

ADMISSIBILITY OF ELECTRONICALLY-STORED INFORMATION (“ESI”)

INTRODUCTION: Given its pervasiveness today, counsel must be prepared to recognize and manage the evidentiary issues associated with the admissibility of ESI.

FIVE ISSUES:

1. Is it **RELEVANT**?
2. Is it **AUTHENTIC**?
3. Is it **HEARSAY**?
4. Is it an **ORIGINAL OR DUPLICATE**?
5. Is there a **DANGER OF UNFAIR PREJUDICE**?

I. RELEVANCE (Rules 401, 402 & 105)

- a. **Rule 401:** *Does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be?* **Low threshold.**

II. AUTHENTICITY (Rules 901-902)

- a. **Rule 901(a):** *Can the proponent show that the ESI is what it purports to be?*

TIP: Easiest way to accomplish → 1. Stipulation at pretrial conference; or
2. Request to admit genuineness (Rule 36)

- b. **STANDARD:** prima facie showing ESI is what proponent claims it to be.

1. Courts have recognized authentication of ESI may require greater scrutiny than typically required for “hard copy” docs -- but have rejected calls to abandon existing rules of evidence when doing so.
 - Ultimately, same Q of assurance that ESI is what it purports to be.
2. Still, increasingly demanding that proponents of ESI evidence pay more attention to foundation than has been customary for “hard copy” docs, e.g.:
 - i. Does a computer processes data rather than merely storing it? If so, authentication issues may arise.
 - Need to authenticate and explain computer’s processing will depend on the complexity and novelty of the computer processing
 - Factors to consider: error rate in data inputting, security of the systems; quality and completeness of data input

c. HOW TO AUTHENTICATE

1. **Testimony of W** with knowledge that matter is what it is claimed to be
2. **Circumstantial evidence** – i.e. “appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances”
3. **by evidence describing a process or system used to produce a result** and

showing that such process/system produces and accurate result

d. **NO SINGLE APPROACH WILL WORK IN ALL INSTANCES.** Use these as a guideline:

1. Email.

- Spontaneous & informal: people tend to reveal more of themselves than in other forms of written communication.
- Often figure prominently in cases where state of mind, motive and intent must be proved.
- i. Most frequent ways to authenticate are via (1) W with personal knowledge; (2) via distinctive characteristics, including circumstantial evidence; and (3) as certified copies of business record.
- ii. Circumstantial Authentication
 - Printouts of e-mails usually bear sender's e-mail address, providing circumstantial evidence that the message was transmitted by the person identified in the e-mail address.
 - In responding to e-mail, person receiving message may transmit reply using the computer's reply function, which automatically routes the message to the address from which the original message came. Use of the reply function indicates the reply message was sent to the sender's listed e-mail address.
 - Contents may help also reveal details known only to the sender and the person receiving the message.

2. Internet Website Postings.

- i. Issues include possibility that persons other than sponsor of website were responsible for content of postings
- ii. Reaction of courts has ranged from skepticism to permissive
 - A. admitting based on dates and presence of identifying web addresses. *perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1153-54 (C.D. Cal. 2002) VS
 - B. requiring party proffering to produce testimony or affidavit from person w/ knowledge (e.g. webmaster) that org hosting website actually posted statements/authorized their posting
- iii. Be prepared to address 3 questions explicitly or implicitly:
 - A. What was actually on the website?
 - B. Does the exhibit or testimony accurately reflect it?
 - C. If so, is it attributable to the owner of the site?

3. Text Messages and Chat Room Content.

- i. Issues similar to those re website evidence
 - chat room messages usually posted by third parties, often using “screen names” – rather than site owner/administrator
 - cannot assume that content found in chat rooms was posted with knowledge or authority of the website host.
- ii. **Suggested foundational evidence to authenticate**
 - A. person used screen name at issue when engaging in chat room conversations (generally or at site in question);
 - B. when a meeting with the person using the screen name was arranged, the individual . . . showed up;
 - Classic underage sex internet “sting” operations
 - C. person using the screen name identified him/herself by name in the chat room conversation;
 - D. individual had in his possession information given to the person using the screen name; OR
 - E. Evidence from hard drive of individual’s computer showing use of same screen name.

4. Computer Stored Records and Data. – Least complicated to authenticate

- i. Issues concern **accuracy** and **authenticity**:
 - A. Accuracy may be impaired by incomplete data entry, programming errors, damage/contamination of storage media, power outages, equipment malfunctions, etc.
 - B. Data integrity may be compromised by improper search/retrieval techniques, data conversion, mishandling etc.

TIP: Common for multiple versions of electronic docs to exist, and thus difficult to establish that a version is the final/legally operative version.

