ESTABLISHING AUTHENTICITY AND SATISFYING THE BEST EVIDENCE RULE: NOT AN INSURMOUNTABLE CHALLENGE

In determining when electronic/digital evidence is admissible, the Courts go through the same type of analysis they do for "paper" documents and records. Those tests are: 1) Relevance, 2) Authenticity, 3) Hearsay, 4) Original writing or duplicate, and 5) ER 403 "unfair prejudice."

This analysis to follow will focus primarily on the authenticity and the "best evidence" or original writing issues, as they are the most distinctive area where treatment of ES1 and paper records is comparable, yet contrasting.

AUTHENTICATION

The threshold question in dealing with ESI/evidence or social media in court is authenticity. A party seeking to admit an exhibit need only make a prima facie showing that it is what he or she claims it is. ER 901 lists various means by which evidence can be authenticated. ER 901(10) specifically deals with email.

> Electronic Mail (E-mail). Testimony by a person with knowledge that (i) the e-mail purports to be authored or created by the particular sender or the sender's agent; (ii) the e-mail purports to be sent from an e-mail address associated with the particular sender or the sender's agent; and (iii) the appearance, contents, substance, internal patterns, or other distinctive characteristics of the e-mail, taken in conjunction with the circumstances, are sufficient to support a finding that the e-mail in question is what the proponent claims.

The federal rules are not as specific on this issue, as Federal Rule 901 provides that evidence can be authenticated by testimony of a witness with knowledge "that an item is what it is claimed to be." Fed. R. Evid. 901(b)(1). In *United States v. Kilpatrick*, 10-20403, 2012 WL 3236727 (E.D. Mich. Aug. 7, 2012), in a racketeering and conspiracy case involving Detroit city officials, the court granted the government's motion *in limine* for pretrial determination of authenticity of text messages sent on city-issued SkyTel pagers. Of the several authentication

methods used by the government and approved of by the court, the government presented the sworn declaration of SkyTel's records custodian who described the process of sending and receiving text messages, the manner in which text messages were archived on SkyTel servers, the process of retrieving the texts from company servers to comply with government subpoenas, and the method of generating spreadsheet data listing the text messages in preparation for trial. *Id*. at *4.

Text messages are treated much like email. Generally, there is a "phone dump" where all the text messages are downloaded and a verbatim report is issued. Also, emails of screenshots of text messages are admissible. *See e.g. In re the Detention of H.N.*, 188 Wn.App. 744, 753-61 (2015). In *State v. Bradford*, 175 Wn. App. 926 (2013), the Court applied ER 901(a) to the text message report and concluded sufficient proof was introduced to support a finding that the matter in question was what the proponent claimed. It is noteworthy that the text messages were on a phone of the person who received them, not the phone from which they were sent. They were authenticated by circumstantial evidence. For example, such as that the threats in the text messages were similar to those made verbally around the same time.[1]

Rule 901 has also supported a court's decision to authenticate screenshots of a website that included information about a defendant's online drug distribution scheme. *United States v. Bansal*, 663 F.3d 634 (3d Cir. 2011) *cert. denied*, 132 S. Ct. 2700, 183 L. Ed. 2d 58 (2012) and *cert. denied*, 133 S. Ct. 225 (2012). In *Bansal*, the government presented screenshots of defendant's website, which had been archived by a company called the Internet Archive, operators of the website The Wayback Machine, which archives prior versions of websites. *Id*. at 667. To authenticate the

[1] Also noteworthy was the fact that the text messages stopped coming during a 2-week period when the defendant was in jail with no cell phone access and resumed the day after he was released.

screenshots, the government presented a witness who testified to the validity and reliability of the Wayback Machine's archival database. *Id*. The witness also compared the images to previously authenticated and admitted screenshots of defendant's website and found the screenshots to be authentic. *Id*. at 668.

Both the Washington and the corresponding federal rule provide that evidence can be authenticated by "the appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances." See ER 901(b)(4) and, as noted, ER 901(10) provides the authentication formula to be used in State Court. It is well established that Rule 901(b)(4) is applicable to authenticating emails. *See e.g, United States v. Safavian*, 435 F. Supp. 2d 36 (D.D.C. 2006) (emails satisfied authentication requirements, despite the possibility of alteration, where emails bore distinctive characteristics, including actual e-mail addresses containing the name of the person connected to the address, signatures within the emails linking the emails to the alleged sender, and discussions in the emails of personal and professional matters known to be associated with the senders).

In *Safavian*, the court further held that e-mails that were not clearly identifiable by their addresses were identifiable by reference to their content. *Id*.; *see also United States v. Fluker*, 698 F.3d 988, 1000 (7th Cir. 2012) (in addition to circumstantial evidence contained in the email addresses themselves, the content of the emails demonstrated that the email's author had significant knowledge of matters the alleged author would have known about). *But see Jimena v. UBS AG Bank, Inc*., 1:07-CV-00367-OWW, 2011 WL 2551413 (E.D. Cal. June 27, 2011) (in a case alleging fraud against Chief Financial Officer at UBS AG Bank in a variant of the well-known "Nigerian advance fee scheme," the court found that there was inadequate foundation to support plaintiff 's claims that the alleged author of emails, USB's CFO, was in fact the true author when

emails sent to plaintiff were "unsolicited, contain[ed] only publicly available, self-serving information, and [contained no] substantive or unique information that support[ed] authenticity").

