Electronic Evidence: Can you lay a foundation for ESI?

By Virginia Jo Dunlap, Esq.

and

Robert Blatt, MIT, LIT

August 2009

Contact:
Blatt@eid-inc.com
(805) 529 - 0600
www.eid-inc.com

Contact:
Dunlap@eid-inc.com
(916) 838 - 6917
www.eid-inc.com

Are you ready for challenges to authenticity and the weight that should be accorded ESI in your case?

At no time since the inception of the rules of evidence has the question of foundation and authentication of evidence been more ripe for challenge than in today's technologically advanced era. We have an evidentiary system rooted in the past, founded on the idea that evidence was physical and could be examined to determine its authenticity – i.e. a witness reviewing a document and attesting to its genuineness because of its physical characteristics such as a recognizable signature. But, we have moved into an age where it is more likely that even if a document began as a hard copy it will have been stored electronically and who can really say if it is the same after it has been stored as bits of electronic confetti, so to speak?

Legislators, courts and litigators have been focused on discovery issues – the new electronic discovery rules in California and at the federal level have garnered much attention and caused much discussion around the fairest methods for obtaining the electronically stored information (ESI) from an opponent. However, the next battleground will be laying proper foundations for introduction and authentication of the ESI evidence. How do you get that electronic evidence crucial to your case before the trier of fact and what arguments do you have to exclude your opponent's evidence?

What do you know about how the ESI was maintained before it was produced?

Learning how your client (or your opposition) has stored the ESI can, not only provide you the ability to determine whether you have received all available ESI but also, provide you with keys to making (or opposing) foundational arguments. And, even if the evidence is admitted over the objection, understanding that the ESI evidence may have been maintained in a less than trustworthy environment can shape arguments to the trier of fact that a particular piece of evidence should be given less weight since its integrity is at issue.

Because there is no legal definition of what a trustworthy or trusted system is courts will undoubtedly look to industry best practices for definition. In fact, the California Legislature has already deemed that official public entity records must be stored in a trusted system. Rather than provide specific standards for defining what a trusted system is, the legislation relies upon the industry standards created by the Association for Information and Image Management (AIIM) and ANSI. (*See* Gov't Code §§12168.7 and 14756.) In June of 2009, AIIM released a revision to the industry best practices that added a section specifying the elements necessary to establish a trusted ESI or document management system. (*See* Association for Information and Image Management, ARP-1 (2009) sec. 5.3.3)[1]

So, whether you are trying to enforce an arbitration agreement or introduce a key medical record into evidence, understanding whether it was stored as ESI and being familiar with the best practices of how that information was maintained can provide additional tools to a litigator who is faced with introducing that evidence.

ARP-1 (2009) Provides Industry Standards for defining how a trusted ESI system should be maintained

As Section 5.3.3. of ARP-1 (2009) states, a document management system must have several key components in order to be considered a trusted system. Security and multiple copies are two pieces of the puzzle, but so is having a combination of media, hardware and software that prevents unauthorized alterations, an ability to independently verify the storage processes through audits, and policies and procedures to support the system. It does little good to have designed the best storage system in the world and then fail to use it properly.

> ***A trusted document management system ensures that that all electronically stored information can be considered to be a true and accurate copy of the original information received regardless of original format.***
>
> ~ ARP-1 (2009) §5.3.3

Security and Location of the ESI

In addition to prohibiting access from outside the organization, consideration must have been given to who has access to the ESI from within the organization and where and how it is stored.

To meet the best practices, as identified in section 5.3.3 of ARP-1 (2009), a trusted system must generate two separate copies of ESI when it is created. And, that "[t]he trusted document management system must write at least one copy of the electronic document or record into electronic media that does not permit additions, deletions, or changes to the original document and that is to be stored and maintained in a safe and separate location."

For example, it would not be within industry best practices to have a system that when a hard copy document is scanned it generates only one copy that is later backed up through the disaster recovery protocol. Industry experts believe that by generating multiple copies to separate locations at the time the electronic document is created substantially reduces the risk of failure, loss, or alteration of the original electronic document so as to better protect the integrity of the information stored.

Integrity of the Information

By requiring the storage of information in a system that uses hardware and media methodologies to prevent "additions, modifications, or deletion" ARP-1 (2009) has captured the concept that users must have confidence in the accuracy of the stored information. A document management system that does not provide the users with confidence that the information put into the system may be regenerated accurately is subject to challenge.

For example, in the context of producing records for a litigation request, a witness must be able to verify that the documents generated were "true and accurate" copies of the documents maintained. Absent being able

to testify that additions, modifications or deletion of records are systemically prevented doubt may be cast on the credibility of the witness.

The standard setting committee that developed ARP-1 (2009) left latitude for designers to create a system utilizing hardware, software and media that best meets the needs the particular business organization, so there is no one way to ensure integrity. For example, an entity that modifies its original document throughout the course of the document lifecycle by appending information may have an entirely different design to its system than an entity that simply needs to maintain the original information. Regardless of how each system is crafted, it must consider preserving the integrity from the original source.

Audit Trails & Historical Data

Another important aspect to the overall document management system is having an independently verifiable audit trail that can demonstrate the ESI has not been altered inappropriately. Once again, this provides added confidence to the end user that the documents maintained and/or generated from the system are accurate. The level of information that is available within document management systems can vary from data indicating who opened and printed a document, to data showing who took what actions including workflow notations and/or routing to other users for review/processing. Being able to demonstrate reliability is directly related to both security and appropriate levels of all forms of historical data that comprise the various audit trails.

Policies and Procedures

The final component identified as a best practice in a trusted document management system is the creation of and use of policies and procedures to support the system. It does little good for a document management system to be created if there are no guidelines for the type of information to be stored or identifying what methodology will be used to generate ESI. From a litigator's perspective, understanding what policies and procedures are in place and testing the application of those procedures in practice can assist in bolstering or discrediting a claim that the ESI is reliable.

Conclusion

Litigators and judges are beginning to acknowledge the idea that just because electronically stored information is produced in court in a hard copy format, it does not logically follow that it may be judged by the same standards of reliability and admissibility applied even 10 years ago. Because of the manner in which ESI is stored, at worst the evidence may be excluded[2] and at best argued to the trier of fact that it lacks credibility. Understanding the industry best practices related to storage of ESI can be a powerful tool for litigators in preparing any case today where ESI is involved.

[1]A complete copy of ARP-1 (2009) may be obtained from www.eid-inc.com
[2]*In re: Vee Vinhnee* 336 B.R. 437 (B.A.P. 9th Cir. 2005) where evidence was excluded because the creditor (American Express) could not lay a proper foundation for the electronic evidence of the debt allegedly owed. *See also Lorraine v. Markel American Insurance Co.* 241 F.R.D. 534 (D. MD 2007) cross motions for summary judgment were denied for failure to address evidentiary issues with electronic evidence.

About the authors

Virginia Jo Dunlap, a former insurance defense litigator, who as a securities lawyer developed processes along with Mr. Blatt to allow for review and analysis of large volumes of ESI in large-scale investigations and cases. She also served in executive positions where, in part, she was responsible for developing policies addressing corporate ESI issues. She currently provides ESI risk assessments and ESI forensics through EID, Inc. and leads the standards committee developing guidance for design of trustworthy document management systems.

Robert Blatt has more than two decades of experience helping clients with content management and workflow issues through the analysis, design and implementation of Electronic Content Management (ECM) systems. He is the president of EID, Inc. and is a recognized national and international subject matter expert in the ECM industry, chairing AIIM's subcommittee responsible for updating ARP-1 best practices regarding a trustworthy system for ESI.