FRCP 34 permits discovery of ESI and identification of form(s) in which it is to be produced. Can request production of ESI in its “native format” which includes metadata, i.e., file name, pathname or directory structure, file format or type, file size, file dates of creation, modification, last access, last metadata modification, file permissions on who can read/run it.

- ii. **Suggested Foundational Elements:**
 - A. business uses a computer.
 - B. computer is reliable.
 - C. business has procedure for inserting data into computer
 - D. procedure has safeguards to ensure accuracy/identify errors.

- E. business keeps computer in a good state of repair.
- F. W had the computer readout certain data.
- G. W used proper procedures to obtain the readout.
- H. computer in working order at the time W obtained the readout.
- I. W recognizes the exhibit as the readout.
- J. W explains how he or she recognizes the readout.
- K. if readout contains strange symbols or terms, W explains meaning of the symbols or terms for the trier of fact.

5. Computer Animation and Computer Simulations.

i. Computer Animation.

- Attractive b/c it in effect condenses disparate pieces of bland evidence into a single evidentiary package
 - ❖ Americans (TV watcher) primarily visual learners – many jurors find animation more understandable than charts or oral testimony.
- Courts usually allow admission if:
 - i. authenticated by testimony of W with personal knowledge of content of the animation; and
 - ii. showing that animation fairly/adequately portrays the facts and will help illustrate testimony given in case.

ii. Computer Simulation.

- A. Usually based on scientific/physical principles/data entered into computer programmed to analyze data & draw conclusions
- B. Generally **need proof of validity of the science** - treated as a form of scientific evidence offered for a substantive rather than demonstrative purpose.
- C. **Foundational requirements:**
 - i. computer is functioning properly;
 - ii. input and underlying equations are sufficiently complete and accurate, and disclosed to opposing party, so that they may challenge them; and
 - iii. program generally accepted by scientific community

6. Digital Photographs.

- Present unique authentication problems b/c they can be manipulated and altered.

A. Original digital photograph

Authenticated same as film photo, by W with personal knowledge of scene depicted who can testify that photo fairly and accurately depicts it.

B. Digitally converted images

Require **explanation of process** by which film photo converted to digital **from W with personal knowledge** that process produces accurate/reliable images

C. Digitally enhanced images

- unlikely any W who can testify how original scene looked if shadow was removed or colors intensified
- Need proof enhancement process produces reliable and accurate results: enters realm of scientific/technical evid

State v. Swinton (Conn. 2004): Δ convicted of murder in part based on **Adobe Photoshop** enhanced images **superimposing Δ's teeth over digital photos of bite marks taken from V's body**. State's bite mark expert testified Δ was source of bite marks on V. Δ testified he was not familiar with how Photoshop made overlay photos. Trial court admitted over objection, but got reversed.

Court: authentication required W who could testify as to exactly what jury was looking at, and Δ had right to X-E. Since state's W lacked computer expertise to do so, Δ was deprived of right to X-E.

i. Suggested Foundation:

1. W an expert in digital photography;
2. testify re creation of digital image composed of pixels & how computer process manipulates them
3. W testifies that processes used are valid;
4. W testifies there has been adequate research into specific application of image enhancement technology involved in case;
5. W testifies that software used was developed from the research;
6. W received a film photograph;

7. W digitized photo using proper procedure then used proper procedure to enhance it by computer;
8. W identifies trial exhibit as the product of the enchantment process s/he performed.

TIP: Courts willing to think outside box to recognize new authentication methods:

- (1) some have held that **documents provided to a party during discovery** by opposing party presumed authentic – shift burden to producing party to demonstrate that evidence they produced was not authentic. *Indianapolis Minority Contractors Ass’n.*, 1998 WL 1988826 (S.D. Ind.) Rationale is that the act of production is an implicit authentication of documents produced.
- (2) Re **contents of website** – N.D. Illinois admitted printout of Δ’s website based on affidavit from a rep of Internet Archive Company, which retrieved copies of the website as it appeared at relevant dates to the litigation through its so-called “wayback machine” – a process it uses to allow website visitors to search for archived web pages of organizations. *Telewizja Polksa USA v. Echostar*, 2004 WL 2367740 (N.D. Ill)

e. Self-Authentication – Rule 902

1. Extrinsic evidence of authenticity is not required for:

- i.** Domestic & foreign public documents under seal or purporting to bear signature in official capacity of government officer or EE
- ii.** Certified copies of public records
 - A. E.g: tax returns, weather bureau records, military records, social security records, INS records, VA records, official records form federal, state and local agencies, judicial records, correctional records, law enforcement records
- iii.** Official publications (e.g. printouts from Census bureau website)
- iv.** Newspapers and periodicals
- v.** Trade inscriptions and the like
- vi.** Acknowledged documents
- vii.** Commercial paper and related documents

2. Advantages:

- i.** No sponsoring W required; admissibility determined simply by examining the evidence;
- ii.** No need to show that computer system producing records was reliable or records accurate!

