Published by Pike & Fischer, Inc., a subsidiary of The Bureau of National Affairs, Inc.

Digital Discovery & e-Evidence

BEST PRACTICES & EVOLVING LAW

Vol. 1, No. 9 | **October 2001**

Building Good Electronic Evidence

Now That E-Records Are Legal, Here's How to Make Them Reliable

Randolph A. Kahn, ESQ

With the passage of the Electronic Signatures in Global and National Commerce Act, the law is more settled than ever before: e-records are on par with their paper counterparts for most purposes and in most jurisdictions. While legal, however, the kinds of data compilations that companies often use may not necessarily protect their interests or properly document their business or governmental activities. In essence, having an electronic record is quite different from having a *complete, trustworthy* and *authentic* electronic record.

The world of e-records is replete with shades of gray. At one end of the spectrum, there are mere "compilations of data" that are not particularly useful. At the other are reliable electronic records that possess all the indicia of acceptable evidence. Simply put, the electronic world creates a variety of records—some good and some bad. As this article explores, merely satisfying the law may not be enough when retaining electronic evidence of e-business transactions.

Merely retaining the content of a transaction, without knowing the context for that content, serves as a largely useless record of that exchange. Paper records always have content merged with context: you know from the face of the document what something is and why it came into existence. For example, a purchase order on paper is one physical record. The date of execution, authorized party, subject, and any other contents that reveal its significance, are all clearly and collectively visible.

The electronic world is precisely the opposite. E-records usually consist of multiple packets of data that are rarely stored in one physical location. Quite often in cyberspace, the content is the only part of the record that is retained. That's the equivalent of taking a paper business letter, cutting off the date and salutation and putting it in one file, cut-

continued on page 2

Lawyers Look to Digital Millennium Copyright Act to Subpoena Pirates Without Suing

Gene J. Koprowski

Lawyers who represent movie and music producers—as well as non-fiction writers whose works are pirated on the Internet—are intensifying their use of a three-year-old discovery tool which gives them fact-finding power akin to that of criminal prosecutors.

Passed in 1998, the Digital Millennium Copyright Act (DMCA), 17 USC 512, provides attorneys for these creative artists, as well as any other individuals who believe their copyrighted works are being expropriated, with the ability to go to the clerk of the court of any federal courthouse and request that a subpoena be issued against the alleged copyright infringer. No lawsuit need be filed, providing a substantial savings to claimants. Moreover, if the alleged infringer does not comply with the terms of the subpoena—and identify the person who violated the copyright in an online posting of words or images or music—he can be held in contempt of court and imprisoned by a federal judge. Generally, in the past, only criminal prosecutors have had the power to issue subpoenas without filing a suit.

continued on page 4

Inside

Digital Discovery & e-Evidence

www.pf.com/digitaldisc.asp

Associate Group Publishers. . Carol L. Eoannou, ceannou@pf.com 800/255-8131 ext. 269

David Fialkoff, dfialkoff@pf.com 800/255-8131 ext. 246

Legal Editor . . . . . Quintin Chatman, qchatman@pf.com 800/255-8131 ext. 261

News Reporter . . . . . Marian Jarlenski, mjarlenski@pf.com 800/255-8131 ext. 232

Group Publishers . Thomas K. Billington, tbillington@pf.com 800/255-8131 ext. 243

Christopher H. Hoving, choving@pf.com 800/255-8131 ext. 245

Production. . . . . Colleen Gratzer
Walter Rust

Copy Editor . . . . . Marie Unger

Publisher: Pike & Fischer, Inc., a subsidiary of The Bureau of National Affairs, Inc., 1010 Wayne Avenue, Suite 1400, Silver Spring, MD 20910

Published monthly, except for August. ISSN: 1521-3285
Subscription rate: $649

POSTMASTER: Send address changes to: *Digital Discovery*, Pike & Fischer, Inc. 1010 Wayne Avenue, Suite 1400, Silver Spring, MD 20910

continued from page 1

ting off the signature and putting it in another file, and placing the body of the letter in yet another file. Separately, the units of those documents are rather useless for record-keeping purposes.

How E-Transactions Work

In the typical electronic transaction, the questions (the boxes that the user must fill out) are not physically retained with the answers (the data that the user types in). The answers would be a separate compilation of data and would most likely be stored in a separate physical space from the questions.

The reason for this lack of unity is simple to understand, but difficult to correct. The computing world was structured in a database-centric way to allow the parsing or separating out of information for various types of uses. Technologists were not thinking of building good business evidence. Therefore, the content of a record is almost never connected to the structure or form of the record unless the system is implemented to capture both. Technologists were promoting information functionality, not trustworthy electronic records.

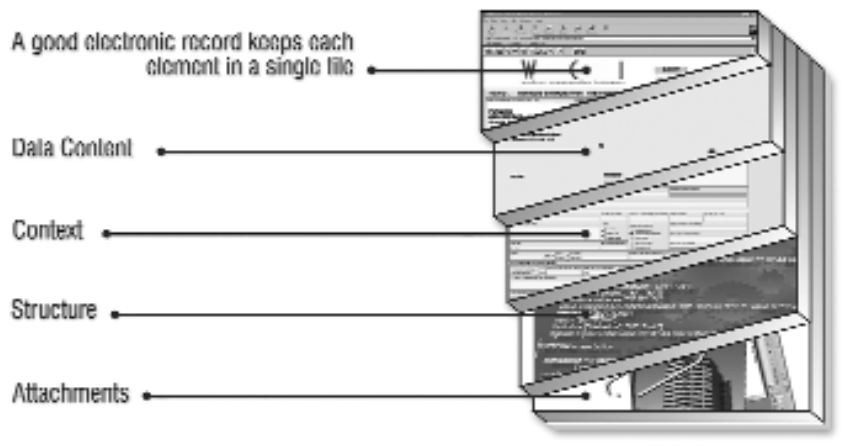
In today's online business world, the signature used to affix to an e-record will likely be in a separate system and most assuredly will be a separate computer file. If you need to prove a document was executed by a particular person, that individual's mere "signature" may not be enough.

First, a signature, according to electronic signature legislation recently enacted by Congress, may be nothing more than a typed name at the bottom of the document. Second, the name will not be affixed in the traditional sense of the word to the document. Therefore, metadata (data that manages data) is needed to link the questions with the signature. If the metadata has not been retained, proving assent to the terms of an agreement will be all but impossible. If metadata is retained, then if and when the "signer" seeks to repudiate the agreement or legitimately argues that he was the signer, metadata could be used to show the computer from which the "signature" was effectuated.

Put simply, in the electronic world, separate e-files stored in separate computers—perhaps stored in separate physical locations—together make up one record. To have one encapsulated record with the content, context, structure, metadata, e-signature, and logic requires that the record be built. Building the right record for the application is in part a technology decision, in part a legal decision, and in part a business decision.

Inherent Problems With E-Records

To further confound the process, the applications, formats or computer



languages that have become popular in the electronic age do not possess the ability to retain and structure records in a trustworthy way. For example, HTML (Hyper Text Markup Language) may be good for retaining content but is not very helpful in retaining the template (what people saw).

