

Digital Discovery & e-Evidence

BEST PRACTICES & EVOLVING LAW

Inside

6 E-mail Management: Big Problems and Best Practices

7 Case Law & Regulation: High Court Declines to Review Ruling That Computer Passwords Vitiates Consent Search • District Court Holds Hacker's Use of 'Trojan Horse' to Search for Child Porn Violates Fourth Amendment • Absent Showing That Defendant's Production Was Inadequate, Request for All Electronic Documents Was Quashed As Overly Burdensome • Mass. High Court Rules Computer Image Is 'Visual Material' Under Porn Statute • Texas Supreme Court Orders All Backup Tapes Produced • E-Mail Exchanges Between Councilmen Constitute 'Meeting' Under Virginia FOIA • Computer Glitches in System for Selecting Jury Pool Require Reversal of Death Sentence • Five Broker-Dealers Settle Case Involving Storage of E-Mails; \$8.25 Million in Fines

12 Best Practices: Content on Bank Web Site Constitutes 'Pattern or Practice,' Fed Examiner Says • ICC Recommends Harmonized, Limited Approach to Law Enforcement Data Needs

13 Talking Tech: South Carolina Opens Nation's First Cybercrime Center

14 News Briefs: 'Explosive' E-mails Allowed into Evidence in Enron Loan Trial • Lawyers Accused of Hack Attack • Lawyers Ordered to Disclose E-mails in Legal Malpractice Case • SEC Wants Web Disclosure of Insider Deals • Companies Share Information to Fight Cybercrime, Survey Says

15 Calendar

Vol. 3, No. 1 | January 2003

Five Common Myths About Electronic Discovery

by Lynn Reilly

The most difficult thing about electronic discovery today is separating fact from fiction. "Expert" advice is everywhere—but much of it is conflicting, impractical, and weighted with unnecessary technical terms.

Despite the significant body of misinformation that has grown up around the process, electronic discovery doesn't have to be that hard. The myth: electronic discovery is difficult, expensive, and dangerous. The fact: electronic discovery offers ease of use, accuracy, and efficiency that lawyers couldn't have dreamed of in paper discovery days.

Witness these five common electronic discovery myths:

1. Electronic discovery is too difficult and too complicated.

Electronic discovery can look intimidating. Lawyers cringe at the technical aspects; litigation support managers worry about managing multiple vendors performing discrete and intricate tasks. But much of this anxiety comes from a basic confusion about the difference between data gathering and computer forensics.

Computer forensics is a specialized application of scientific principles and practices. Reconstructing damaged information, defeating efforts to destroy

continued on page 2

Conference Highlights Theory and Practice in Electronic Records Management

by Wendy R. Leibowitz

"How many people have a good records management program?" asked Rae Cogar-Shelton of the crowd of in-house counsel at the Princeton Club in New York City in December. Not one hand went up. This may change in the near future.

The speakers at Pike & Fischer's Electronic Records Management & Liability conference held on December 9 were all proponents of "e-knowledge"—the need for lawyers to understand their own practice's document retention policies and to advise their clients knowledgeably about the best practices in a field many lawyers once associated with clerical or librarian tasks. Welcome to 2003, a brave new world where electronic records are front and center in every field from homeland security—do you know how well your network is

continued on page 4

Digital Discovery
& e-Evidence
www.pf.com/digitaldisc.asp

Associate Group Publisher Wendy Leibowitz, wleibowitz@pf.com
800/255-8131 ext. 234
Legal Editor Robert Emeritz, remeritz@pf.com
800/255-8131 ext. 258
News Editor Scott Sleek, ssleek@pf.com
800/255-8131 ext. 291
News Reporter Faith Ruderfer, fruderfer@pf.com
800/255-8131 ext. 288
Group Publisher Zachary Wheat, zwheat@pf.com
800/255-8131 ext. 229
Copy Editor Marie Unger
Layout and Design Manager Jennifer Andruzzi

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

No reproductions may be made without prior written authorization from Pike & Fischer, nor shall this information, either in whole or in part, be redistributed or put into a computer without the prior written permission of Pike & Fischer.

Published monthly, except for August. ISSN: 1537-5099
Subscription rate: \$549



Copyright ©2003 Pike & Fischer, Inc. All rights reserved.