A similar process for authentication applies to text messages and online chats. *See State v. Bradford, supra*. *See also United States v. Teran*, 11-4791, 2012 WL 5359505 (4th Cir. Nov. 1, 2012) (finding no error when the evidence of defendant's text messages threatening the recipient of the text messages and his family were admissible when the recipient testified to the personal nature of the messages and showed how they aligned with defendant's knowledge of recipient's family); *Kilpatrick*, 2012 WL 3236727, at *4 (finding text messages made on SkyTel pagers were properly authenticated by distinctive characteristics including auto signatures, nicknames used, recognized phrases in signature lines and other personal information confirming the identity of the sender and by defendants' admissions that they regularly communicated with each other by text message on the SkyTel pagers); *United States v. Sterlin*, 466 F. App'x 792, 797 (11th Cir. 2012), *cert. denied*, 133 S. Ct. 452 (2012), and *cert. denied*, 133 S. Ct. 453 (2012) (noting that while there was no specific rule for text messages under Rule 901 like there is for telephone conversations, see Fed. R. Evid. 901(b)(6), text messages were otherwise authenticated by investigating agent who identified the numbers, matched them to defendants, and demonstrated that text message from one defendant referenced a traffic stop and search of other defendant's car the previous day); *United States v. Lundy*, 676 F.3d 444 (5th Cir. 2012) (testimony from law enforcement officer about transcripts of online chats he witnessed and recorded between defendant and a person defendant believed to be a 15 year-old girl was sufficient to authenticate the chats to support their admission in prosecution for attempting to persuade, induce, and entice a minor to engage in illegal sexual activity).

Additionally, Rule 902 of both the Superior Court and the Federal Rules provide that extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to some materials which are self-authenticationing. At least two types of materials covered in Rule 902 are potentially relevant to ESI in general. Rule 902(6) provides that newspapers and periodicals are self-authenticating. Under the 2011 Amendments to the Federal Rules of Evidence, Rule 902(6)'s reference to printed material now includes written material that exists online without the requirement that such material actually be "printed." *See* Gregory P. Joseph, *Internet and Email Evidence, Part 1*, The Practical Lawyer, Feb. 2012, at 22; *see also Ciampi v. City of Palo Alto*, 790 F. Supp. 2d 1077, 1091 (N.D. Cal. 2011) (finding that copies of newspapers, as well as print-outs of internet publications, that Plaintiff submitted in support of her defamation claim were admissible where the printouts contained "sufficient indicia of authenticity, including distinctive newspaper and website designs, dates of publication, page numbers, and web addresses," but declining to admit those printouts that did not include web addresses or dates). The corresponding Washington Evidence rule, ER 902(f), does not contain the specificity of its federal counterpart. Nonetheless, a proffer of online text or "news" items and online periodicals using the federal approach, as in *Ciampi*, may well succeed.

REQUIREMENT OF THE "ORIGINAL"

According to Federal Rule of Evidence 1003, an "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An "original" of a photograph includes the negative or any print therefrom and if data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original." The "original" of information stored in a computer is further specified in the Federal Rule of Evidence, 1001 (d). The position of the Federal Law in US is therefore adequate, as the Rules reflect the electronic evidence and covers the realities of change in information media from print formats to electronic presentation. Washington evidentiary rules are not close to this level of sophistication, but it can be anticipated that State Court judge-made law will be consistent.

Also in the case of **Laughner v. State**, 769 NE2d 1147 (Ind. Ct. App. 2002), a ruling came down that recognized content from internet chat rooms that was copied and pasted into word processing document as original writing vis-à-vis the original writing rule. In *Laughner*, an undercover officer was able to support the prosecution of an adult soliciting sex from children by posing as a child in a chat room, then copying and pasting the text content of their chats into word document. This material was subsequently printed and entered into evidence. The court interpreted the Federal Rules of Evidence to include any textual representation of information as long as it proves the content of the original document – electronic or physical.

While it is technically feasible to capture social media at a forensic level, often mirror images of a hard drive and screenshots of web pages will overcome a "best evidence" (now called the "original document rule") objection. For example, the most common way to present "text" messages as trial evidence is through a printout of a device's text messages. Such a "document"

has been deemed an admissible "duplicate" under Rule 1003. *See, e.g., United States v. Nobrega*, 2011 U.S. Dist. LESIX 55271 (D. Me.) In *Nobrega*, the court admitted a print out of an online chat session.

Finally, it is important to keep in mind that failure to properly object to the introduction of electronic evidence in any form as a violation of the original document rule will likely be considered a waiver on appeal. *Lorraine v. Markel American Insurance Co*., 241 F.R.D. 534, 579 (D.MD. 2007)