Needless to say, what people see has become more important than ever. According to the new privacy regulation for the securities industry, for example, notice of a brokerage's privacy policy must be "clear and conspicuous." It is wholly inadequate to discard or lose the precise privacy information that the customer reviewed. Such issues as retention of the form of the record that the customer viewed—and proving that the form at issue was the form in use when the transaction was completed—becomes central to prevailing. Changes to forms, fonts, colors, and software (unless backward compatible) can and will affect the look, size and appearance. Being able to deliver the precise record that was viewed and used has great utility not only with regard to SEC compliance (and compliance with other similar new regulations) but also lessens confusions and increases trust in the transaction effectuated.

What Makes Acceptable Evidence

Even if the new generation of e-records and e-signatures laws has been generous in not mandating the precise record to be retained, the fact remains that incomplete, untrustworthy records will be excluded from evidence or otherwise attacked as lacking integrity.

Certain regulations have been somewhat helpful to guide companies in building the right evidence to satisfy their regulatory environment. For example, the FDA electronic record/electronic signature rule advises that, when using an e-signature, metadata must be captured "linking" the signature to the record. To comply with FDA policies, a signature that isn't logically and/or physically linked to the underlying record fails to comply with the agency's rule. So, the applicable rules should be consulted to ensure that the e-records under construction will satisfy the relevant regulator.

Using Acceptable E-Signatures

The technologically neutral brand of laws that has evolved allows the use of any type of e-signature, provided that it evinces the users' intent to be bound by the alternative to the manual "wet signature." While that is good because businesses are free to use whatever type of technology they deem necessary under the circumstances, the fact remains that not all e-signatures are created equally. For example, "xxx" at the bottom of e-mail could be sufficient to satisfy the language of the federal law on electronic signatures (commonly known as E-Sign). However, it provides little verification of the signer's true identity. Truly anyone could use or "forge" such a signature. Authenticity in that case would clearly be an open question.

Similarly, a typed name at the bottom of the page would seem to satisfy E-Sign, but the same concerns around authenticity and trustworthiness would persist.

Some types of e-signatures, however, can better confirm that the signer is who he/she claims to be, thereby minimizing concerns about repudiation, contracting with minors, etc. Biometric signatures—unique physical attributes like eye scans, finger prints, or voice scans—would satisfy E-Sign *and* provide much greater comfort in the identity and integrity of the relationship. Similarly use of Digital Signatures (asymmetric cryptography or encryption sometimes referred to as Public Key Infrastructure "PKI") allows information to be sent in an encrypted form and secured during transmission, and also allows parties to "sign" a contract with the use of a "private key." Assuming there are controls in place regarding the issuance of the Digital Certificates, use of the key pairs, and access controls, a recipient of a documents signed with a Digital Signature can have greater comfort that the "signature" is authentic and that the user cannot easily repudiate the transaction. (*see inset*)

The Proper Safeguards

This discussion makes clear that all electronic signatures are not equal in their inherent security, or their ability to address issues of authenticity, trustworthiness, and repudiation. Utilizing electronic signatures will require controls and procedures to ensure that e-signatures are used properly and with authorization.

For example, if companies use ID and password in place of a handwritten signature on paper to allow employees to change the type of investment or beneficiary on their retirement plan, then controls around access to employees' identification and passwords will be critical to prove that the authorized employee—and not another person with access to the system—effectuated the change. Additionally, metadata will be crucial to show the computer or telephone

There is substantial confusion in the terminology surrounding electronic signatures. Laws and commentators often use the words electronic signatures and digital signature synonymously. They are not. *Electronic Signature* is the broad category that includes digital, digitized, biometric, ID, password, etc. *Digital Signature* involves asymmetric cryptography, which does not resemble a signature at all. Rather, Digital Signatures are code that use a mathematical algorithm to encrypt the message. Private and public key pairs are also used to indicate the identity of the holder of the private key. *Digitized Signature* is when you manually write your signature but the image is captured by a computer and can be subsequently affixed to a document. —R.K.

number where the change originated. Such ancillary information, if captured, can provide great support and evidence for the event. Failing to have the metadata makes authentication difficult, and may undermine the transaction by forcing a party to rely on a "signature" that can be easily challenged.

When making decisions regarding the type of electronic signatures utilized, companies should consider the need to rely on it in the future and the ability to prove identity and authenticity as well as to preempt issues that may arise regarding the veracity of the signature or true identity of the "signer." In that regard, there is a need to understand the relative merits of the various kinds of e-signatures to be able to make the right choice for the application at issue.

So here we are in a world that allows business to happen with the use of a telephone line and computer. Business and government function in an anonymous electronic fashion, where information free-flows around the globe and where business partners can be introduced on a third party exchange in cyberspace. The parties never meet and remain faceless to each other throughout their relationship. In such a world there is a profound need to have good evidence available to document business events.

There are a whole host of internal business processes (HR functions, Sales Information, e-filing with regulators, etc.) that are now conducted electronically. For each of those transactions, the objective should be to build the same kind of evidence that was relied upon in the paper world. If you need good records in the paper environment, then build them in the electronic world.

Technological solutions will continue to be offered to help bridge the trust gap that currently exists when doing electronic business. As companies and consumers grow comfortable doing business solely within an electronic environment, the size and value of transactions will increase. As the size and risk of transactions goes up, so too will the need to have trustworthy records memorializing the events and activities. While the law has allowed us to make choices, companies can ill afford to make bad decisions.

The task of building good e-evidence has to move quickly up companies' priority lists. Failing to retain acceptable and trustworthy electronic business records will have devastating consequences. Companies will spend enormous resources to store e-data that may not be useable or legally sound.

Randolph Kahn is vice president, Legal and Compliance Practices for PureEdge Solutions, Inc. He writes and speaks frequently as a legal expert in digital evidence, e-business, electronic records and signatures laws. Mr. Kahn can be reached by e-mail at <rkahn76867@aol.com>.

Lawyers Look to Digital Millennium Copyright Act

continued from page 1

Though the DCMA is something of a hodgepodge of statutory solutions to problems encountered by Internet Service Providers and digital firms during the late 1990s, the measure is a "good litigation tool" in that it helps copyright owners protect their works while avoiding litigation in a very large number of instances, according to Steve Englund, a partner who practices copyright law with the Northern Virginia office of the powerhouse law firm Arnold & Porter. "It is important to remember that while a handful of high profile copyright cases have attracted a lot of attention, on any given day there are thousands of FTP [file transfer protocol] or other sites distributing infringing copies of copyrighted software, motion pictures, music, and other works," says Englund. "These sites present no novel legal issues, but are clearly infringing. It is my impression that Section 512 has worked reasonably well, for both copyright owners and service providers, by providing a framework to work together to control this infringement without litigation or the threat of litigation."

The DCMA emerged when an array of companies whose works were being pirated online—from Hollywood producers to Silicon Valley software shops—were looking for a way to fight back. "Copyright infringement on the Internet often occurs in a manner such that the copyright holder does not know the identity of the person or entity that is posting copyrighted songs, movies or other information," explains Roy Goldberg, a partner at Schnader Harrison Segal & Lewis LLP. He has extensive experience in representing ad agencies and companies on copyright and trademark matters. "There are a myriad of ways that an infringer can conceal his or her identity, even when using a web site to disseminate the infringing material."

