (11th Cir. 1985)).

Keith Lanzon attempted to solicit an undercover officer for a sexual encounter with what he believed to be an underage girl, the government charged Lanzon with “attempting to persuade, entice, or coerce a minor to engage in sexual activity.”<sup>42</sup> At trial, the government offered into evidence a transcript of the American Online (AOL) chat sessions between Lanzon and the undercover officer.<sup>43</sup> The government also introduced the testimony of the officer who testified about his role in the online conversation and about his method of preparing the transcript, including copying, pasting, and comparing the online chat with the Word document he created to ensure accuracy.<sup>44</sup> According to the court, the officer’s testimony, as a witness with knowledge, was sufficient to demonstrate that the transcript of the online conversation was what it purported to be and was therefore sufficiently authenticated.<sup>45</sup>

## 2. Comparison by an Expert Witness or the Trier of Fact

A proponent may also authenticate evidence by comparing it with a previously authenticated piece of evidence.<sup>46</sup> For example, in *United States v. Safavian*, the government introduced e-mail evidence that had been authenticated under FRE 901(b)(4), the “distinctive characteristics” provision discussed *infra*.<sup>47</sup> The government also sought to introduce a number of additional e-mails that lacked similarly distinctive characteristics.<sup>48</sup> Those e-mails only contained the e-mail address “MerrittDC@aol.com.”<sup>49</sup> However, the previously authenticated e-mails included e-mails from “MerrittDC@aol.com,” which included a signature block that provided “the defendant’s name and the name of his business . . . (as well as other information, such as the business’ address, telephone, and fax numbers) . . . .”<sup>50</sup> According to the court, this information sufficiently connected the defendant to the e-mail address in question—MerrittDC@aol.com.<sup>51</sup> Therefore, under FRE 901(b)(3), by comparison, the e-mails with only the e-mail address and no

---

(detective testifying that transcripts were accurate copies of online conversations sufficient evidence to authenticate).

<sup>42</sup> *Lanzon*, 639 F.3d at 1296.

<sup>43</sup> *Id.* at 1300.

<sup>44</sup> *Id.* at 1300–01.

<sup>45</sup> *Id.* at 1301.

<sup>46</sup> MCM, *supra* note 33, MIL. R. EVID. 901(b)(3); FED. R. EVID. 901(b)(3); see also *United States v. Crandall*, 1986 CMR LEXIS 2255, at \*4–5 (N.M.C.M.R. 1986) (finding signature comparison with known and unknown signatures satisfied MRE 901(b)(3)).

<sup>47</sup> 435 F. Supp. 2d. 36, 40 (D.D.C. 2006); see also *infra* Part II.C.3.

<sup>48</sup> *Safavian*, 435 F. Supp. 2d. at 40.

<sup>49</sup> *Id.*

<sup>50</sup> *Id.* at 40–41.

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

signature blocks were also properly authenticated as e-mails of Safavian.<sup>52</sup>

## 3. Distinctive Characteristics and the Like

Evidence may also be properly authenticated if its distinctive characteristics, “taken in conjunction with circumstances,” demonstrate that it is what it purports to be.<sup>53</sup> For example, when law enforcement officers apprehended Raul Trujillo for his connection with a cocaine smuggling ring, Trujillo was put through the standard “booking” procedures.<sup>54</sup> Trujillo at some point in the process asked to use the restroom, and used that opportunity for respite to attempt to eat a note with evidentiary value.<sup>55</sup> Special agents, noticing Trujillo’s attempt, pulled Trujillo from the bathroom “and saw a piece of paper ‘flutter’ into the toilet.”<sup>56</sup> The agents also retrieved the remainder of the paper from Trujillo’s mouth.<sup>57</sup> At trial, Trujillo challenged the authenticity of the scraps of paper.<sup>58</sup> However, based on the testimony of the agents about the circumstances surrounding the paper’s discovery, the court found that “given the proximity of time and the circumstances surrounding the obtaining of this evidence,” it was properly authenticated under FRE 901(b)(4).<sup>59</sup>

Similarly with digital evidence, forensic examiners compare hash values—the unique “fingerprints” of digital files—and metadata<sup>60</sup>—essentially data about data. Hash values and metadata are created and stored with digital evidence in the “background” of a user’s activity, often without the knowledge of the user.<sup>61</sup> Each of these processes provides the proponent of digital evidence the ability to authenticate evidence through its own distinctive characteristics.<sup>62</sup>

---

<sup>52</sup> *Id.* at 41.

<sup>53</sup> MCM, *supra* note 33, MIL. R. EVID. 901(b)(4); FED. R. EVID. 901(b)(4); see also *United States v. Worthington*, 2006 CCA LEXIS 410, at \*7–9 (A. Ct. Crim. App. 2006) (finding e-mail exchange properly authenticated with witness testimony regarding distinctive characteristics).

<sup>54</sup> *United States v. Trujillo*, 146 F.3d 838, 842–43 (11th Cir. 1998).

<sup>55</sup> *Id.* at 843–44.

<sup>56</sup> *Id.* at 843.

<sup>57</sup> *Id.*

<sup>58</sup> *Id.*

<sup>59</sup> *Id.* at 843–44.

