


[Home](#)
[Search Database](#)
[Members](#)
[Calendar](#)
[Education & Training](#)
[About](#)
[Related Links](#)
[Help](#)
[Back](#)

## Electronically Stored Information: A Primer - A Litigator's Guide

Jules Epstein, Esquire <sup>1</sup>

In less than a decade, the judicial attitude toward and the litigator's reliance on electronically stored information (ESI) have changed dramatically. In 1999, judicial resistance to webpage evidence that might have been 'hacked' was so great as to exclude it outright; yet by 2007 its authenticity was deemed to be presumptively correct. The wealth and volume of data available from electronic sources are so great that concern is now being expressed that the costliness of discovery might limit access to the courts for many litigants. (See "The Big Data Dump," *The Economist*, August 28, 2008).

Mastery of ESI requires the knowledge and skillful adaptation of traditional evidentiary rules. To ensure admissibility, the capable litigator must focus on five issues: investigation; discovery; authentication; hearsay concerns; and the issue of "original writings" [known colloquially as the "best evidence" rule].

Locating electronic evidence will be dependent on several factors. If the investigator is a state official, her/his searches will be cabined by Fourth Amendment strictures, while private actors will be restricted by state privacy and electronic communications [wiretap] laws. Privacy principles will govern when one spouse 'searches' a partner's computer, or when an employer checks that of an employee. The same is true when accessing e-mails or similar electronic communications. Once litigation has commenced, subpoena power and other discovery tools come into play. To this end, the Federal Rules of Civil Procedure have been amended, as one court explained:

Federal Rule of Civil Procedure 26(a) requires a party to disclose all documents, including electronically stored information, that the party may use to support its claims or defenses without awaiting a discovery request. Fed.R.Civ.P. 26(a)(1)(A)(ii).... Furthermore, Rule 26(b)(2) only limits the discovery of electronically stored information from sources that the party identifies as

not reasonably accessible because of undue burden or cost. Fed.R.Civ.P. 26(b)(2)...<sup>2</sup>

Where the ESI is on the Internet sophisticated search tools such as the "wayback machine" can be utilized. This program, available through the "Internet Archive"<sup>3</sup>, permits the user to "[b]rowse through 85 billion web pages archived from 1996 to a few months ago..." and see the content of a page on a particular date. Where the ESI is on a computer's hard drive, forensic software can search for particular types of files or content. One such program, EnCase, describes its capacities as including displays of "deleted emails, notes, contacts and calendar entries for PSTs, as well as copy/un-erase email messages to popular message formats for external reviews [and]...decod[ing] Web-browsing history and reveal[ing] cached HTML pages and associated images[.]"<sup>4</sup>

Often critical to a search of ESI are the discovery and interpretation of metadata. Essentially a hidden set of codes, metadata can reveal file dates (e.g., creation date, date of last data modification, date of last data access, and date of last metadata modification), and file permissions (e.g., who can read the data, who can write to it, who can run it).<sup>5</sup> If a discovery order requires the disclosure of metadata, that information can be provided on disk along with the documents in question; otherwise, access to or a mirror copy of the data storage device (hard drive, flash drive, etc.) and the appropriate software can reveal the pertinent codes. The absence of metadata may show that "anti-forensics" software has been used to delete/destroy data.<sup>6</sup> A related set of data is denominated "embedded information," which may reveal a "blind copy" address in an e-mail.

Assuming the ESI has been located, three remaining evidentiary obstacles (beyond that of assessing relevance) must be overcome to ensure admissibility. First, the evidence (e-mail, webpage, digital photograph) must be "authenticated," or shown to be the proof at issue "by evidence sufficient to support a finding that the matter in question is what its proponent claims."<sup>7</sup> This may be accomplished by calling a witness with knowledge who can identify the item(s); by establishing them as business records; by admission or stipulation in civil proceedings; or by showing the information was generated by/with a process that produces reliable results.<sup>8</sup>

Digital photographs are a case in point. Although easily subject to manipulation with readily available<sup>9</sup> computer software programs, the evidentiary standard for admissibility is low. The photograph may be authenticated by the photographer or someone familiar with the scene depicted; and where the digital photo has been enhanced or is a converted image, testimony of an expert is an essential addition to explain the process used and the proven track record of generating reliable results.<sup>10</sup>