Before passage of the DMCA, Goldberg says, a copyright holder had little choice but to sue the Internet Service Provider (ISP) for contributory copyright infringement, or at least for injunctive relief to try to obtain the identity of the ISP's customer who was allegedly violating the copyright. "The subpoena provision in the DMCA enables the copyright holder to obtain the identity of the ISP's customer without having to sue the ISP. That is by and large a good thing," said Goldberg. "It also protects the ISP against a claim by its customer that it improperly disclosed the customer's identity because the ISP is under a court order to do so."

Another benefit of the act is that it gives attorneys the power to investigate cases that otherwise might be turned over to the FBI or federal prosecutors—or never resolved at all. "The realistic prospects of actually getting either the

FBI or a US attorney's office to act on criminal piracy cases is as close to zero as it's possible to get," insists Dave Powell, managing director of Copyright Control Services, an online service that helps company's track copyright violations.

Lawyers say that the provisions of the law regarding the issuance of subpoenas are very straightforward. The attorney for the claimant will follow a three-stop process to get the subpoena. First, he will write a letter to the clerk of the federal court, spelling out the allegations against the copyright infringer and the provisions of the law.

The letter must state the following: "This request is being made under the provisions of the Digital Millennium Copyright Act. The act states that a copyright owner, or a person authorized to act on the owner's behalf, may request that the clerk of any United States District Court issue a subpoena to a service provider for identification of an alleged infringer."

Once that letter is received by the clerk, he or a deputy will contact the lawyer's office, informing it that it can issue the subpoena, but that it must send a paralegal or secretary to the clerk's office to get the subpoena docketed and have a case file created. A judge is then assigned to the case, should there be a need for contempt hearings if the subpoena is ignored.

Lastly, the attorney can mail out the subpoena, as long as it is accompanied by a cease and desist letter indicating that a copyright violation civil suit will probably not be undertaken against the ISP if the name of the actual poster of the copyrighted material is provided within 21 days.

"The DMCA is a good litigation tool because it is designed to eliminate unnecessary litigation—not only by creating a "safe harbor" to protect Internet Service Providers from being sued for copyright infringement when they are innocent of any wrongdoing—but also to provide a mechanism where information can be obtained from the ISPs without having to sue them," comments Goldberg.

Some litigators, however, worry that the law gives copyright owners too much power, without judicial supervision. "Generally, only the government has the authority to subpoena information before a lawsuit is filed—through issuance of a Civil Investigative Demand (CID), and this power is subject to important restrictions," notes Englund. "We must remember that merely because a court clerk issues the subpoena does not mean that there is independent scrutiny by a judge before the subpoena is delivered to the ISP." He urges caution in using the power. "Otherwise, before we know it we will have a system of non-government entities acting like government entities, without being subjected to the restrictions imposed on agencies. This could have a snowball effect with unchecked power and privacy intrusions that explode out of control," says Englund.

But other attorneys disagree, respectfully. "Remember, the highly publicized legal battles to the death—i.e., *Napster* etc.—are the tip of the iceberg," reminds John Rapoport, an intellectual property attorney in New York. "Enhanced discovery in those cases is simply one more issue to use to protract the battle. In the vast majority of cases filed the parties are not looking to litigate into the next millennium. They merely want a resolution of a dispute."

Gene Koprowsk is an independent writer based in Chicago.

Document Management Guide

Records of Employee E-mail Widely Available, Although Employer Monitoring Measures Remain Controversial

Fear of lawsuits dictate employer practices

The majority of U.S. companies monitor employees' e-mail and Internet use, according to a survey released by the American Management Association.

The survey, *Workplace Monitoring & Surveillance: Policies and Practices*, revisited an earlier 2001 AMA survey with a follow-up questionnaire. The new report looks at the motivation, policies, and practice of computer surveillance by 435 employers of various sizes.

More than 60 percent of employers responding to the survey said they monitor Internet connections, and about 47 percent said they store and review employees' e-mail messages.

Legal liability, according to the respondents, is the most important reason to monitor employee use of e-mail and the Internet. Over two-thirds of respondents rated liability as having a high importance for monitoring.

Fifteen percent of surveyed companies said they had been involved in one or more legal issues related to computer use, such as receiving a subpoena for employee e-mail or defending a harassment claim based on employee e-mail and Internet use. Out of these companies, nearly 82 percent rated legal liability as an important reason to monitor employees.

Employers also are creating computer-use policies directed at Internet use, AMA said. Four out of 10 surveyed companies said they allow employees full and unrestricted use of office e-mail; only one in 10 allows the same access to the Internet.

"Companies are far more concerned with keeping explicit sexual content off their employees' screens than with any other content or matter," AMA said. More than three-fourths of the surveyed companies restrict sites with explicit sexual content, while entertainment, sport, and shopping sites are restricted by less than 20 percent of survey respondents.

When employees violate an e-policy, almost 80 percent of the companies previously involved in some legal action said they have taken disciplinary action, while fewer than half of other companies took disciplinary action. Overall, half of the surveyed employers said they took action when e-policies were violated.

"To reduce liabilities, protect corporate assets, and stay out of court, employers must manage employees' online behavior," said Nancy Flynn, executive director of The ePolicy Institute, the survey's co-sponsor. "Written e-policies and monitoring software are indispensable business tools for employers operating in the age of e-mail and the Internet." The ePolicy Institute is an online resource site that aims to help employers limit electronic risks through the development and implementation of effective e-mail, Internet, and software policies. A sample policy prepared by The ePolicy Institute accompanies this article.

According to AMA, 95 percent of companies that are actively monitoring employees have written policies, compared with 75 percent of those who do not monitor.

While the federal Electronic Communications Privacy Act gives employers the right to monitor company computer use, Flynn said, it will not "prevent outraged employees from filing invasion-of-privacy claims." She recommended that employers use written computer-use policies to notify employees that they cannot expect privacy, that the company has the right to monitor computer use, and that the company intends to exercise that right.

California Legislature Again Sends E-Mail Privacy Measure to Governor

Although e-mail monitoring seems to be a fact of corporate life, efforts to regulate it persist. In California, for example, the state legislature has sent Gov. Gray Davis (D), for the third time in as many years, a bill that seeks to prohibit employers from secretly monitoring employee electronic mail unless they first advise their employees of their privacy policies.

In each of the last two years, Davis has vetoed bills similar to this year's measure, S.B. 147 by Sen. Debra Bowen (D). This year's version is identical to last year's bill, S.B. 1822, which Davis vetoed, saying it increased regulatory burdens and legal liabilities on employers. Representatives of the governor tried to negotiate language that would be acceptable to Davis, but were unsuccessful.

Bowen's latest bill received final legislative approval Aug. 30 on party-line votes, with Democrats generally favoring it and Republicans opposed. It would amend the state Labor Code to provide that "[A]n employer may not secretly monitor the electronic mail or other computer records generated by an employee." However, the bill qualifies that prohibition by allowing employers to inspect or review electronic records and communications if they first inform employees either in print or electronically of their workplace privacy and electronic monitoring policies and practices.

Employees must acknowledge receipt of the policy under the measure. If an employee refuses to do so, the employer still may institute the monitoring policy if it documents that it has provided a copy of the policy to the employee.

Bowen likened the protections in her bill to prohibitions elsewhere in California law on secret monitoring of telephone conversations. S.B. 147 would create a similar "right-to-know" protection for employees who use computers, she said.