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

Disclaimer: Pike & Fischer, Inc., has created this publication to provide you with accurate, concise and authoritative information on developments in electronic evidence and discovery. However, the information in this publication should not be interpreted as legal advice, and should not be used as a substitute for advice from an attorney. Pike & Fischer is not responsible for any claim, liability, or damage related to the use of information in *Digital Discovery & e-Evidence*. Also, the views expressed by outside authors do not necessarily represent the views of Pike & Fischer.

Name _____

Title _____

Organization _____

Address _____

City _____ State _____ ZIP _____

Country _____ Phone _____

Fax _____ E-mail _____

Check enclosed (MD, NY and Canada: add sales tax; overseas: add \$33 for postage.)

Bill me (add \$20 for shipping)

Charge my: VISA AmEx Discover Diners

Card number _____ Exp. date _____

Signature _____

MAIL or FAX a copy to:
Digital Discovery, Pike & Fischer, 1010 Wayne Avenue,
Suite 1400 Silver Spring, MD 20910; 301/562-1521

continued from page 1

evidence, retrieving deleted information, and retracing user activity are all examples of the work of forensic specialists. Forensics requires expensive expert help and highly specialized hardware and software. Analyzing a single hard drive can cost thousands of dollars.

In contrast, data gathering is simply the process of collecting electronic evidence from computers. Using forensically sound practices to collect potentially responsive documents is much less complex than actual forensics work requiring a specialist.

Forensic evidence has figured in some attention-getting cases, spotlighting the impressive results of experts' work. However, this notoriety has created a perception that computer forensics plays a role in every e-discovery case. Many lawyers mistakenly believe that the first step in e-discovery is to retain a team of forensic scientists to gather client documents for review. In fact, that level of expertise is rarely necessary. In the vast majority of cases, data gathering can be accomplished with cooperation from client IT personnel, relatively inexpensive tools, and some good advice or hands-on assistance from an e-discovery service provider.

Outside of the limited cases in which you may need highly specialized assistance, a single e-discovery service provider should be able to help you find data, gather potentially responsive documents, restore backup tapes and other legacy data if necessary, review documents electronically, and produce them in the format you choose.

2. Electronic discovery is too expensive.

For most companies, avoiding discovery costs altogether is not an option. The question is how to minimize them. Some lawyers dismiss e-discovery as too expensive without fully understanding its benefits. But clients' need to control discovery costs is an important concern that deserves attention. An informed budget decision calls for a reasoned cost-benefit analysis of every alternative.

Many lawyers believe they are saving money by printing electronic documents. But handling paper incurs the costs of printing, shipping, copying, Bates stamping, storing, and possibly scanning and coding the paper for storage in a database. Keeping documents electronic eliminates all these unnecessary steps and associated costs. Lawyers using traditional desktop litigation support databases should also consider the cost savings of Web-based discovery, which eliminates the hardware, software, and IT costs of housing data locally within a firm.

Besides saving pass-through costs, electronic discovery saves attorney review time. Sophisticated electronic search functionality allows reviewers to quickly master a large volume of data, finding and organizing documents in a fraction of the time it would take to manually search paper. Lawyers can use a single interface to precisely target critical information and then review, annotate, redact, number and mark documents. They can create case-specific subsets of documents that are organized by subject matter, issue or witness—to name just a few examples. Internet access to documents alleviates the costs of traveling to wherever the paper is stored. With online access, firms can also maximize use of their own personnel in all offices, rather than hiring temporary attorneys.

Discovery can be expensive—but electronic discovery is typically 80 to 90 percent less expensive than the alternatives.

3. Electronic discovery is only for big cases.

Nearly all business documents are created on computers,¹ so there is no reason to assume that e-discovery is only for huge cases. Practically speaking, though, most lawyers' introduction to e-discovery does come in very large cases: lawyers do not investigate e-discovery services until the volume of information they are facing forces them to reconsider their old methods.

This has fueled the belief that e-discovery is efficient only for huge cases. Many legal professionals do not realize that the technology scales down as well.

Those who initially adopt the technology for a large case find that the efficiencies of handling documents electronically apply as well in smaller cases.

E-discovery services base pricing on the volume of documents; there is no additional technology investment. Many attorneys contemplate e-discovery technology in terms of the traditional desktop litigation support databases they have used in the past. These applications require investment in software seat licenses, extensive training on the databases, and possibly additional hardware as well. The law firm houses the data and its IT department provides support. All of this infrastructure adds up to a significant investment. Volume-based costs of preparing documents for upload to the database are additional.

