Authenticating E-Discovery As Evidence

The Editor interviews **Tom Klaff,** *CEO of Surety, LLC.*

Since the e-discovery amendments to the Federal Rules of Civil Procedure went into effect in December 2006, much has been said about the need for organizations to produce *electronic evidence (including email, instant messaging (IM) logs and other electronically stored information) during litigation, but since that time a new issue has emerged: can that e-discovery be* authenticated *to establish that it is what you say it is and ensure it gets admitted into evidence?*

Recent precedent confirms that courts are requiring rigorous electronic record authentication. In Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534 (D. Md. 2007), United States Magistrate Judge Paul W. Grimm refused to allow either party to offer emails in evidence to support their summary judgment motions, finding that they failed to meet any of the standards for admission under the Federal Rules of Evidence. The emails were not authenticated but simply attached to the parties' motions as exhibits, as has become common practice. Magistrate Judge Grimm opined: "If it is critical to the success of your case to admit into evidence computer stored records, it would be prudent to plan to authenticate the record by the most rigorous standard that may be applied."*

The Editor spoke to Tom Klaff, CEO of Reston, Va.-based IT security software company Surety, LLC, to discuss authentication issues surrounding electronic records. Surety operates a trusted third-party time-stamping service (often termed a "digital notary"), called AbsoluteProof, that enables its customers to legally defend the authenticity of their electronic records.

Editor: Why is authentication becoming such a hot issue?

Klaff: I've seen statistics that indicate that more than 93 percent of all corporate data is created electronically, and equally alarming statistics which indicate that more than 80 percent of all security breaches and electronic record tampering occur inside an organization's perimeter. Coupled with the e-discovery amendments to the Federal Rules of Civil Procedure and a few high profile cases involving the tampering of electronic evidence, evidentiary questions surrounding electronically stored information (ESI) are taking the limelight.

Tom Klaff

__Tom Klaff__ is the CEO of Surety, bringing over fifteen years of high-tech management experience to the company, most recently as Founder and CEO of Reliacast, Inc., a leading digital media software company. Prior to Reliacast, Mr. Klaff founded College Town, Inc., the first web portal for college admission widely used by students to purchase college-related items and to apply for financial aid. After College Town, Mr. Klaff established a management consulting firm to provide contract marketing and sales services to Internet-centric businesses. In that capacity, he developed strategic marketing and sales plans, managed large projects and helped his clients build an effective sales force. Mr. Klaff received a Bachelor of Arts degree in English from Brown University and a Masters of Science in Industrial Administration from the Graduate School of Industrial Administration, Carnegie Mellon University.

As a result, now more than ever, organizations have a much greater obligation to ensure that their electronic records are secured in their original state without alteration. Courts are requiring organizations to prove, irrefutably, that their electronic evidence – including trade secrets, legal documents, accounting records, emails, IM logs and image files – and its associated metadata were never deleted or altered any time during the life of the document. The problem is that electronic records, including imaged files, can be easily deleted, altered or manipulated by anyone with motivation and minimal tech-savvy.

Editor: You mentioned the e-discovery changes to the Federal Rules of Civil Procedure. Specifically, how does authentication figure into these changes?

Klaff: Rule 34 governs requests for production of documents. Under the amendments, parties are required to address the issue of the form in which ESI will be produced (e.g., TIFF, PDF, native, etc.). The requesting party has the option to specify a preferred form, and gives the producing party the option to object to the requested form and suggest its own preference. In the event of a dispute, the court will be required to resolve it. Interestingly, the new amendments provide that if the requesting party does not specify the form for producing ESI, it is incumbent upon the responding party to produce the information in a form or forms which are "reasonably usable" or in which the information is "ordinarily maintained." "Ordinarily maintained" generally means in its "native" format.

Authentication becomes a critical issue when dealing with native electronic records. Whenever a native file is opened, the metadata associated with that record changes to reflect the time that file was opened and by whom. Technically, the file was altered, resulting in a chain of custody issues. Based on the Federal Rules of Evidence, companies must be able to prove that throughout a record's chain of custody, its intended content and metadata are pristine. If they are unable to do this, the file may not be legally admissible.