"More and more businesses are buying cheap, off-the-shelf 'spyware' to track employees' every click and keystroke to find out what employees are writing in e-mail messages, what Web sites they're visiting, and much more—all without the employee's knowledge," Bowen said. "The bill doesn't prevent a company from monitoring what its workers do; it simply makes sure people know they're going to be watched before they log on to their computer," she explained.

But major business groups strongly oppose S.B. 147. The California Chamber of Commerce warned that if S.B. 147 becomes law, an employer could be liable for criminal penalties if it inspected employee e-mail or computer records in a manner that did not comply with the privacy policy it disclosed to the employee. The California Manufacturing and Technology Association said the notification and verification provisions would be onerous for employers.

If it becomes law, Bowen's bill would apply to all private employers in California, and to public employers and the state's higher education system.

Judiciary Subject to Most Executive Branch Rules

Meanwhile, a recent warning to federal courts that computer use would be monitored set off a firestorm of debate this summer about whether judges and court employees had an expectation of privacy while using court computers. The federal courts started examining computer use by federal court employees, including judges, when they found the transferring of large files, mostly downloaded music, was clogging the computer network. As a result, on September 19, the Judicial Conference of the United States, the policy-making body of the federal court system, adopted most of the

same rules for computer and Internet use under which federal executive branch employees now live. One notable exception is the courts' omission of a provision of the executive branch rules that warns employees they should not have an expectation of privacy while using their workplace computers. Like other federal employees, however, those attached to the courts are officially prohibited from viewing pornography and downloading large music files under rules the recently-adopted rules.

Sample Employee Internet Usage Policy

As part of this organization's commitment to the utilization of new technologies, many/all of our employees have access to the Internet. To ensure compliance with copyright law, and protect ourselves from the threat of viruses and/or hacking into our server, the following is effective immediately:

1. It is (Organization's) policy to limit Internet access to official business. Employees are authorized to access the Internet for personal business after-hours, in strict compliance with the other terms of this policy. The introduction of viruses, or malicious tampering with any computer system, is expressly prohibited. Any such activity will immediately result in termination of employment.

2. Employees using (Organization's) accounts are acting as representatives of (Organization). As such, employees should act accordingly to avoid damaging the reputation of the organization.

3. Files are downloaded from the Internet must be scanned with virus detection software before installing or executing. All appropriate precautions should be taken to detect a virus and, if necessary, prevent its spread.

4. The truth or accuracy of information on the Internet and in e-mail should be considered suspect until confirmed by a separate (reliable) source.

5. Employees shall not place company material (copyrighted software, internal correspondence, etc.) on any publicly accessible Internet computer without proper permission.

6. Alternate Internet Service Provider connections to (Organization's) internal network are not permitted unless expressly authorized and properly protected by a firewall or other appropriate security device(s).

7. The Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third party. Employees must exercise caution and care when transferring such material in any form.

8. Unless otherwise noted, all software on the Internet should be considered copyrighted work. Therefore, employees are prohibited from downloading software and/or modifying any such files without permission from the copyright holder.

9. Any infringing activity by an employee may be the responsibility of the organization. Therefore, this organization may choose to hold the employee liable for the employee's actions.

10. This organization reserves the right to inspect an employee's computer system for violations of this policy.

I have read (organization's) Internet policy and agree to abide by it as consideration for my continued employment.. I understand violation of the above policy may result in my termination.

_____

Employee Signature

_____

Date

It's Not Your Father's Discovery: Paper and TIFF Responses Are on the Road to Obsolescence

Are you ready to produce native files and non-textual data?

It seems inevitable that requestors will eventually refuse to accept paper or even TIFF, when the source materials were born digital and maintained digitally in the ordinary course of business. How will your company fare when faced with a successful request for native e-mail and digital data in a format other than paper and/or TIFF? Will you be able to comply? How much risk will the corporation be exposed to as a result of compliance? How will you reference those electronic files? How will you authenticate them? How will you deal with files that do not contain text (e.g., voicemail, digital video, etc.) or that can't be reduced to paper (e.g., CAD drawings, etc.)?

Michael Prounis

Amendments to the Federal Rules of Civil Procedure require the producing party to affirmatively produce electronic files as part of the initial production of data, even in the absence of an explicit request. This change, made last December, will over time drive a wedge into the old boy's network of digital discovery practice, which has survived for years on the quid pro quo of "if you don't ask (for electronic data), I won't either." Compliance with this tacit understanding is a major reason why productions have largely persisted on paper or in TIFF, even as the digital age has advanced.

As we sail further into the new Millennium, however, this approach will sow the seeds of embarrassment (or worse) for unsuspecting legal support teams. Simply put, not asking for 100% of responsive data means ignoring a potential reservoir of important information.

The Technical Problem

Computer forensics has highlighted the differences between native files and their paper or TIFF renditions. Such differences include certain document properties (often referred to as metadata), comments appended to business documents (e.g., notes to word processing files and PowerPoint presentations), and formulae and hidden columns in spreadsheets. Failing to review and produce responsive content from an electronic file is a serious oversight that diminishes the credibility of your digital discovery and production process, on even the most basic cases.

Moreover, inadvertent modifications to source electronic files may be construed as intentional file alterations. These modifications result from merely opening a file, and certainly include such activities as eradicating viruses, making redactions, and expanding certain compressed file formats.

Yet, today the vast majority of e-mail and electronic data productions are amazingly paper-based. Parties often negotiate away their rights to the native files, often because they don't know what to do with the raw data and/or because they fear the double-edged nature of the digital discovery sword. Only in the current world of digital discovery can data born digital be produced as paper or TIFF, requiring the other side to rescan it using Optical Character Recognition (OCR) to make it searchable. (Clearly, if you can get your opponent to agree to that, take those terms every time!) But, how long will this state of affairs continue? The idea that paper or TIFF is an equivalent to native format or some widely accepted "rich text" file format (e.g., Portable Document Format ("PDF")) is likely to be harder and harder to sell, particularly as courts begin to only accept PDF filings of pleadings and other submissions.

What is the rationale for providing paper or TIFF when the subject documents were born digital? And since documents born digital can be searched digitally in their native state, why does providing a searchable format constitute an unfair benefit?

Most applications are automatically linked to some type of searching functionality. From an efficiency standpoint, the production of digital data in a paper or TIFF format is a non-starter. It fails to recognize the societal transformation that has taken place in the last 15 years. When the printing press became widely available, writing tablets and papyrus were abandoned. When the analog photocopier took hold, carbon paper was discarded. How can parties who benefit on a daily basis from the advancements of modern computer technology hope to justify the use of paper or TIFF production of digital discovery data? Again, if the other side will accept it, do it every time, but don't expect to win much sympathy from the court if your opponent demands a more flexible format. Moreover, don't act as if native files and paper/TIFF are completely identical; such an attitude can cost you and your client much in terms of credibility with respect to the completeness of your effort.

A Question of Completeness

Not only are they inefficient and costly, but paper and TIFF productions of digital discovery data may also be incomplete. TIFF images are merely pictures of a document. Moreover, there are major quality problems associated with the accuracy of any OCR text conversion of TIFF images of spreadsheets and other non-e-mail business documents necessary to make the TIFF files searchable. The typical OCR drivers used to convert

TIFF images to searchable text not only change the format of the original file, but also provide an unacceptable level of accuracy in terms of creating the searchable text component. Even with today's modern search engines, searching is far from a perfect research method. Studies going back to the mid-1980s highlight the problems of full-text searching, even when the accuracy of the source data is perfect. The ambiguities of the English language are considerable, and the research problem is compounded exponentially when the OCR converted source data may contain millions of errors. Twenty thousand pages scanned at a 97 percent accuracy level will contain approximately 1.2 million errors—and it is near impossible to achieve a 97 percent accuracy level when dealing with the non-e mail types of business documents (such as spreadsheets).