In contrast, true electronic discovery services are priced on a per-page or per-gigabyte basis. You do not need to buy additional hardware to store documents—reviewing lawyers need only a Web-connected PC to review documents online. They do not invest in software. Per-page costs include support, preserving the resources of your firm's IT department. Training time is usually less than an hour for anyone who has used the Internet.

Because costs are relative to case size, the efficiencies of e-discovery are available no matter the size of the case. Clients save money, and review teams save time, by eliminating unnecessary costs of dealing with paper and finding essential documents in minutes. Gaining these advantages is just as important for a small concern with a limited litigation budget as for a large entity in major litigation.

4. Meta data is dangerous.

Meta data is the electronic information behind the face of a document. It may reveal a document's author, creation date, modification date, edits, bcc recipients, and a trove of other information not apparent on the document's face. Frequently, when lawyers learn about meta data, their first thought is disclosure to the opposing party: How can they produce electronic information without revealing meta data? A related concern is that producing in electronic

form leaves documents open to alteration. Their impulse may be to print everything.

While lawyers should be aware of the implications of producing native electronic documents, those using sound practices need not worry about producing information they do not intend to reveal. Protecting meta data from disclosure and documents from being compromised is not complicated from a technological perspective. The key is awareness of the need for a format suited for production.

In their concern about inadvertent disclosure, lawyers can overlook the advantages of meta data. Meta data is what enables detailed, precise searches of electronic information. Sorting and filtering by custodian, file type, date range, distribution list, and modification date are just some of the practically endless ways to review and order a body of evidence. In finding and organizing evidence, meta data is an attorney's best ally.

Though many think of meta data in terms of the damage it can do, the substance of meta data information can help in either asserting or defending a claim. If information is potentially problematic, lawyers have the opportunity to find it quickly, analyze and prepare to confront it, and prepare defenses accordingly. Whatever the substance of the information they find, they have the advantage of finding it quickly.

A service provider should use methods that capture original document meta data, so that the reviewer can retain its benefits and can produce it if necessary.

5. The best way to control e-discovery costs is to hire the lowest bidder.

As the legal profession makes the paper-to-electronic shift, many litigation support firms that started off copying, scanning, and storing paper are now holding themselves out as e-discovery "experts." The quality of service offered in the industry varies widely. It is critical to investigate whether the so-called expert is a proven, experienced technology company or a paper vendor attempting the transition to electronic discovery.

A recent case spotlights the hazard of dealing with a vendor who lacks the expertise to properly handle electronic

information.² The plaintiff failed to produce requested e-mails in time for trial because the vendor it engaged was unable to retrieve them.

Though the nonproduction was attributable to the vendor, the court held it appropriate to sanction the plaintiff. Specifically, the court questioned whether the plaintiff acted in good faith in continuing to rely on the same vendor "throughout months of apparently fruitless attempts to retrieve the critical e-mails." It focused on the "discrepancy in competence" between the parties' vendors, noting that the defendants' vendor was able to identify and begin retrieving the e-mails in four days.

The message: courts will hold parties accountable for their decisions in dealing with providers of electronic discovery services. Considering the possible consequences, choosing a service based on price alone is not a sound alternative.

With the right help, electronic discovery is easier and more efficient than the alternatives. Those who are new to the process can benefit from a service provider's experience in assisting with practical advice at every step: finding and gathering potentially responsive information, then processing, reviewing and producing it. One way to avoid misinformation is to question the source. A skilled service provider should offer expertise to simplify the process, not issues to further complicate it.

Lynn Reilly, Esq., is educational programs manager with Applied Discovery Inc., a full-service electronic discovery service provider. Ms. Reilly can be reached at lynn.reilly@applieddiscovery.com. Learn more about Applied Discovery online at www.applieddiscovery.com.

Endnotes

1. For example, studies show that 60 percent of business-critical information is now stored within corporate messaging systems, up from 33 percent in 1999.

2. *Residential Funding Corp. v. DeGeorge Home Alliance, Inc.*, 2002 U.S. App. LEXIS 20422 (2nd Cir. September 26, 2002).

continued from page 1

protected?—to employment management practices to cost reduction and spoliation during discovery.