One way to remove all metadata from electronic evidence is to print and store redundant copies of each native file, but this is costly, burdensome and would require an unimaginable amount of space to achieve. Beyond this, the printed records would be prone to forgery and spoliation. Alternatively, record managers could also convert each file into image files, such as TIFF or PDF, but those file formats can be easily compromised with commercial off-the-shelf software.

Trusted time-stamping cryptographically seals native electronic records, proving to all stakeholders, even during the e-discovery and review process, that the file and its metadata were never altered, even when opened.

Editor: How hard is it to alter electronic records?

Klaff: It isn't hard at all. Email chains can be edited when they are forwarded or replied to, permanently altering the record. Motivated insiders with access to software products like PDFcracker.com can easily compromise those documents.

On our Web site, we maintain a Wall of Shame filled with horror stories from various sectors where critical electronic records have been manipulated. In June, a lawyer for Best Buy admitted that he altered TIFF imaged emails and a memo he handed over in the case, which certainly could end up costing the company millions more in fines.

Editor: What is a trusted digital time-stamp, and how does time-stamping answer the authentication question?

Klaff: An external or trusted time-stamp is a data-level security control that enables organizations to unquestionably prove the authenticity of their electronic records. Trusted timestamps associate a reliable time-value with a document and can be requested at any point in an organization's electronic record workflow process – at data capture, generation, management or archive. When affixed to a digital record, trusted timestamps give an organization the ability to prove – independently from potential bias – that their electronic records existed at a specific point in time, and that people within the organization and outside the corporate perimeter neither altered nor backdated any electronic data.

Editor: Surety operates the AbsoluteProof trusted time-stamping service – how does it actually work?

Klaff: AbsoluteProof is an Internet-based service designed to provide independently verifiable, long-term proof of the content and time integrity of electronic records, making it ideally suited for organizations that rely on electronic records for legal, regulatory and other critical business processes.

When a document is time-stamped with AbsoluteProof, the service creates a hash or "fingerprint" of the file, a time-stamp token, and unique identifiers. These are "packaged" within the Surety Integrity Seal (Seal) and reside in the organization's repository alongside the original electronic document or within the metadata of the associated document.

AbsoluteProof is designed so that Surety never sees or handles the electronic record, alleviating any concern regarding the release of sensitive data to an outside party. During the process, only a hash of the original document is transmitted to Surety and a Seal is returned to the client. The content of the electronic document cannot be determined from the Seal, nor can the document be reverse-engineered from its hash, thus preserving confidentiality and security.

Once created, the Seal is used to conclusively prove that the associated electronic record existed at a specific point in time and has not been altered since. This allows an organization to detect tampering or inadvertent altering of electronic data and to maintain verifiable evidence of data authenticity for the document's lifecycle.

Editor: Authentication issues around electronic evidence are fairly new. How well is the legal community addressing these issues with their clients, and how are you working with the law firms on these issues?

Klaff: E-discovery is certainly a top-of-mind consideration across legal and technology communities. Since the e-discovery amendments went into effect, I've personally met with dozens of litigators, corporate counsels, judges and executives from several litigation support and records management companies to talk about these issues. I recently saw a comment from an executive at one legal consulting firm predicting that every firm with a litigation practice will have its own e-discovery attorney who will help establish e-discovery best practices, advise clients on e-discovery and litigation readiness and manage the intersect between law and technology. I believe we'll see this prediction come true.

We're working closely with the legal community to educate the industry on the evidentiary issues associated with electronic evidence. There are specific authentication issues associated with producing electronic records that lawyers haven't had to deal with in the past. Because we've been dealing with data authentication issues for years, a significant number of e-discovery leaders have been coming to us for advice on how to advise their clients, and what processes need to change in order to ensure the admissibility of critical electronic evidence. The attorneys I've talked to are worried about chain-of-custody issues associated with the electronic records of their clients. Without a method to authenticate content and its associated metadata, attorneys run the risk of losing the ability to enter key electronic records into evidence.

Please email the interviewee at tklaff@surety.com with questions about this interview.