At least with PDF renderings of source digital discovery files, the conversion accuracy (from native format to PDF) improves by an order of magnitude and the document formatting problem completely disappears, as PDF maintains the look of the original electronic file. These are two of the key reasons for its adoption by the federal courts. But even PDF renderings may contain less complete information than the original file—paper and TIFF versions of source digital discovery data will surely be incomplete.

A paper print-out, TIFF image, or PDF file most likely was created using the print range last invoked by the creator of the document. This means that any comments that may exist in a word processing file, spreadsheet, or graphics presentation may have been excluded from the paper, TIFF, or PDF rendering of the file. Accordingly, when that image or piece of paper is searched manually or programmatically, it will contain less information that the original source file.

The foregoing is completely unrelated to the forensic world of deleted files or earlier versions of a file. At issue is what constitutes a final file and/or whether a print-out or TIFF image contains everything that the final version of the electronic file contains. For many types of digital document, this is a meaningful difference. Again, it could be certain comments contained in a word processing file, notes appended to a PowerPoint presentation, or hidden columns in a spreadsheet. Clearly, depending on the material at issue, forensic analysis can uncover a number of other differences. But, most cases do not warrant forensic analysis. And for those that do, there is a question of who should pay for it. The bottom line is that every case will have a digital discovery and production component, and the process you use to address it must be defendable and dependable.

Anticipate Increased Scrutiny of Your Digital Discovery and Production Process

Regulators and plaintiffs will continue to place heightened emphasis on not only production format but also upon the specific process employed to comb the corporate archive of electronic records and produce the responsive information to which the requestor is entitled. Sometimes, if the facts are not on your side, it makes sense to attack the process.

How will your company hold up under increased scrutiny from a process standpoint? The "old boy network" will quickly become obsolete as previously-ignored details become more important. Prepare to answer questions such as: How good is the documentation? Which search engine and search terms were used? Did the software search e-mail attachments? Did you first search the native files or did you search the paper or the TIFF image after it was scanned/OCR'd? Was the proper universe of files searched? How did you handle the metadata? How did you handle viruses? What steps were taken to protect privileged data and trade secrets? How did you break up e-mail and attachment pairs? Did you make electronic productions of native files without first assigning/branding Document Control Numbers onto the produced files? How were redactions made? How did you process difficult to read file formats? What is the precise chain of custody? Even if you know how these issues were handled on the last case, go back and confirm these answers on the next and all future discovery requests before you produce electronic records.

Impact of New Digital Discovery and Production Tools

Fortunately, new solutions exist to help simplify and solve many of today's digital discovery problems. For instance, Evidence Exchange (www.evidenceexchange.com) has introduced a new service and evidence exchange format called the Secure Digital Photocopier ("SDP"). The SDP method always preserves the original file. Although designed specifically for digital discovery and production, in a sense, it's today's equivalent of a traditional photocopier. Instead of duplicating paper, it securely duplicates digital documents of disparate types, creating a cryptographically secure link between copy and original.

SDP relies on Surety's time-stamping technology to first extract DNA (i.e., Digital Notary Algorithm, analogous to the chemical compound that makes each person unique) from an original file and then brand that DNA string into a PDF rendering of the original source file. In the normal course of processing files, the SDP process also wraps the metadata and provides a comprehensive set of documentation detailing the electronic data conversion methods used as well as the complete chain of custody. The canonical format used to render electronic documents is fully searchable, readable and printable.

Using Evidence Exchange's SDP process, lawyers can fully automate the difficult task of finding and/or producing the e-mails, word processing files, spreadsheets, etc. that exist in compressed file formats on servers throughout today's enterprises. The SDP process also works with non-textual files (e.g., voicemail, photographs, etc.).

Authorized users can utilize the service to determine whether a produced file has been altered or to prove that an electronic archive remains pristine (i.e. preserved without change during the obligation period). Selected files can be numbered with custom prefixes and references to protective orders, etc. branded into the document footer. The SDP exchange format—print ready branded PDF—supports high-speed printing of up to 180 pages per minute per machine. Alternatively, digital evidence can be exchanged via CD-ROM or the Web. Deposition or trial exhibits can be quickly authenticated individually or in bulk, by the court or by the individual parties, via the World Wide Web, a method that has the added benefit of saving the court's valuable time.

Summary

Digital discovery and production processes must change to accommodate the new ways of conducting business dictated by the technology explosion. Likewise, as more corporate assets become only electronic based, file/document verification and authentication will become pressing issues. The good news is that the new solutions cost considerably less than the existing ones and yield a superior product. The emerging solutions, including SDP, will truly streamline the digital discovery and production process. But organizations lacking the mettle and vision to move quickly to safe harbor, whether through modified process or new approaches, may be left behind, casualties of a potentially fatal self-inflicted wound.

Michael Prounis is the CEO and co-founder of Evidence Exchange. He has worked in legal information systems since 1977. Evidence Exchange is located at 21 Penn Plaza, New York, NY 10001. The phone number is (212) 594-2500 and the e-mail address is <michael.prounis@evidenceexchange.com>.

Web Site Records Retention: Maintaining Records in a Dynamic Environment

Scott Sleek

Web sites are not just a way to promote and sell your organization's wares or services. Today, they're a vital and often overlooked source of important business records—the type that may end up being central to a legal dispute.

Today, any company engaged in electronic commerce or other types of transactions via the Internet needs to capture its web site pages as records. Those pages can end up the focal point of litigation in areas ranging from transactional disputes to product liability actions to accusations of intellectual-property infringement.

In addition, companies may need to maintain web site records to prove their compliance with regulations and laws. Screen captures can prove, for example, that an organization has at all times posted its privacy policy or advertising disclaimers in the appropriate place on the web site, as required by law.

But maintaining web site records can be far more daunting than retention of paper records, two consultants pointed out in September at the 2001 Managing Electronic Records Conference, hosted in Chicago by the management consulting firm Cohasset Associates, Inc. Web sites can generate hundreds or thousands of updates to their pages daily, Dick Fisher, a Cohasset senior consultant, pointed out.

"The world is operating at Web speed," Fisher said. "Everything has to be updated immediately. Unfortunately, that's leaving some of the discipline [of records retention] behind in the Web environment."

What's more, many web sites offer personalized information for each customer, based on information the individual provides. That can drastically increase the number of pages any Web site operator generates in a single day.

"Let's say you have two million clients and each can customize the web site to their liking." Fisher said. "Are you then required to retain 2 million versions?"

Creation of Web content also creates problems. In the building or updating of a web site, authors create the content, which can range from advertising copy to graphics. If necessary, that content then goes through staff counsel, regulatory agencies, or other governing bodies to make sure it conforms with relevant laws or policies. (For example, a company may have to capture an online advertisement to prove it has met Federal Trade Commission requirements on truth in advertising.) The content then proceeds to production staff for editing or formatting.