Many lawyers don't think electronic records management is their concern. James Michalowicz, the manager of legal services at E.I. DuPont de Nemours and Company, said that electronic records were like a baseball card collection. People with rich but disorganized baseball card collections are less aware of the value of their collection's contents, and they are less able to leverage their collection than someone with a well-organized and well-catalogued collection. Similarly, when a lawyer presents a judge with a well-organized electronic records retention program, the judge seems to credit the claims of that lawyer more, awarding valuable "points" for organization and demerits for an unmanageable mess, said Michalowicz. "Do you have a policy? How is it enforced? Communicate those points to the judge," he advised.

Further, electronic-era judges are less sympathetic to claims that discovery requests are overly burdensome. "That defense does not work anymore," said Michalowicz, perhaps because judges think that searching electronic records is easier than searching paper records. Thus, if your client thinks a request is burdensome, it's probably because your electronic records program is poor—a sign, perhaps, of poor counsel.

Risks in Managing Electronic Records

Chanley Howell, a partner in the Jacksonville, Florida office of Foley & Lardner and the author of "Document Retention in the Electronic Workplace" (Pike & Fischer, 2001), spoke of the human challenges in electronic records preservation and storage.

The greatest problems are human, not technological: employees who ignore computer-use policies and abuse computer privilege. This problem is one of company discipline and culture, said Howell, which must be remedied both through education and example.

Education can be straightforward—

"These files are not bags of trash. They are records. Keeping them orderly is part of your job," he emphasized. Rules can also be enforced through an awards program, such as one that recognizes "records champions," and through technology itself. Many e-mail and software programs will require people to flag a document if it is to be saved, or it will be automatically destroyed after a certain time. "Impose discipline to keep what's of value," he emphasized, and—equally as important—to discard what is not. He emphasized that the records retention policy must be "claims and litigation neutral." That is, it must be consistently applied without regard to whether documents are helpful or damaging.

Finally, employees should be informed that compliance with the policy is mandatory, and that records need to be retained by law. The scope of the policy includes all records and notes maintained or created by any employee, on or off company property.

Another issue arises at the interface of employee and equipment, said Howell: high-tech employees who keep data on antiquated computer ware. This is usually a financial decision—if it's not broken, why upgrade? But the old machines can be tricky to maintain, and sometimes when people think that records are being safely stored, and quickly accessible if needed, they are not.

As part of spring cleaning, counsel compliance or annual inventory, lawyers should test the back-up systems to make sure that what is needed is truly backed up. The periodic "technology audits" should be modified as technology advances.

Howell also suggested that there should be one document policy for both paper and electronic records, perhaps by scanning paper documents into electronic form. "Electronic copies of paper records must be complete and accurate replicas of the originals, and must be accessible in tangible form."

Consequences of Poor Management

The result of this unbending empha-

sis on records management, perhaps, will be akin to the changes that followed the Y2K computer bug scare: people upgraded and educated themselves and their equipment. While many of the upgrades were not necessary for the year 2000, the backups and disaster preparation plans fell into perspective following the terrorist attacks of September 11, 2001.

Howell noted that many people were now focusing on electronic records because of recent developments in which poor records management resulted in criminal sanctions—the Sarbanes-Oxley Act of 2002, which followed the destruction of records in the Enron/Arthur Andersen scandal; added sections to the federal criminal code; and the expansion of 18 U.S.C. §1512 to prohibit anyone from "corruptly" engaging in the alteration or destruction of a document in connection with an official proceeding.

Howell ended by detailing the criminal and civil charges associated with records destruction. The case law is growing in the spoliation area. Though the document destruction that brought down Arthur Andersen was highly publicized, the touchstone decision is *In re Prudential Ins. Co.*, 169 FRD 598 (D.N.J. 1997), where sanctions were imposed even though there was no proof of intentional destruction of documents. "Haphazard and uncoordinated approach to document retention indisputably denied the opposing party its opportunity to establish facts in dispute," wrote the court. "Corporations, like Prudential, who seek access to the federal courts, have an obligation to comply with both the spirit and intent of the rules."

Koch v. Koch Industries, 197 FRD 463 (N.D. Ok. 1998) specifically cited the negligence of senior management in the destruction of computer records relevant to the litigation, at a time when the defendant had a duty to preserve the records. "The defendant had no formal document retention policy and no ... procedure for notifying its employees of imminent or pending litigation,

and the obligation to preserve records.” Some courts allow an inference that the unavailable records would be damaging; others find that the impact of spoliation sanctions is damaging enough on a client’s case, said Howell.