<sup>60</sup> For a more detailed explanation of metadata and a discussion about the ethics of mining and scrubbing metadata, see Major Brian J. Chapuran, *Should You Scrub? Can You Mine? The Ethics of Metadata in the Army*, ARMY LAW., Sept. 2009, at 1.

<sup>61</sup> See *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 546–48 (D. Md. 2007).

<sup>62</sup> See *id.* at 546–48.

#### 4. Evidence About a Process or System

A proponent of evidence may also authenticate evidence by describing a process or system that created the evidence and demonstrating that it “produces an accurate result.”<sup>63</sup> For example, in *United States v. Espinal-Almeida*,<sup>64</sup> the government introduced data obtained from a GPS unit seized from aboard a vessel used to smuggle cocaine from the Dominican Republic to Puerto Rico.<sup>65</sup> Jose Durand, “a forensic scientist with Customs,” testified that he examined the GPS, secured the data, and used the GPS software to analyze the data.<sup>66</sup> Durand also testified extensively about how the GPS and the software worked, including the intentional margin of error that manufacturers build into each commercial GPS unit to distinguish them from government units.<sup>67</sup> The court found that even though Durand did not testify about whether or not the device and software were in good working order, such evidence could be reasonably inferred, and the GPS data and analysis were properly authenticated under FRE 901(b)(9).<sup>68</sup>

#### 5. Weight Versus Admissibility

Even when a proponent’s efforts to authenticate evidence are not perfect, minor defects in evidence regarding authentication generally go to weight rather than admissibility.<sup>69</sup> For example, in *Laurentz v. State*, prosecutors offered evidence of James Laurentz’s Facebook messages to the child victim with whom he had sexual contact the night before.<sup>70</sup> In the messages, Laurentz was apologetic and begged for forgiveness.<sup>71</sup> Laurentz challenged the authenticity of the messages, arguing, among other things, that the victim’s “name [was] misspelled on the exhibit.”<sup>72</sup> However, the court ruled that the state had sufficiently authenticated the messages “through witness testimony and circumstantial evidence,” and noted that the misspelling of the victim’s name was merely a factor for the “jury to consider when evaluating the weight and credibility of the witness testimony linking the correspondence to [the victim].”<sup>73</sup>

<sup>63</sup> MCM, *supra* note 33, MIL. R. EVID. 901(b)(9); FED. R. EVID. 901(b)(9).

<sup>64</sup> 699 F.3d 588, 611 (1st Cir. 2012).

<sup>65</sup> *Id.* at 595–96, 608.

<sup>66</sup> *Id.* at 611.

<sup>67</sup> *Id.* at 611–12.

<sup>68</sup> *Id.* at 612.

<sup>69</sup> WEINSTEIN’S EVIDENCE MANUAL § 8.01[1] (citing *Orr v. Bank of Am., NT & SA*, 285 F.3d 764, 773 n.6 (9th Cir. 2002)).

<sup>70</sup> 2013 Tex. App. LEXIS 12603, at \*1–5 (Tex. App. 2013).

<sup>71</sup> *Id.* at \*3–4.

<sup>72</sup> *Id.* at \*15.

<sup>73</sup> *Id.* at \*11, \*15–16.

#### III. Analysis

The traditional methods of authentication readily lend themselves to the authentication of digital evidence. Courts have already turned to those traditional methods to authenticate websites and e-mail.<sup>74</sup> Though cloud based evidence is different, evidence obtained from the cloud is closely analogous to evidence obtained from websites and e-mail.<sup>75</sup> Thus, though no case law on this subject matter exists just yet, thoughtful consideration of the similarities and differences between cloud based evidence, e-mail, and webpages, coupled with application of the traditional means of authentication, will enable counsel to satisfy the relatively low threshold requirements of MRE 901.

##### A. Criminal Evidence in the Cloud

The importance of cloud based digital evidence in criminal prosecutions is slowly starting to reveal itself in the record of published criminal decisions. Cloud storage is remote and accessible from virtually anywhere the user can access the internet. Users can therefore distance themselves from the data stored on the cloud. Users can also reduce the ability of the government to discover the data by either hiding their cloud storage activities or by using secure anonymous cloud service providers.<sup>76</sup> Thus, once the government does secure cloud-based digital evidence, it can prove invaluable in a variety of aspects.

The District Court for the Eastern District of New York recognized the intrinsic value and, in particular, the dangerous nature of cloud-based evidence when it assessed the continued pre-trial detention of Adam Savader.<sup>77</sup> In *Savader*, the government’s criminal complaint described the conduct of a defendant who, using a variety of methods,

<sup>74</sup> See *infra* Part III.B.

<sup>75</sup> See *infra* Part III.C.