All the stakeholders in this process should collaborate constantly, counseled Fisher and his fellow Cohasset consultant Laurie A. Fischer. They offered the following suggestions on maintaining web site records:

- **Inventory your web sites.** Profile the tools used to create and manage the content, and look at such factors as personal customization capabilities, the number of dynamic web pages produced, encryption used, and third party information on the site.

- **Determine the content to be retained.** Decide, for example, whether every customized screen should be preserved. Companies should decide what is to be retained, how it's to be retained and for how long.
- **Investigate vendor offerings.** Right now few consulting firms and software companies can offer the type of functionality needed to capture and manage web site information. And most of the existing products provide no retention capabilities and aren't designed to manage large amounts of information. As more and more organizations realize the importance of preserving Web data, other vendors will develop products to offer help in storing and organizing that information, Fisher said.

And when building a new web site, the consultants suggested, all stakeholders should get together to create design and preservation policies that can be factored into the creation of the site. This involves steps ranging from establishing the content approval process to defining storage media for web site records.

For more information, contact Cohasset Associates, 800-200-7667, **www.cohasset.com**

Scott Sleek is the former News Editor for Digital Discovery and e-Evidence.

Case Law & Rules Update

Marginal Utility of Extracting Files from Backup Tapes Must Be Balanced by Expense

Not only must there be a reasonable certainty that backup tapes will contain information relevant to a claim or defense, but the burden or expense of extracting files from those backup tapes must also be taken into account before a party will be ordered during discovery to undertake such retrieval, a magistrate judge of the U.S. District Court for the District of Columbia ruled Aug. 1 in *McPeek v. Ashcroft*, 8 ILR (P&F) 3060. In light of this balancing test, the court ordered the defendant to perform a test run in order to determine the burden of accessing its backup tapes, which might contain the text of e-mail messages relevant to a sexual harassment case.

Background. The plaintiff in the harassment case, an employee of the Bureau of Prisons, had filed an internal complaint with the U.S. Department of Justice against the then-director of the bureau, alleging sexual harassment. In 1992, the parties reached a settlement agreement that was to be kept confidential. The plaintiff there then became the plaintiff here, alleging that his colleagues nevertheless learned about the complaint he had filed and that he suffered humiliation and retaliation as a result. He also alleged that he suffered further retaliation after he hired counsel.

The plaintiff sought discovery of evidence of retaliation from the DOJ, including from backup tapes of the department's computer systems. The defendants argued that it was unlikely that relevant documents would be found on the tapes and that the burden of examining the tapes would be very high.

Backups not designed as archives. "Using traditional search methods to locate paper records in a digital world presents unique problems," Magistrate Judge John M. Facciola writes. "In a traditional 'paper' case, the producing party searches where she thinks appropriate for the documents requested under [Federal Rule of Civil Procedure] 34. She is aided by the fact that files are traditionally organized by subject or chronology.... Backup tapes are by their nature indiscriminate. They capture all information at a given time and from a given server but do not catalogue it by subject matter." This is because backup tapes are intended only to serve in case of a particular day's data loss, and are not meant to be a reference for all material stored on the computer systems.

The defendant, by refusing to undertake such an onerous search of its backup tapes, ran "the risk that the trial judge may give the jury an instruction that this failure to search permits the inference that the unfound files would contain information detrimental to [it]." But the possibility existed that the trial judge may decline to give such an instruction. There was therefore not much "incentive" for the defendant conduct a search. "Given the potential costs involved, [the] defendant may be more than willing to decline to search the backup tapes and take the chance that either the court will not give such an instruction at trial, or that if [it does], defendant will still prevail." Another concern was that the potential for settlement would be diminished if the defendant had the option to simply choose not to do the search. "[D]iscovery advances the prospects of settlement[,] ... and there is good reason to think that information on the backup tapes might induce one party or the other to settle."

However, finding that "[t]here is no controlling authority for the proposition that restoring all backup tapes is necessary in every case," the court focuses on the question of whether the plaintiff or the defendant should bear the cost of such restoration when it is appropriate.

Who pays? "The one judicial rationale that has emerged is that [making] backup tapes is a cost of doing business in the computer age," the court states. After all, "[w]hat alternative is there? Quill pens?"

Still, large businesses and government organizations could indeed elect to have no backup systems if they are

forced to restore them whenever they are sued. While that may seem unlikely, "courts should not lead them into temptation." "Furthermore, making the producing party pay for all costs of restoration as a cost of its 'choice' to use computers creates a disincentive for the requesting party to demand anything less than all of the tapes."

The other option would be to shift the financial burden to the party seeking backup retrieval—"so that the requesting party literally gets what it pays for." But there are problems with this approach as well. In this case, for instance, the defendant agency is not a "profit-producing entity," and so "it cannot be said that [the receipt of] costs in this case would yield the same 'profit' [to the defendant] that other foregone economic activity would yield." In addition, because of the possibility that sensitive information could be viewed, the government could not grant records access to outside parties. A government employee would still be required to conduct the retrieval in order to ensure security. Furthermore, for the party seeking the information, it would not be fair if there were an additional cost simply because the data sought was in electronic storage rather than on paper, the court said.

Therefore, "a fairer approach" would be based, by analogy, on the economic concept of "marginal utility." In this context, that means that "[t]he more likely it is that the backup tape contains information that is relevant to a claim or defense, the fairer it is that the government agency search at its own expense." Conversely, the less likely it is that pertinent evidence will be found, the more "unjust" it would be to make the agency pay.

The degree of utility of the information sought must then be balanced by consideration of the burden or expense of such retrieval. "If the likelihood of finding something was the only criterion, there is a risk that someone will have to spend hundreds of thousands of dollars to produce a single e-mail," the court said. "That is an awfully expensive needle to justify searching a haystack." It must also be kept in mind that ordering the producing party to restore backup tapes upon a showing of likelihood of relevant information alone would give the plaintiff "a gigantic club with which to beat his opponent into settlement."

The court decides, "[g]iven the complicated questions presented, the clash of policies[,] and the lack of precedential guidance," to "take small steps" and order only a "test run." The DOJ must perform backup restoration of all e-mail files attributable to the plaintiff supervisor's computer during a period of one year preceding the plaintiff's initial allegation of retaliation. This seems "a convenient and rational starting point to search for evidence." E-mail files were chosen because of their "universal use" and also because the restoration might uncover communications both sent by and sent to the supervisor.

"Upon the completion of this search, the DOJ will then file a comprehensive, sworn certification of the time and money spent and the results of the search." Once it does, the magistrate judge will "permit the parties an opportunity to argue why the results and the expense do or do not justify any further search."

The plaintiff was represented by Debra Susan Katz, Ari Micha Wilkenfeld, and Lisa Jean Banks of Bernabei & Katz, Washington, D.C. The federal defendants were represented by Allison C. Giles and Carlotta P. Wells of the Justice Department, Washington, D.C.

Prosecutors Seek Protection of CIPA to Limit Disclosure of Key Logger Details

In the face of an order to reveal how its "key logger" technology works, federal prosecutors have sought the protection of the Classified Information Procedures Act, claiming that open disclosure would be a national security issue, according to a request filed in the U.S. District Court for the District of New Jersey by the federal government. The court had issued an order asking prosecutors to disclose the workings of its "key logger" technology, used to track the computer activities of an alleged mobster (*United States v. Scarfo*, D.N.J., Crim. No. 00-404 (NHP), brief filed 8/23/01).

