BEST'S REVIEW
July 2008

Timing Is Everything

Under emerging court rules, insurers' digital content must be meticulously maintained to be used as evidence.

by T. S. Glassey

Illustration by Angel M. Negron

Years ago, all business processes were essentially based on first-person testimony. Someone took a paper which said something to another party, and that paper was granted legal status.

In today's world, that isn't necessarily true anymore. For instance, a document being exchanged may be a collection of digital bits that exists only in a computer's data storage system. But if needed, digital content can be introduced as evidence in legal proceedings, just as paper has been for hundreds of years.

Both the source of the data being introduced, and the believability of the data, have become extremely important. Equally

Contributor T. S. Glassey is the chief scientist and founder of Certichron Inc. He may be reached at tglassey@earthlink.net.

▶ **What's Up:** More and more insurance cases rely on electronic evidence to defend against claims.

▶ **What's New:** Swamped with e-evidence, courts have laid out rigid requirements for e-data admissibility.

▶ **What's Next:** Risk managers must use new methods to produce and maintain e-records that clear these hurdles.

important is how that data is maintained, due to the emerging concept of "anti-data spoliation": keeping digital evidence in a pristine and unaltered state.

New evidence standards are necessary today because of the ease with which digital content can be destroyed or altered. Access to data creates a liability that risk managers and underwriters must factor into their operations to ensure that the terms of their underwriting contracts can be enforced in court.

Where did this curveball come from? Simple. The dominant factor is the new set of standards American courts use to determine to what evidence the courts will automatically grant "admissible digital evidence" status.

These new guidelines resulted from changes to the Federal Rules of Civil Procedure which took effect in December 2006. And they have manifest implications for underwriters because the insurance industry relies on the courts to resolve disputes.

Furthermore, based on mechanical changes in how interpersonal commerce occurs in today's electronic world, there is a significant impact on underwriting and risk modeling, which needs to be addressed at the policy language level. (Advances in technology now require end-users to be savvy even on international law and treaties.)

There is another effect on commerce, one that's based on the massive proliferation of intercommunication facilities. The global deployment of "mobile technologies"—phones, PDAs, iPods and more—and the spread of the merged voice-data network illustrate this very well. Today, the plethora of devices mandates a uniform evidence model across all insured parties' operations, to ensure that this vital information can be reviewed properly before the courts to protect insurance providers.

Electronic Discovery Emerges

With the recent rulings from the courts on e-discovery—compounded by the proliferation of mobile technologies into commercial operations—these changes mandate a new vision and methods for managing digital content as evidence.

As such, any new standard of care the courts may impose has a direct effect on the digital content used as evidence regarding events or organizations which are underwritten. To protect themselves and to provide external guidance for arbitrators, the courts are specifying proper management of digital content to prequalify electronic evidence for summary filings. At the same time, the courts are restricting poorly maintained or unauthenticated data. This means that in order to use digital logs and machine testimony, processes that comply with the new standards must be employed.

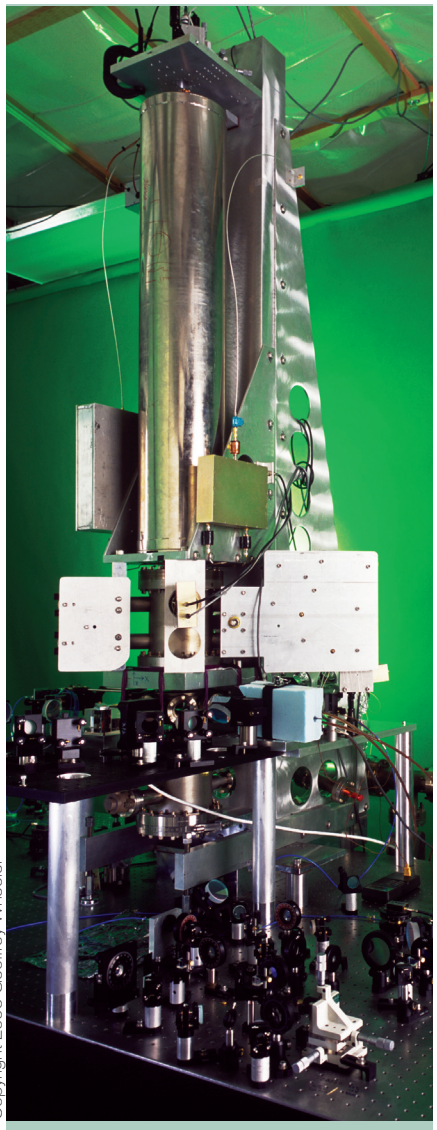
To auditors and underwriters, this means that for each system and each source of evidence it produces, five questions must be answered with regard to the control or evidence produced, specifically:

- **Relevance:** How is the evidence produced relevant to the assertion the evidence purports?
- **Authentication:** How is the content authenticated and how is the system that produces the data to be demonstrated as "fit for production"?
- **Hearsay**, if offered for truth: Which first-person or third-person digital testimony models will be used?
- **Original or Duplicate:** Is the evidence produced by a notified or a transaction system?
- **Probative Value:** Is the value of the evidence outweighed by prejudicial value?