<sup>76</sup> An assortment of cloud storage providers now offer “anonymous” storage. See, e.g., *FAQs, SPIDER OAK*, [https://spideroak.com/faq/category/privacy\\_passwords/](https://spideroak.com/faq/category/privacy_passwords/) (last visited May 1, 2014) (“SpiderOak is, in fact, truly zero knowledge. The only thing we know for sure about your data is how many encrypted data blocks it uses . . . .”); *Anonymous Cloud Servers, HOST CONFIDENTIAL*, <http://hostconfidential.com/page.php?id=20> (last visited May 1, 2014) (“Dedicated anonymous cloud servers look, behave, and work exactly like anonymous dedicated servers. These instances run in a [sic] anonymous virtualized cloud environment, . . . .”). Data Shell offers cloud storage and accepts BitCoin for payment, which takes cloud storage anonymity to a new level. *DATA SHELL*, <http://www.datashell.co.uk/> (last visited May 1, 2014); see also *PROSPECTIVE ANALYSIS ON TRENDS IN CYBERCRIME FROM 2011 TO 2020*, *supra* note 31, at 11. “In general, the anonymity of the Internet and the global breadth and depth of networks support the impunity of the criminals, and cloud computing will make it even more difficult to look for and record evidence.” *Id.* For a thorough discussion on BitCoin and its use in criminal endeavors, see Derek A. Dion, Note, *I’ll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-economy of Hackercash*, 2013 U. ILL. J.L. TECH. & POL’Y 165 (2013).

<sup>77</sup> *United States v. Savader*, 2013 WL 1943014 (E.D.N.Y. 2013).

victimized fifteen young women “through unauthorized access to computer systems, extortion and cyber stalking.”<sup>78</sup> With some skill and social engineering, Savader managed to secure the passwords of his victims, gain access to their personal data, and gather “compromising photos of the victims—usually in various states of undress . . . .”<sup>79</sup> Savader would then use the information he obtained to extort and threaten his victims.<sup>80</sup>

For the court, Savader’s continued detention would turn not on the nature of his offenses, but rather on the continued threat Savader posed if released.<sup>81</sup> Because Savader’s charges did “not appear to constitute crimes of violence,” under the Bail Reform Act, the government could only secure Savader’s continued detention if he posed a potential future threat to the witnesses or victims.<sup>82</sup>

In assessing Savader’s risk, the court looked primarily to the government’s evidence of Savader’s cloud storage account.<sup>83</sup> Although the government had secured “approximately 25 computer devices” from Savader’s home,<sup>84</sup> it was the discovery of his cloud storage account that was most relevant to the detention application.<sup>85</sup> In his cloud account, Savader stored files that bore the names of the victims, which “presumably contain[ed] the photograph files used as part of the extortion.”<sup>86</sup> Because Savader had the ability to access these cloud-based files from almost anywhere, the court reasoned, Savader had “effectively ‘weaponized’ these items, presenting a significant risk [to his victims].”<sup>87</sup> In the end, though, the court characterized it as a close call, and approved Savader’s continued detention to effectively prevent Savader from accessing his “secret cache of weapons.”<sup>88</sup>

As this decision pertained to a pre-trial detention hearing, there was no discussion regarding the admissibility of the evidence the government had obtained. However, one

---

<sup>78</sup> *Id.* at \*1.

<sup>79</sup> *Id.* at \*2.

<sup>80</sup> *Id.* at \*2–3.

<sup>81</sup> *Id.* at \*12–13.

<sup>82</sup> *Id.* The Bail Reform Act outlines the requirements for the “release or detention of a defendant pending trial.” 18 U.S.C. § 3142 (2014). Under the act, the government can request a hearing to secure continued detention for defendants who committed a “crime of violence,” an offense with a potential sentence of life imprisonment or death, or certain controlled substances offenses. *Id.* § 3142(f)(1). The government may also request continued detention if the government suspects that the defendant will flee or attempt to obstruct justice. *Id.* § 3142(f)(2).

<sup>83</sup> *Savader*, 2013 WL 1943014, at \*13.

<sup>84</sup> *Id.* at \*4.

<sup>85</sup> *Id.* at \*13–14.

<sup>86</sup> *Id.* at \*13.

<sup>87</sup> *Id.* at \*14.

<sup>88</sup> *Id.* at \*14–17.

of the first hurdles at trial would be the authentication of the evidence the government obtains, including any cloud-based evidence.

## B. Authenticating E-mail and Web Pages—An Intermediate Step

Before considering an acceptable approach to authenticating cloud-based evidence, a discussion regarding authentication of closely related digital evidence is helpful. E-mail and webpages, though distinct, share similar characteristics to cloud-based evidence. By drawing from the procedures now well established for authentication of e-mail and webpages, counsel can develop a methodology for authenticating cloud-based evidence.

### 1. Authenticating E-mail

Authentication of some forms of digital evidence, at one time a challenge, has now become well-established practice.<sup>89</sup> In fact, in 2007, when parties to a civil suit proffered nothing but unauthenticated e-mail traffic as evidence, one district court magistrate judge took to authoring a 100-page decision to express his intolerance for the misstep, and dismissed the suit.<sup>90</sup> In drafting what is essentially a handbook on authenticating digital evidence, the court noted that e-mail evidence is extremely common and “there are many ways in which e-mail evidence may be authenticated.”<sup>91</sup>

According to the court, the most frequent methods used to authenticate e-mail under FRE 901 include testimony from a person with personal knowledge of the e-mail, comparison with authenticated samples, evidence of distinctive characteristics, and certified copies of business records.<sup>92</sup> For example, a proponent of an e-mail message may show, with either direct or circumstantial evidence, that the message included the sender’s and recipient’s e-mail address, that the recipient replied to the message, or that the message was discussed in subsequent conversations.<sup>93</sup>

When Eugene Devbrow, a prisoner in the custody of the Indiana Department of Corrections, filed suit alleging retaliation by a prison guard, he sought to introduce an e-

---

<sup>89</sup> “Indeed, it is not unusual to see a case consisting almost entirely of e-mail evidence.” *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 554 (D. Md. 2007); see also WEINSTEIN’S EVIDENCE MANUAL § 8.01[3][f] (outlining the process of authenticating e-mail and chat room conversations).