III. HEARSAY (Rules 801-807)

- a. Hearsay issues pervasive when ESI evidence is introduced.
- b. To properly analyze 5 questions must be answered:
 1. Does the evidence constitute a “statement”? Oral or written assertion, or nonverbal conduct of a person, if intended by person as an assertion.
 2. Was the statement made by a “declarant”?
 3. Is it being offered to prove the truth of its contents?
 4. Is the statement excluded from the definition of hearsay [Rule 801(1)]?
 - i. **Prior inconsistent “testimonial statements”** under oath excluded:
 - A. prior consistent statements offered to rebut express or implied allegation of recent fabrication, or improper influence/motive
 - B. statements of ID of a person made after perceiving that person.
 - C. Admissions by Party Opponent
 - i. Express, adopted, authorized or co-conspirator
 - ii. Must be offered against that party, cannot offer own out of court statements as admissions.
 5. If statement is hearsay, is it covered by one of the hearsay exceptions?
 - i. *Most often used -- exceptions dealing with perceptions, observations, state of mind, intent and sensation.*
 - A. Present sense impressions. Near simultaneous expression of explanation or description of event with its perception - militates against any memory deficiency, or opportunity to intentionally misstate what occurred.
 - B. Excited utterances. Statement relating to a startling event or condition made while declarant under stress of excitement caused by the event or condition.
 - Ubiquity of cell phones, Blackberries, etc. enhances ability to rapidly send messages describing events as they happen.
 - C. Then existing mental, emotional, or physical condition. Includes intent, plan, motive, design, mental feeling, pain, bodily health.
 - Particularly useful re email evidence - prone to candid statements of state of mind, feelings, emotions and motives
 - D. Business records.
 - Foundational Elements Required:
 - i. prepared in the normal course of business;

- ii. at or near the time of the events it records;
- iii. Based on personal knowledge of entrant/informant who had a business duty to transmit info to entrant;
- iv. Made in regular course of regularly conducted business activity, for which it was regular practice of business to maintain a memorandum

➤ **Courts differ on rigorousness of showing needed**

- i. Some have required showing that electronic record retrieved from computer files was the same one as originally entered into its computer
 - Focus not on circumstances of creation, but on circumstances of preservation - so as to assure document being proffered is the same as the one originally created.
- ii. Others have used much more relaxed standard. *U.S. v. Kassimu*, 2006 WL 1880335 (5th Cir. 2006)
 - Neither maker of record nor even custodian required, just a W qualified to explain the record keeping system of organization

IV. THE “BEST EVIDENCE” / ORIGINAL WRITING RULE (Rules 1001-1008)

- a. Rule requires an original or duplicate original to prove contents of a writing, recording or photograph unless secondary evidence is deemed acceptable.

Example Laughner v. State, 769 N.E.2d 1147 (Ind. Ct. App. 2002):

Δ charged with attempted child solicitation. State offered printouts of IM chats between Δ and undercover PO posing as a 13 YO boy. PO “cut-and-pasted” the text of IMs from internet chat room into a word processing program; printouts that were introduced into evidence were prepared from that program. Δ objected that printouts were not “original” text of IMs. Court agreed that state was proving content of a writing, and that the original writing rule required an original, but found the printout was an original, reasoning “According to [the PO] he saved the conversations with Δ after they were concluded, and the printout document accurately reflected the content of those conversations. Therefore, the printouts could be found to be the ‘best evidence’ of the conversations btw Δ and the PO.”

- b. **Rule 1003** - duplicates co-extensively admissible as originals, unless genuine issue exists re authenticity of original or circumstances indicate it would be unfair to admit duplicate in lieu of original.
 - 1. Thus, duplicates are more often admitted into evidence than originals.
 - 2. Also note that the “original” of information stored in a computer is the readable display of the information on the computer screen, the hard drive or other source where it is stored, as well as any printout or output that may be read, so long as it accurately reflects the data.

V. UNFAIR PREJUDICE?

- a. *Is the probative value of the ESI substantially outweighed by the danger of unfair prejudice or other factors such that it should be excluded despite its relevance?*
- b. Courts particularly likely to consider whether admission of ESI would be unduly prejudicial in the following circumstances:
 1. Evidence contains offensive or highly derogatory language that may provoke an emotional response;
 2. When analyzing computer animations, to determine if there is a substantial risk that the jury may mistake them for the actual events in the litigation, *Friend v. Time Manufacturing Co.*, 2006 WL 2135807 at * 7 (D. Ariz. 2006).