The possibility of judicial sanctions aside, the high cost of retrieving data that has been stored haphazardly, and the risks of inadvertently disclosing confidential information that exists in data files, render the cost of “bad” records management just as high as good management, concluded Howell.

The Fundamentals of E-Documents

Cogar-Shelton explained that in addition to creating and implementing an electronic records policy, lawyers must be aware that electronic records are filled with much greater content than paper records. Hidden data, called “metadata,” unwittingly created in Word documents, e-mail, and other electronic records, can disclose information, such as prior drafts and information edited out, the names of people who worked on the document that the producing party might not want disclosed, and the location where the document was created and stored. One way to protect this information is to convert the document into a PDF file before producing it, she said.

Computer files can be easily altered, bringing their authenticity into question, which might work to one’s advantage or disadvantage, Cogar-Shelton observed.

She also discussed the reality that copies of a single electronic document may exist in places lawyers might not even consider, such as instant-messaging databases, Palm Pilots, cell phones, and home laptops. Cogar-Shelton addressed storage and security issues, emphasizing the need to protect the privacy of customers and employees and guard trade secrets from hackers and rogue employees.

Finally, Cogar-Shelton emphasized the problems with a “policy” that states, “keep everything, destroy nothing.” A

company that enforces such a policy need never worry about being sanctioned for the destruction of records, but the costs of maintaining all records in storage could be “staggering,” she said. A records policy should be tailored to the company, its employees, and its needs. That does not mean keep everything forever, said Cogar-Shelton. Rather, it requires a quality index of all record holdings, active and inactive. Even lengthening retention periods could have potential costs and risks to the company, she concluded. (*See DDEE, “Records Retention Programs: How to Create One, and Why You Must,” by Rae Cogar, April 2002*).

Implementing the Policy

The most brilliantly conceived policy can be nullified by poor implementation. Michalowicz discussed the best ways to roll out a policy, and how to obtain “buy-in,” or approval and support, from senior management in various departments.

First, there must be a clear rule about who the “owner” of a record is. Usually, it’s the person who creates the document. That person has the duty to retain the record according to the policy. “Every employee is a potential custodian of records,” he said.

This turns the usual lawyer’s perspective on its head. It’s not “someone else’s job” to adhere to the policy; it is the lawyer’s job to see that the policy is understood and enforced consistently, he said. This can represent a major culture change in law firms, in-house departments, and clients.

“There is a comfort level to paper that electronic records do not replicate,” Michalowicz acknowledged. “Make people feel safe” with electronic records by having a good policy and explaining why the policy exists, he suggested. Paper and electronic records must be treated the same way, he emphasized. “Marry them.”

Michalowicz ran into several misunderstandings about the records retention policies at Dupont. The policy was to retain e-mail records for three months.

But the Charlotte office, seeking to be “super-compliant,” kept the e-mails for a year. That attitude did not end up helping the company, he noted, since it indicated that the policy was not diligently enforced company-wide, and by implication, made other offices appear to be hiding something. “Remember, there’s always a Charlotte office,” said Michalowicz, and lawyers should be diligent in ensuring that no one is unintentionally violating the policy while trying to be helpful or “super-compliant.”

Outside vendors and contractors should be informed of the policy, where appropriate, and the policy must be updated as technology changes. New technologies exist to ensure that computers aren’t being misused or compromised—thus potentially making the company safer and more efficient.

Gradually, if electronic records are stored well, there are fewer “paper touches,” Michalowicz said, when retrieving older documents. The resultant savings of time and money come to be appreciated, slowly, by senior management, he said, especially those that remember the warehouse days, when armies of paralegals patrolled documents in warehouses. Those days are not yet gone. But, with proper legal guidance, the future can be better.

In DDEE, October 2002, “Spilling Your Own Secrets: Hazards of Word-Processing Software,” by Scott Sleek, experts discuss methods of concealing metadata. To view tips on minimizing metadata from Microsoft Word, log onto <http://support.microsoft.com> and use the search term “metadata” in the “Knowledge Base” fields on the left side of your screen. To learn how to minimize metadata in WordPerfect, log onto http://cache.corel.com/Storage/Cor Document/Minimizing_metadata_in_\WordPerfect_10_documents,0.pdf.