Two issues remain after authentication. First, the contents of the ESI will undoubtedly contain hearsay, i.e., statements being introduced for the truth of the matter asserted.<sup>11</sup> This concern may be obviated by application of any number of hearsay exclusions or exemptions - the statement may be an admission of a party opponent<sup>12</sup>; an excited utterance<sup>13</sup> or present sense impression<sup>14</sup> (consider, in this regard, instance messages, text messages, and e-mails); a declaration of state of mind<sup>15</sup> or one made for purposes of medical diagnosis or treatment<sup>16</sup>; or a declaration against interest.<sup>17</sup> Many ESI documents will be admissible as business records;<sup>18</sup> others may be admissible as reports of government agencies.<sup>19</sup>

Two further cautionary notes apply regarding hearsay and ESI. Records generated by a system or process, such as a print-out of dialed telephone numbers or a toll booth receipt showing the date and time of payment, do not implicate the hearsay rule, as there is no assertion and there was no 'person' who originated the data. These records are the products of a process, and require authentication of the process' mechanism and reliability.<sup>20</sup> Second, chatroom dialogues (often utilized in internet sexual enticement prosecutions) will contain assertions not only by the accused but by others in the exchange. The latter will not be hearsay, as they are not admitted to prove the truth of what the third parties stated, but to provide context to the defendant's words.

After hearsay issues are resolved, the final evidentiary concern is the “original writings” [often termed the “best evidence”] requirement.<sup>21</sup> Because the contents of the writing [the e-mail, the webpage] are at issue, this rule requires production of an original. As duplicates are approved under the rule<sup>22</sup>, however, this should rarely be a barrier to admission.<sup>23</sup>

In sum, ESI offers a wealth of information. Its use depends on knowledgeable investigation and the recognition that introduction merely requires applying ‘old’ rules of evidence to new forms of proof.

[Up](#)

<sup>1</sup> Jules Epstein is Associate Professor of Law at Widener University School of Law, where he teaches Evidence and subjects in criminal law and procedure. Professor Epstein has worked with the National Institute of Justice and NCSTL on forensics projects and presentations. Thanks are due to Widener Adjunct Professor Richard Hermann, a partner at Morris James in Wilmington and a true expert in e-discovery, for his comments and assistance.

<sup>2</sup> *Square D Co. v. Scott Elec. Co.*, 2008 U.S. Dist. LEXIS 54917 (W.D. Pa. July 15, 2008).

<sup>3</sup> <http://www.archive.org/web/web.php>

<sup>4</sup> [http://www.guidancesoftware.com/law\\_enforcement/index.aspx](http://www.guidancesoftware.com/law_enforcement/index.aspx)

<sup>5</sup> *Scotts Co. LLC v. Liberty Mut. Ins. Co.*, 2007 U.S. Dist. LEXIS 43005 \*11 (S.D. Ohio June 12, 2007)

<sup>6</sup> *S. New Eng. Tel. Co. v. Global NAPs, Inc.*, 251 F.R.D. 82, 89 (D. Conn. 2008).

<sup>7</sup> Rule 901, Fed.R.Evid.

<sup>8</sup> Rule 9901(b)(9), Fed.R.Evid.

<sup>9</sup> See, e.g. [http://www.photographyreview.com/cat/digital photography software/editing software/PLS\\_3078crx.aspx](http://www.photographyreview.com/cat/digital%20photography%20software/editing%20software/PLS_3078crx.aspx) (last visited October 31, 2008; offering reviews of commercially available photography software).

<sup>10</sup> Rule 901(b)(9). For an excellent discussion of this and other ESI evidentiary issues, see *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 562 (D. Md. 2007).

<sup>11</sup> Rule 801, Fed.R.Evid.

<sup>12</sup> Rule 801(d)(2), Fed.R.Evid.

<sup>13</sup> Rule 803(2), Fed.R.Evid.

<sup>14</sup> Rule 803(1), Fed.R.Evid.

<sup>15</sup> Rule 803(3), Fed.R.Evid.

<sup>16</sup> Rule 803(4), Fed.R.Evid.

<sup>17</sup> Rule 804(b)(3), Fed.R.Evid.

<sup>18</sup> Rule 803(6), Fed.R.Evid.

<sup>19</sup> Rule 803(8), Fed.R.Evid.

<sup>20</sup> Rule 801(b), Fed.R.Evid., defines a declarant as a “person who makes a statement.”

<sup>21</sup> Rule 1001, Fed.R.Evid.

<sup>22</sup> Rule 1003, Fed.R.Evid.

<sup>23</sup> *But see*, *United States v. Bennett*, 363 F.3d 947, 953 (9th Cir. Cal. 2004) (original writings rule violated where agent testified to what GPS system showed without producing a printout).