The questions for risk managers are: First, how do these five rules apply to commercial processes and the records they produce; and next, what does that do to standards of care for the records those underwritten entities produce?

It appears that each system, process or internal control will have to be weighted with these five questions, and then reviewed as to how well it meets the needs of its designed purpose. This review process may resemble an extension of existing Sarbanes-Oxley-type reporting controls.

Being prepared for e-discovery is a new high-level requirement of risk modeling. This assures the underwriter that there is compliance with the policy's choice of law statement. This standard also



Copyright 2005 Geoffrey Wheeler

REAL TIME: A solution to meeting the new e-discovery readiness requirement is to run a uniform time base throughout all digital systems. But to implement acceptable time standards, global industries rely on the National Institute of Standards and Technology's new cesium fountain atomic clock. The clock uses a fountain-like movement of cesium atoms to determine the length of the second so accurately that—if it were to run continuously—it would neither lose nor gain one second in 80 million years.

pertains to the new concepts of e-discovery and its impact on the cost of liability insurance for federally regulated companies across the United States.

In one fell swoop, the courts did what SOX and HIPAA couldn't. The net effect is the creation of standards for the management and submission of content to the courts. They immediately affect any and all entities that could be prosecuted in U.S. courts, or use the courts to defend or advance civil claims. Judges have further interpreted these new rules to mean that maintenance standards of digital evidence are the same, whether the matter before the courts is criminal or civil in nature.

The Precedent Case

The courts have a legitimate need to protect themselves from being drowned in digital content. They must draw the line when awarding status to evidence; decide how it's to be authenticated; and issue maintenance requirements to continue the admissibility of that content.

And because originals can be copied or fictitious content easily created, the courts must have a Digital Content Admissibility Standard, the first of which emerged with the December 2006 updates to the Federal Rules of Civil Procedure.

A key case in U.S. District Court for Maryland, *Lorraine v. Markel American Insurance Co.*, last year set a standard for the admissibility of a number of types of digital data. Ruling for the court, Chief Magistrate Judge Paul W. Grimm held that data content that didn't meet or exceed certain standards would not be acceptable for summary rulings, but would require specific hearings and ultimately may be discounted as hearsay.

Grimm's ruling enforced and set actual standards for the management of digital content which could be admitted as evidence. It also set specific new data management and anti-spoliation requirements for digital content from a court's perspective.

His ruling admonished attorneys bringing digital content into court to "get it right the first time" and to ensure that their clients—those supplying the content in the first place—maintain it in a form that makes it possible for their attorneys to get it admitted as evidence.

This get-it-right-the-first-time mandate also directly pertains to risk profiling and underwriting liability operations within the insurance industry, and establishes a model for bonding as well as data-maintenance requirements for all warranties today.

The underwriting industry has new business opportunities in digital content underwriting as well as bonding and warranty programs; and for these opportunities, digital evidence and content standards are key to their success. Underwriters and risk managers need to evaluate the strength and controls of their evidence models, and then apply the final layer—the believability review—to determine if e-evidence gathered under prevailing systems is not only admissible but also believable in its detail.

One way of looking at these new requirements is to recall that many of the processes that individuals directly engage in today were previously done by some third-party who was responsible for process as well as delivery.

Today, technological systems have collapsed many of these functions; the individuals have been replaced but the process requirements still remain. By automating the handling and the management of data, we are keenly responsible for its proper storage and containment.

A solution to meeting this new e-discovery readiness requirement is to run a uniform time base throughout all digital systems. Being able to use the same time base as the core of each logging system would permit all of the entity's records to meet the same rigid requirements as the trading systems of yesterday.

In today's global network, insurers also must address global interoperability and synchronization requirements. The parties involved must agree on many basics, such as use of time scales (seconds, hours, days, zones); measurements (gallons, liters); and other standards for every place on the planet.

Generally, this is accomplished by using the International Bureau of Weights and Measures' guidance. But to implement acceptable time standards, global industries rely on the National Institute of Standards and Technology's new cesium fountain atomic clock, the most advanced timekeeping device in the world.

For instance, electronic time- and date-stamping in securities trading, which is required in the United States, is based on NIST-regulated time. NIST is the official keeper of American time and is incorporated into more than 130 Mutual Recognition Agreements for conformity between countries.

So from a commercial standpoint, the emerging need is for an interoperability framework to assure that time-of-day in transaction records is traceable. To that end, a NIST-based method is the only attestable metrological standard available.

That said, the reliance on unauthenticated and unlogged time services from anywhere, and especially ones which are not tracked with a formal time management practice, provide at best hearsay sources of time data. They should be avoided in commercial or underwriting operations.

With today's ever-changing technology, ways to meet these requirements now fit in the palm of one hand. Cell phones or other nomadic e-devices should be enabled to comply with the key treaties enabling international commerce.

The risk for failure to deal with this issue will continue to increase radically as mobile and personal devices become more and more integrated into everyday life. BR

Copyright © 2008 by A.M. Best Company, Inc. All Rights Reserved. Reprinted with Permission.