<sup>90</sup> See *Lorraine*, 241 F.R.D. at 534–35.

<sup>91</sup> *Id.* at 554.

<sup>92</sup> *Id.* at 555; see also *supra* Part II.C.

<sup>93</sup> WEINSTEIN’S EVIDENCE MANUAL § 8.01[3][f].

mail to evidence his claim.<sup>94</sup> Devbrow received the e-mail directly from the prison, which he argued was sufficient to satisfy the authentication requirements of FRE 901.<sup>95</sup> The Seventh Circuit recognized that certain circumstantial evidence, “such as an e-mail’s context, e-mail address, or previous correspondence between the parties,” might serve the purposes of FRE 901.<sup>96</sup> However, “the most direct method of authentication is a statement from the author or an individual who saw the author compose and send the e-mail.”<sup>97</sup>

The guard who engaged in the retaliatory conduct allegedly authored the e-mail Devbrow sought to introduce.<sup>98</sup> Try as he might, it is unlikely that, as an inmate, Devbrow would have the ability to secure direct evidence of authenticity.<sup>99</sup> Without direct evidence, and because Devbrow also failed to provide sufficient circumstantial evidence of authenticity, the Seventh Circuit held that exclusion of the e-mail by the trial court was proper.<sup>100</sup>

## 2. Authenticating Webpages

Authentication of a commercial web page is only slightly more difficult than the authentication of e-mail. Because of the increased potential for third-party manipulation, courts “require proof by the proponent that the organization hosting the website actually posted the statements or authorized their posting.”<sup>101</sup> However, webpages from social networking sites, deemed particularly susceptible to manipulation, garner more scrutiny from courts and require more substantial authentication.<sup>102</sup> Still,

<sup>94</sup> Devbrow v. Gallegos, 2013 U.S. App. LEXIS 22278, at \*4-5 (7th Cir. 2013).

<sup>95</sup> *Id.* at \*5.

<sup>96</sup> *Id.* at \*6.

<sup>97</sup> *Id.*

<sup>98</sup> *Id.* at \*5.

<sup>99</sup> “But Devbrow did not show that either he or anyone else saw Gallegos actually compose or transmit the e-mail . . . .” *Id.* at \*6.

<sup>100</sup> *Id.* \*5-6.

<sup>101</sup> Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 555 (D. Md. 2007) (citation omitted). See also the strange case of *United States v. Jackson*, involving a wayward law student who attempted to defraud United Parcel Service and then cover up the fraud by attributing the matter to a white supremacist group. 208 F.3d 633 (7th Cir. 2000). Jackson sought to introduce postings from the group’s website that purported to take responsibility for the damage for which she sought compensation. *Id.* at 638. The trial court, however, properly excluded the evidence “because it lacked authentication.” *Id.* “Jackson needed to show that the web postings . . . actually were posted by the groups, as opposed to being slipped onto the groups’ web sites by Jackson herself, who was a skilled computer user.” *Id.*

<sup>102</sup> See, e.g., *Griffin v. Maryland*, 2011 Md. LEXIS 226 (Md. 2011). In *Griffin*, the government authenticated a MySpace page with evidence of date of birth, residence, and photographs of the purported user offered by an investigating detective. Reversing the accused’s murder conviction, the appellate court suggested soliciting evidence from the purported author, searching the author’s computer for corroborating evidence, or obtaining

as with e-mail, for the proponent to demonstrate that the website is what it purports to be, the proponent might offer direct or circumstantial evidence from a witness with personal knowledge,<sup>103</sup> demonstrate distinctive characteristics of the site, or establish indications of official endorsement by the owner.<sup>104</sup>

In *State v. Rossi*, Nicholas Rossi sought a new trial following his conviction for sexual imposition and public indecency following a sexual encounter that occurred in the stairwell of a community college campus.<sup>105</sup> The basis for Rossi’s request was “newly discovered evidence” of the victim’s recantation and motive to lie.<sup>106</sup> As proof, Rossi offered a “blog post copied from the Myspace web address which Rossi alleges was written and posted by the victim . . . after his trial was concluded.”<sup>107</sup>

At the hearing on Rossi’s motion for a new trial, the court ruled that Rossi failed to properly authenticate the post from the webpage.<sup>108</sup> The state, in response to Rossi’s

---

corroborating evidence from the social networking service provider. *Id.* at \*3-4, \*34-36. See also *United States v. Standing*, where the court found that the defendant’s website was properly authenticated when an agent testified that the domain registrant was an associate of the defendant (who was using a pseudonym). 2005 U.S. Dist. LEXIS 41330, at \*5-6, \*17 (D. Ohio 2005).