The issue arose in the government's prosecution of Nicodemo S. Scarfo. In building its case, investigators employed key logger software in order to access Scarfo's computer and track online communications. Scarfo filed a motion to suppress the evidence, arguing that the government had violated the Wiretap Act, 18 U.S.C. §2510.

On Aug. 7, Judge Nicholas H. Politan ordered the government to turn over information regarding how the key logger works in order to determine whether its use was constitutional. The court declined to accept on its face the government's contention that fully explaining the technology would jeopardize national security or endanger the lives of law enforcement agents.

In its current motion, the government argued that the key logger technology is classified and its disclosure would be a matter of national security. Therefore, the government sought the protection of the Classified Information Procedures Act, 18 U.S.C. app. III.

The motion argued that the information regarding the workings of the key logger is a matter of national security under 18 U.S.C. app. III §1, which defines national security as "the national defense and foreign relations of the United States."

CIPA says that a court may allow the government "to delete specific items of classified information from documents to be made available to the defendant through discovery ..., to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove."

Prosecutors proposed to file the requested information with the court under seal and submit to the defense only an unclassified summary statement. The government would also submit in camera an ex parte statement designed to allow the court to confirm that no critical information would have been withheld from the defense.

The federal government was represented by Robert J. Cleary and Ronald D. Wigler of the U.S. Attorney's Office, Newark, N.J.

The defendant was represented by Vincent C. Scoca of Bloomfield, N.J., and Norris E. Gelman of Philadelphia.

Unrelated Internet Postings Relevant to Defamation Suit

In *Graham v. Oppenheimer*, No. 00-CV-57, 2000 WL 33381418 (E.D. Va., December 15, 2000), the plaintiff alleged that the defendant had defamed him in an Internet posting, and the trial judge admitted into evidence other postings by the defendant. On defendant's motion for a new trial, the court found no error in its decision to admit this evidence: "Rule 404(b) allows for the admissibility of prior acts to show proof of motive, opportunity and intent, preparation and plan, knowledge, identity, and so forth.... The evidence of unrelated messages posted on the internet by [the defendant] clearly goes to some of these issues, including opportunity, preparation, plan, and identity. Further, such evidence was relevant to [plaintiff's] claim that [defendant] acted with malice. In addition, the disputed evidence satisfied the requirements of and was thus also properly admitted under Rule 406 to prove that [defendant's] use of aliases when he posted the defamatory message was in conformity with his routine practice of hiding his identity. Finally, the Court finds that the probative value of this evidence was not substantially outweighed by its prejudicial nature, which I didn't find it to be at all."

The court also reaffirms its decision to exclude evidence of a "test message" which the defense posted on the Internet. "Defendant's test message was properly excluded for lack of relevancy, as defendants failed to articulate any nexus between the test message and the number of persons who did or did not see the alleged defamatory statement. Furthermore, the test message was irrelevant because widespread publication is not an element of the tort of defamation in Virginia."

Computer Files Are Not Result of "Process or System" for Authentication Purposes

In order to demonstrate that a defendant charged with selling a gun to a minor had often neglected to conduct the required instant background check, and instead created phony approval numbers, the government introduced printouts of computerized records showing the approval numbers actually issued by the state bureau of investigation to the defendant's firearms business. The defendant objected to these printouts, based on a lack of authentication. On appeal, the U.S. Court of Appeals for the Tenth Circuit affirms the admission of the evidence. The court notes that the requirement of authentication is met very simply by "evidence sufficient to support a finding that the matter in question is what its proponent claims." The government met this burden by presenting a witness who testified that the printouts were a record of all transactions between the defendant's business and the state bureau. This was consistent with Federal Rule of Evidence 901(b)(7), one of the Rules providing examples of authentication and specifically providing that a public record can be authenticated by evidence that the record "is from the public office where items of this nature are kept". The court also quotes from the Advisory Committee Note to Rule 901(b)(7): "Public records are regularly authenticated by proof of custody, without more. [Example (b)(7)] extends the principle to include data stored in computers and similar methods ...." The defendant tried to direct the court instead to Rule 901(b)(9), another example of authentication which states that foundation evidence should describe the "process or system used to produce a result" and show "that the process or system produces an accurate result." However, "[t]he computer printouts were not the result of a 'process or system...'; they were merely printouts of preexisting records that happened to be stored on a computer." The government offered sufficient circumstantial evidence that the printouts accurately depicted the approval numbers issued to the defendant's business, and nothing more was required. *United States v. Meienberg*, No. 00-1390, 2001 WL 967841 (August 27, 2001).

Court Chides Party Over Request for Judicial Notice of Web Site

Want to get a judge to take judicial notice of your opponent's web site? Better provide details. A civil party trying to establish the court's personal jurisdiction over the defendants in a dispute regarding promissory notes simply asked the court to take notice of defendant company's web site without providing so much as the web address. The court was able to find the site (by adding ".com" to the company name), but still took issue with the plaintiff's imprecise request. "As an initial matter, this type of information [was] not appropriately brought to the court's attention by way of judicial notice. The court was not provided with [the company's] website or the date on which the plaintiff 'discovered' the website." The court quotes Federal Rule of Evidence 201(d): "A court shall take judicial notice if requested by a party and supplied with the necessary information." It also related the defendants' contention that "web site jurisdiction" is not a an appropriate matter for

judicial notice under Rule 201(b) ("A judicially noticed fact must be one not subject to reasonable dispute..."). In any event, the website located by the court *sua sponte* is deemed insufficient to confer jurisdiction. *Callahan v. Harvest Board International, Inc.*, 138 F. Supp. 2d 147 (March 28, 2001).

Exclusion of Computer Calculation Testimony Was Harmless Error, Utah High Court Decides

An accident reconstructionist's testimony about a computer program used to verify his findings was admissible because accident reconstructionists reasonably and regularly relied on computer software programs, the Utah high court ruled July 27 (*Green v. Louder*, Utah, No. 980277, 7/27/01).

The Utah Supreme Court said the trial court erred in failing to admit plaintiff's expert's testimony about the computer program under the inherent reliability test. But the error was harmless, the court said, and affirmed summary judgment for the defense. While there may be situations where computer software programs contain novel elements that would require an inherent reliability determination, in this case the type of calculation the program performed is standard in the accident reconstruction field.

The court also said it was not error to admit the testimony of a defense expert who said that the plaintiff's expert had agreed in deposition with his calculations.

Auto Accident

In 1995, plaintiff Lora M. Green was a passenger in an automobile driven by her mother, Marlene Murray. Murray's automobile collided head-on with a truck driven by Lloyd Louder.

Green suffered a compound fracture of her left wrist and degloving on her arms and legs. Despite skin grafting and surgery, Green lost function of her wrists and suffered scarring. She also alleges the accident accelerated the effects of pre-existing arthritis and lupus, and left her arm disabled between 30 and 35 percent.

Green sued Murray and Louder for negligence. Murray settled and was dismissed before trial. The jury returned a verdict for Louder and Green appealed.

Standard, Not Novel Program

During trial, Green's accident reconstructionist, Ronald Probert, testified that he used a computer program called Winslam to assist him in reconstructing the speed of the accident.