<sup>103</sup> See *United States v. Bansal*, 663 F.3d 634, 667-68 (3d Cir. 2011). *Bansal* involved the prosecution of an illegal online pharmacy operation. *Id.* at 640-42. Bansal challenged the authentication of the screenshots of his website. *Id.* at 667. The government had offered screenshots of the website obtained from the Internet Archive’s “Wayback Machine.” *Id.* Because “the government called a witness to testify about how the Wayback Machine website works and how reliable its contents are,” and “compared the screenshots with previously authenticated and admitted images,” the evidence was sufficient to support authentication under FRE 901(b)(1). *Id.* at 667-68.

<sup>104</sup> See *Lorraine*, 241 F.R.D. at 556; see also FED. R. EVID. 901(b). Additional considerations include

[t]he length of time the data was posted on the site; whether others report having seen it; whether it remains on the website for the court to verify; whether the data is of a type ordinarily posted on that website or websites of similar entities (e.g., financial information from corporations); whether the owner of the site has elsewhere published the same data, in whole or in part; whether others have published the same data, in whole or in part; [and] whether the data has been republished by others who identify the source of the data as the website in question.

*Lorraine*, 241 F.R.D. at 555-56 (quoting Gregory P. Joseph, *Internet and E-mail Evidence*, 13 PRAC. LITIGATOR (Mar. 2002)), reprinted in STEPHEN A. SALTZBURG ET AL., FEDERAL RULES OF EVIDENCE MANUAL pt. 4, at 20 (9th ed. 2006).

<sup>105</sup> 2012 Ohio App. LEXIS 2236, at \*P2-P3, \*P16 (Ohio Ct. App. 2012).

<sup>106</sup> *Id.* at \*P3. The post read, *inter alia*, “But I have done went so far by lying n [sic] getting some stranger to go to jail and in legal so you wouldn’t think I would cheat on you even when I did slip because he was cute, but I didn’t give in to my desire . . . . I’m drunk right now, but maybe when I [sic] sober we can talk about it.” *Id.* (emphasis in original).

<sup>107</sup> *Id.* at \*P9.

<sup>108</sup> See *id.*

proffer, presented testimony from a forensic expert.<sup>109</sup> The expert stated that the blog post had an incorrect day-date match (i.e., the day of the week did not match with the calendar date of the year), which indicated the post had been fabricated or altered.<sup>110</sup> The expert also testified about the ease and simplicity of such an alteration.<sup>111</sup> Additionally, the expert testified that the victim was unequivocal in her denial of authorship of the post.<sup>112</sup> Therefore, in light of the testimony, and the internal inconsistency, it was proper for the trial court to find that the webpage post was not properly authenticated.<sup>113</sup>

### 3. Hybrid Cases

At times, the challenge of authentication is complicated when the evidence is a social networking webpage with traits of e-mail messaging. For example, in *Campbell v. State*,<sup>114</sup> the Court of Appeals in Texas was confronted with an authentication challenge involving Facebook messages. The state charged Travis Campbell with aggravated sexual assault and aggravated assault with a deadly weapon, stemming from an incident that followed his girlfriend's receipt of a Facebook message from another man.<sup>115</sup>

At trial, the state introduced evidence of inculpatory messages that Campbell sent to his girlfriend.<sup>116</sup> Each of the messages contained a header that included Campbell's name and a date stamp.<sup>117</sup> The appellate court analyzed the authentication issue under Texas Rules of Evidence 901, which is modeled closely after its federal counterpart.<sup>118</sup> Recognizing that social media sites such as Facebook are susceptible to fraud, the court stated that it is insufficient to merely argue that on its face, a message purports to be from a person's social networking account.<sup>119</sup>

However, to satisfy the rule in this case, the state

---

<sup>109</sup> *Id.* at \*P18.

<sup>110</sup> *Id.* The post stated it was published on Monday, May 16, 2008. However, May 16, 2008, was actually a Friday. *Id.*

<sup>111</sup> *Id.* at \*P19.

<sup>112</sup> *Id.*

<sup>113</sup> *See id.* at \*P21–22.

<sup>114</sup> 382 S.W.3d 545, 547 (Tex. Ct. App. 2012).

<sup>115</sup> *Id.* at 546–47.

<sup>116</sup> *Id.* at 550.

<sup>117</sup> *Id.*

<sup>118</sup> *Id.* at 547–48. The Texas rules provide that “[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.” TEX. R. EVID. 901(a).

<sup>119</sup> *Campbell*, 382 S.W.3d at 549. For example, “anyone can establish a fictitious profile under any name” and “a person may gain access to another person’s account by obtaining the user’s name and password.” *Id.*

presented additional circumstantial evidence to authenticate the messages.<sup>120</sup> First, Campbell’s girlfriend and victim testified that she received the messages, that she did not send the messages to herself, and that at the time the messages were sent, the victim did not have access to Campbell’s Facebook account.<sup>121</sup>

Additionally, the messages revealed an internal consistency upon which the court also relied to support the threshold showing of authenticity.<sup>122</sup> Campbell, who was of Jamaican decent, testified at trial and his unique speech pattern was reflected in the messages that he sent to his victim following the attack.<sup>123</sup> The messages also included references to the attack and the potential for criminal charges.<sup>124</sup> Thus, when considered together with the relevant undisputed testimony, the proffered evidence was at least “within the zone of reasonable disagreement,” and the jury was entitled to make the determination of authenticity.<sup>125</sup>

### C. Authenticating Evidence from the Cloud

Digital evidence from the cloud can be similar in many ways to e-mail and webpage evidence. E-mail or webpages may be remotely stored, they are accessible online, across multiple platforms, and are susceptible to manipulation or fraud. A user’s cloud account, much like a webpage or e-mail account, can be “hacked,” faked, or shared with other users.<sup>126</sup>

---

<sup>120</sup> *Id.* at 549–50.

<sup>121</sup> *Id.* at 550.

<sup>122</sup> *Id.* at 550–51.

<sup>123</sup> *Id.* For example, one message read, “[I] did you bad something that you would never though [sic],” and another read, “[I] should never put my hand on you, who is me to do that to you.” *Id.* at 550. By way of comparison, at trial, Campbell testified that “I take up the knife out of her way, her reach, and tell her that, this, you cannot play with knife because knife will give you a cut.” *Id.* at 551 n.3.

<sup>124</sup> *Id.* at 550–51. For example, Campbell wrote, “[D]on’t lock me up please i am begging you,” and “i am so f---ing stuppid [sic] for hurthig [sic] u i am guilty.” *Id.* at 550.

<sup>125</sup> *Id.* at 551–52 (quoting *Tienda v. State*, 358 S.W.3d 633, 638, 645–46 (Tex. Crim. App. 2012)); *see also* *United States v. Grant*, 2011 CCA LEXIS 217, at \*3–5 (A.F. Ct. Crim. App. 2011) (finding Facebook messages properly authenticated with testimony regarding timing, photograph, and message content).

<sup>126</sup> *See, e.g., Campbell*, 382 S.W.3d at 548–49 (“[I]n evaluating whether an electronic communication has been sufficiently linked to the purported author, we recognize that electronic communications are susceptible to fabrication and manipulation.”). In *Campbell*, the court went on to discuss the authentication issues associated with false account creation and unauthorized access. *Id.* at 549. For a more thorough discussion of internal consistency as it relates to authentication, see *supra* notes 122 through 125 and accompanying text.

However, cloud-based data, unlike e-mail, lacks the readily identifiable characteristics, such as a sender and recipient, that tend to make authentication of e-mail easier.<sup>127</sup> Therefore, in the absence of an acknowledgement of authorship and authenticity from a party with relevant knowledge, cautious counsel should consider gathering additional circumstantial evidence of authenticity to satisfy the requirements of MRE 901.<sup>128</sup>

Combining the established methods for authenticating webpages and e-mail with the following additional considerations, counsel will be better prepared to deal with the challenge of authenticating cloud-based digital evidence. These additional considerations include: ownership or authorship of the evidence, data integrity, redundancy, and the nature of the cloud service itself.

### 1. Establishing Ownership/Authorship

Establishing ownership or authorship of digital evidence obtained from the cloud can assist with authentication under MRE 901. As is the case with e-mail and webpages,<sup>129</sup> showing that a relevant party owned or authored the evidence may be an important part of the circumstantial evidence portrait that a proponent paints during the authentication process. To determine ownership or authorship, the cloud service provider's terms of service are a good starting point.<sup>130</sup>

First, knowing what procedures the service provider uses to record transactions and assign those transactions to particular users can be helpful. Some cloud service providers collect an extensive amount of user information when the user accesses the service. Dropbox, for example, collects information regarding the device and software used to access the service, including the internet protocol address, the last webpage visited before visiting Dropbox, user searches within Dropbox, the user's mobile carrier, and "date and time stamps associated with transactions, system

configuration information, [and] metadata . . ."<sup>131</sup> Dropbox also warns that while it does not currently geolocate a user via their application software, it may do so in the future, and does collect geolocation data that may be included in any photos that a user uploads to its cloud service.<sup>132</sup> This information can serve to circumstantially link the subject to the evidence in question, or, in the case of shared folders, may demonstrate the proponent of the evidence needs to dig deeper to establish ownership or authorship.

Second, the cloud service provider's terms of service may provide guidance regarding ownership of content. Ownership information can vary greatly among cloud service providers. For example, Dropbox informs users that "Your Stuff is yours. These terms don't give us any rights to Your Stuff . . ."<sup>133</sup> Google, however, notes that while user submitted content belongs to the owner, Google has a license to use or modify that content as Google sees fit.<sup>134</sup>

Finally, the evidence itself may share internal consistencies that demonstrate ownership or authorship.<sup>135</sup> For example, an accused may take a "selfie"<sup>136</sup> with his iPhone at the scene of the crime, and the photo may then be uploaded to iCloud. In a process similar to authentication of a Facebook message, the proponent may seek to show that the photo reveals the defendant's face and arm, as he holds the phone to take the picture, while standing at the scene of

<sup>127</sup> Nonetheless, sender and recipient information alone is generally insufficient to authenticate e-mail evidence. *Campbell*, 382 S.W.3d at 550 ("[T]he messages themselves purport to be messages sent from a Facebook account bearing Campbell's name to an account bearing Ana's name. While this fact alone is insufficient to authenticate Campbell as the author, when combined with other circumstantial evidence, the record may support a finding by a rational jury that the messages were authored and sent by Campbell.").

<sup>128</sup> *Campbell v. State* is instructive in this matter. See *supra* Part III.B.3.

<sup>129</sup> See *supra* Parts III.B.1 and III.B.2.