Finding the Winslam program a novel scientific principle or technique, the trial court applied the inherent reliability test set out in *State v. Rimmasch*, 775 P.2d 388 (Utah 1989). The trial court excluded Probert's testimony about the Winslam calculations because Probert was unable to establish the validity of the computer program: Probert admitted he was unfamiliar with the principles and mathematical equations used by Winslam to estimate speed.

The Utah Supreme Court said there may be situations where computer software programs contain novel elements that would require an inherent reliability determination. But in this case, the state high court said, the type of calculation performed by Winslam is standard in the accident reconstruction field.

"The proper inquiry is whether accident reconstructionists reasonably and regularly rely on computer software programs, such as Winslam, to verify the accuracy of their findings," the high court said, citing *State v. Clayton*, 646 P.2d 723 (Utah 1982).

Probert only used Winslam to verify the accuracy of his findings, and did not use the program to find exact answers. And Louder did not dispute that computer programs are universally used by accident reconstructionists in this manner, so the evidence should have been admitted, the court said.

But, the state high court said, the exclusion of Probert's testimony was harmless error because speed was not a determining factor in the causation of the collision.

No Veracity Inquiry

Greg Duvall, Louder's expert, opined that at the moment of impact Louder was traveling 18.8 miles per hour and Murray was traveling 38 miles per hour. During his deposition, Ronald Probert, Green's expert, testified he did not disagree with the calculations of Duvall, Louder's expert.

At trial, Green objected when Duvall mentioned that Probert had agreed with his calculations.

Green argued under Rule 32 of the Utah Rules of Civil Procedure, the deposition of a witness may only be used for impeachment purposes, not to bolster an expert's conclusion. Further, Green said, under *State v. Rimmasch*, 775 P.2d 388 (Utah 1989), a witness is precluded from being an "oath-helper"—someone who verifies the truthfulness of another witness's testimony.

The Utah Supreme Court said *Rimmasch* did not apply because there was no inquiry made regarding the veracity of Probert's deposition testimony.

Therefore, Duvall's testimony was properly admitted, the court said.

Judge Christine M. Durham wrote the opinion.

Jackson Howard, Kenneth Parkinson, and Leslie W. Slaugh of Howard, Lewis & Petersen in Provo, Utah, represented the plaintiff.

David N. Mortensen and R. Phil Ivie of Ivie & Young, also in Provo, represented the defendant.

Federal Courts to Place Civil Cases Online, to Decide on Criminal Case Access in 2003

Documents for federal civil cases will be made available electronically to the same extent they are available at the court house, the federal courts announced Sept. 19. But the courts will wait two years before deciding whether to do the same with criminal case documents.

The civil case documents will not be available through regular Web sites. Instead, those seeking documents will have to sign up with PACERNet, a computer system run by the federal courts. While that service is open to anyone, users must first register with the federal courts for a password and account, and will be charged per page that they view.

The new policy was approved by the Judicial Conference of the United States, the policy-making body for the federal judiciary. The panel is composed of 27 federal judges led by Chief Justice William Rehnquist.

Public Access Versus Privacy

In making court documents available electronically, judges are weighing the benefits of greater public access against the potential privacy concerns of witnesses, law enforcement officials, and business-practice secrets contained in those documents. While the documents under consideration are available at local federal courthouses, making those documents available over remote computer systems will give them much greater circulation.

Civil case documents will be electronically published, but "personal data" identifiers—Social Security numbers, birth dates, financial account information, names of minor children—will be partially blocked out, the judges decided. Bankruptcy cases also will be made electronically available under similar rules, including partial blocking of personal identifiers. District Judge Jerry Davis from the northern district of Mississippi in Aberdeen, who chairs the conference's Committee on Court Administration and Case Management, said bankruptcy courts are far ahead of other federal courts in making civil case materials available electronically.

Test-Run for Criminal Cases

Davis said the conference wants to see how the electronic distribution of the civil cases works before making criminal case material available electronically. "We're in unknown territory," Davis told reporters via satellite. "We want to look at [criminal cases] in two years to see our experience with civil filings," he said.

Current access to court docket sheets through PACERNet and to court opinions through each court's respective web sites will not be affected by the new policy. The rules for availability of files at each courthouse also will not be changed.

The conference had planned to adopt the new electronic documents plan at a meeting on Sept. 11. But the terrorist attacks caused the meeting to be postponed, and the vote of the 27-member panel was conducted via mail ballots, which were received this week.

Canada Postpones Similar Initiative

Approximately one month prior to the US court announcement, the Supreme Court of Canada decided to shelf temporarily its project to begin putting online all documents filed in the cases it hears. On August 12, Chief Justice Beverley McLachlin cited "privacy concerns" as the reason for the delay.

The court hopes eventually to have a fully functional e-filing system for the cases it hears, but there are major technological implications and serious issues of policy such as privacy and access to the court by unrepresented litigants, McLachlin said in a speech to the Canadian Bar Association's annual meeting.

"We realize that the Supreme Court of Canada is expected to show national leadership in this area so that as other courts embark on similar projects there will, ideally, be a single coherent and compatible system throughout the country," she said. "At the same time, we are acutely aware that the policy implications are serious and must be given due attention at this early stage."

The court had hoped to implement at least electronic posting of factums on its Internet site before the end of 2001, but has delayed even that first step because of the privacy and access concerns, she said. "We are holding off a bit longer even on this aspect of the electronic project to ensure we have adequately considered the policy implications," she said.

Concern for Identities of Rape Victims, Children

McLachlin said she was particularly concerned about the impact of providing unrestricted access to court records and arguments in the area of family law, which sometimes contain "sensational or sometimes even scurrilous" allegations. The thousands of documents filed annually with the court can contain the names of rape victims and children involved in custody disputes, she said.

"Our concern arises from the experience of some of the American courts who simply went 'e' very quickly, as I understand it, and ran into problems of voyeuristic access and found it was really compromising the justice system," she said.

Canadian law requires courts to provide access to court documents to anyone who physically goes to the courthouse to view them. Canadian legal observers have suggested that the Supreme Court should post all publicly-available documents online and avoid potential privacy and access issues by having sensitive information excluded from court filings in the first place.

Third Annual
BNA Public Policy Forum:

International E-Commerce & Internet Regulation

November 14, 2001 ▪ Omni Shoreham ▪ Washington, D.C.

Presented by
CONFERENCES

In affiliation with
COMPUTER LAW ASSOCIATION

Hear from top regulators from two of America's largest trading partners, the European Union and Canada, about the risks and liability of operating an e-business abroad:

Keynote Speakers

John Mogg, Director General of the Internal Market Directorate General, European Commission
(Responsible for the EU Data Privacy and Electronic Commerce Directives; negotiated the Safe Harbor Guidelines)

George Radwanski, Privacy Commissioner of Canada
(Responsible for enforcing the new Personal Information Protection and Electronic Documents Act that will impact any firm collecting personally identifiable information from Canadians)

What legal challenges do your clients face operating on the Internet internationally?

Get critical insights and guidance from top officials representing:

The U.S. Copyright Office
U.S. Customs Service
Yahoo!
The European Union, Canada and more
General Electric
Oracle Corp.
Amazon.com

Sponsored by: ALSTON&BIRD LLP GIBSON, DUNN & CRUTCHER LLP

Register Online at http://ecommerce.pf.com or call 800-255-8131, ext. 284.