<sup>130</sup> Counsel may introduce evidence of a cloud service provider's terms of service through a witness with knowledge of the terms, and need not necessarily be a witness with "personal" knowledge. See generally *United States v. Swecker*, 2001 CCA LEXIS 107, at \*12 (A.F. Ct. Crim. App. 2001) ("The case law interpreting this rule indicates that the foundation witness need not be the person who prepared the record, nor need they have personal knowledge of the entries. The witness need only have sufficient knowledge of the record-keeping system to establish its reliability.").

<sup>131</sup> *Privacy Policy*, DROPBOX, available at <http://www.dropbox.com/privacy> (last visited Dec. 1, 2013).

<sup>132</sup> *Id.* Similarly, when a user accesses Google Drive's cloud service, Google collects search queries, telephone numbers, time and date information, internet protocol address, device information, and, at times, geolocation information. *Privacy Policy*, GOOGLE DRIVE, <http://www.google.com/policies/privacy/> (last visited May 1, 2014). Apple's iCloud service makes consent to geolocation a part of their service as well. *iCloud Terms and Conditions*, APPLE ICLOUD, <https://www.apple.com/legal/internet-services/icloud/en/terms.html> (last visited May 1, 2014). Geolocation refers to the ability to pinpoint the location of the user through a device's GPS, wireless, cell-tower, or Bluetooth access. In re *Smartphone Geolocation Data Application*, 2013 WL 5583711, at \*7 (E.D.N.Y. 2013) ("One important aspect of smartphone technology is the ability of these devices to identify, in real time, their geographic location, which data can be shared with certain programs and providers to enable advanced functions.").

<sup>133</sup> See *Terms of Service*, DROPBOX, <http://www.dropbox.com/terms> (last visited May 2, 2014).

<sup>134</sup> See *Google Documents Terms of Service*, GOOGLE, <http://www.google.com/intl/en/policies/terms/> (last visited May 1, 2014) ("When you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content.").

<sup>135</sup> See, e.g., *Campbell v. State*, 382 S.W.3d 545, 551-52 (Tex. Ct. App. 2012).

<sup>136</sup> "The term 'selfie' is the name given to a self-portrait photograph, 'often snapped at odd angles with smartphones[.]' and 'typically made to post on a social networking website (or sen[t] in a text message)[.]'" *United States v. Doe*, 2013 WL 4212400, at \*8 n.6 (W.D.N.C. 2013) (citation omitted).

the crime. Taken together with some additional corroborating evidence for example, testimony that indicates the background is indeed the scene of the crime, or geolocation data, and evidence that the iCloud service belonged to the defendant, the purposes of MRE 901 would be served.

## 2. Data Integrity, Alterations, and Tampering

In addition to establishing authorship or ownership of digital evidence obtained from the cloud, counsel should also consider the procedures the service provider uses to ensure data integrity. This is significant because some cloud services make no guarantees of data integrity.<sup>137</sup> Evidence that shows signs of corruption, alteration, or tampering may or may not be admissible.<sup>138</sup> If altered evidence is sufficiently authenticated and admitted, the fact finder may accord that evidence less weight.<sup>139</sup>

In *United States v. Hock Chee Koo*, the government charged Shengbao Wu with conspiracy to commit wire fraud, computer fraud, and theft of trade secrets.<sup>140</sup> In the course of the investigation, Wu's laptop was secured by the government from Lawrence Hoffman, Wu's employer.<sup>141</sup> Hoffman "had filed a civil lawsuit against Wu the day before he obtained Wu's laptop."<sup>142</sup> Then, over the course of two days, Hoffman used the laptop and perused its contents.<sup>143</sup> A subsequent FBI forensic examination revealed that Hoffman's actions, combined with those of a civilian

forensic examiner hired by Hoffman, resulted in the access, alteration, or deletion of over 1,000 files.<sup>144</sup>

Because Hoffman and his examiners tampered with and altered the evidence, the trial court excluded the FBI's forensic image of Wu's laptop.<sup>145</sup> Despite the government's assertion that the evidence of alteration should go to weight, not admissibility, the government failed to demonstrate that the laptop was "in 'substantially the same condition as when the crime was committed.'"<sup>146</sup> Thus, the laptop image was not properly authenticated under FRE 901(a) and was excluded.<sup>147</sup>

## 3. Redundancy

Even if digital evidence is altered, tampered with, or corrupt, the cloud service provider may have sufficient redundancy to provide a copy of the original unaltered or intact content. For example, Dropbox advises its users that Dropbox keeps redundant backups of all data over multiple locations to prevent the remote possibility of data loss. "In fact, if you're using the Dropbox desktop application, your files are backed up several times."<sup>148</sup> Thus, if authentication due to corruption, alteration, or tampering becomes an issue, counsel should inquire into the service provider's policy regarding backup timing and frequency.<sup>149</sup> This may afford the proponent of such evidence the ability to secure an unaltered or undamaged version of the evidence.

## 4. Nature of the Cloud Service

Finally, in considering potential issues regarding digital evidence obtained from the cloud, counsel should inquire into the nature of the cloud service itself. Cloud services can be free public services, paid private services, or a hybrid of both.<sup>150</sup> Additionally, the cloud service may provide the

---

<sup>137</sup> See, e.g., *Terms of Service*, DROPBOX, *supra* note 133 ("You, and not Dropbox, are responsible for maintaining and protecting all of your stuff. Dropbox will not be liable for any loss or corruption of your stuff, or for any costs or expenses associated with backing up or restoring any of your stuff."); *iCloud Terms and Conditions*, APPLE ICLOUD, *supra* note 132 ("Apple does not guarantee or warrant that any content you may store or access through the service will not be subject to inadvertent damage, corruption, loss, or removal . . .").

<sup>138</sup> See, e.g., *State v. Ararat*, 2006 Ohio App. LEXIS 1592, at \*P56 (Ohio Ct. App. 2006) (finding that security video altered to put the video in chronological order and padded, "wherein duplicate images are inserted between the photos taken by the security cameras at set intervals, in order to create a final product that approximates real time viewing" was properly admitted by the trial court); *United States v. Dawson*, 425 F.3d 389, 392-93 (7th Cir. 2005) (recordings of conversations with defendants were properly authenticated even though they contained gaps and erasures and possibly exculpatory information). *But see* *United States v. Hock Chee Koo*, 770 F. Supp. 2d 1115 (D. Or. 2011) (finding alterations were too significant to permit authentication of evidence).

<sup>139</sup> See, e.g., *United States v. Safavian*, 435 F. Supp. 2d 36, 41 (D.D.C. 2006) (rejecting defendant's argument that because e-mail can be altered, especially when replied to or forwarded, it could not be properly authenticated, finding instead that "defendant's argument is more appropriately directed to the weight the jury should give the evidence, not to its authenticity.").

<sup>140</sup> 770 F. Supp. 2d 1115, 1118-19 (D. Or. 2011).

<sup>141</sup> *Id.* at 1119, 1124.

<sup>142</sup> *Id.* at 1125.

<sup>143</sup> *Id.*

<sup>144</sup> *Id.*

<sup>145</sup> *Id.* at 1126.

<sup>146</sup> *Id.* (citation omitted).

<sup>147</sup> *Id.*

<sup>148</sup> *Security Overview*, DROPBOX, <https://www.dropbox.com/help/122/en> (last visited May 2, 2014) ("By default, Dropbox saves a history of all deleted and earlier versions of files for 30 days for all Dropbox accounts.").

<sup>149</sup> This note does not address the implication of Federal Rules of Evidence 1001-08, the "best evidence rule." For a thorough discussion of the application of the best evidence rule to digital evidence, see *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 576-83 (D. Md. 2007). See also *State v. Bellar*, 217 P.3d 1094, 1110 (Or. Ct. App. 2009) (Sercombe, J., dissenting) (quoting Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 564 (2005)) (asserting that an "original" is likely a distinction without a difference when it comes to digital evidence).

<sup>150</sup> Apple's iCloud is a service provided to Apple product users, though it does offer some PC support through Apple software. *iCloud*, ICLOUD, <http://www.apple.com/icloud/> (last visited May 2, 2014). Dropbox and Google Drive offer free public services with an option to buy more storage space. DROPBOX, <https://www.dropbox.com/upgrade> (last visited May 2,

user the option to publicly or privately share access to the stored files.<sup>151</sup> Shared access to files creates a potential authentication issue when considering ownership or authorship.<sup>152</sup>

However, providing some evidence of each of these cloud-specific characteristics will help counsel when authenticating, or challenging the authentication of, cloud data. Coupling this evidence with the established methods for authenticating e-mail and webpages will help ensure that the proffered cloud based evidence can be authenticated under MRE 901. Regardless, as noted above, the threshold is low and counsel need only show that the evidence proffered is what it purports to be.<sup>153</sup>

#### IV. Conclusion

Storing data in the cloud is becoming more and more commonplace. Its frequency of use will likely only continue to increase. As a result, a growing number of litigants will turn to the cloud for relevant evidence. To ensure admissibility of that evidence at trial, counsel need to establish a sufficient foundation for authentication.

Currently, there is a dearth of case law and guidance regarding proper methods of authentication of cloud data, but counsel are not without guideposts. Though cloud-based digital evidence is different from e-mail and webpages, coupling evidence of ownership, authorship, data integrity, and the nature of the cloud service with traditionally accepted methods of authentication for e-mail and webpages, will enable counsel to meet the threshold requirements of MRE 901 and clear one of the first hurdles of admissibility.

---

2014); *Storage Plan Pricing*, GOOGLE DRIVE, <https://support.google.com/drive/answer/2375123?hl=en> (last visited May 2, 2014). Amazon offers both free public and private business solutions. *Amazon Web Services*, AMAZON SIMPLE STORAGE SERVICE, <http://aws.amazon.com/s3/> (last visited May 2, 2014).

<sup>151</sup> See, e.g., *Dropbox Terms of Service*, DROPBOX, <https://www.dropbox.com/privacy#terms> (last visited May 29, 2014) (“The Services provide features that allow you to share your stuff with others or to make it public. There are many things that users may do with that stuff (for example, copy it, modify it, re-share it). Please consider carefully what you choose to share or make public. Dropbox has no responsibility for that activity.”).

<sup>152</sup> See *supra* Part III.C.1.

<sup>153</sup> See *supra* notes 33–35 and accompanying text.