E-mail Management: Big Problems and Best Practices

by Peter Sloan

The general counsel of Monolith Corporation shook his head in exasperation. Months earlier, the idea of an unfair competition lawsuit against rival Paragon, Inc. had seemed worthwhile. Paragon had entered Monolith's market five years earlier, and for the last three years Monolith had taken a beating. Somehow Paragon was capturing customers at a rapid rate, including customers Monolith had served for years. There had been movement of salespersons between the companies' employment, and Monolith's management became convinced Paragon's success was built upon proprietary Monolith customer information that had walked out the door. So four months earlier, Monolith's general counsel had hired a law firm and filed suit against Paragon, alleging a variety of theories built upon the claimed wrongful use of customer information.

Big Problems

Defendant Paragon propounded discovery, requesting all communications by and between Monolith's sales staff regarding a lengthy list of common customers, including e-mail. The judge brushed aside Monolith's objections by imposing a confidentiality order.

The nightmare started when Monolith began to prepare for its first-ever, broad scale identification and production of e-mail. Monolith had no records management process in place for e-mail. The corporation had a records retention schedule, but it only addressed paper documents. E-mail had become the predominant means of communication for Monolith's sales staff, and Monolith's Exchange servers were overloaded with nearly 100 gigabytes of e-mail and attachments. Monolith's IT Department commonly waived individual user account volume limits at the insistence of individual managers. Monolith had no electronic document management system, nor had it ever adopted or enforced a practice of structured storage, by which the small percentage of e-mail with lasting importance could be topically organized and retained. The IT Director reported that while he could segregate e-mail by user account, the company had no available tools to use full-text searching in Exchange to identify e-mail mentioning the numerous customers at issue.

To make matters worse, the IT Department was sitting on a mountain of e-mail backup tapes. Monolith's backup protocol called for nightly server backup, rotated each week, yet with the weekly full backup to be maintained indefinitely. And a large number of weekday backup tapes, for the most part unlabeled, were found in a filing cabinet.

Monolith's general counsel kicked himself for never having found the time to focus on electronic data retention. He had actually thought he was ahead of the game by paying

for a paper records retention schedule and pushing through a computer use policy. He looked again at the cost estimates for segregation, identification, privilege screening, substantive review, and production of the requested e-mails, and he winced at the number of zeroes. But then he chuckled, muttering "Okay, let's share the pain. If Paragon can do this to us, we'll do it to them."

Bigger Problems—and Best Practices

Four months later, Monolith's general counsel was fit to be tied. He was astounded that his classic discovery strategy had backfired.

Monolith had aggressively pursued electronic discovery of Paragon, with similar requests for Paragon's e-mail and also a designate deposition. But Paragon had only a manageable quantity of responsive e-mail, which it agreed to produce along with an appropriate privilege log of some withheld attorney-client privileged e-mail.

The deposition of Paragon's designate on e-mail management was a disaster for Monolith. Years earlier, Paragon had implemented a comprehensive management approach for e-mail, coordinated with Paragon's company-wide emphasis on records and information management:

1. Paragon's retention schedule applied to all of its records, including electronic data. Both paper and electronic files, including e-mail, were tied to functional record categories with the appropriate retention period for the records' content, based upon legal retention requirements and business considerations. In a well-documented, annual review process, Paragon properly disposed of paper and electronic records that were no longer required to be kept for legal or business reasons.

2. Paragon had successfully implemented a "move it or lose it" approach to e-mail. The relatively small percentage of e-mail to be kept due to legal requirements or business considerations was moved out of the network e-mail storage environment into either company-defined structured storage or, in some departments, an electronic document management system. The retained e-mail was therefore organized by content under the Paragon retention schedule and could be easily located when needed. All e-mail not required to be kept due to legal requirements or business considerations was automatically purged in the ordinary course of business after 60 days.

3. Paragon backed up e-mail solely for disaster recovery purposes. Since there was no need to have backup of e-mail for more than three business days, Paragon operated a very tight e-mail backup rotation.

4. Paragon had appropriately staffed its records and information management function, trained its employees on what was expected of them, and periodically audited compliance with its records and information management policies.

5. Paragon had a sound protocol for records preservation that it implemented whenever a preservation duty

arose due to impending litigation. A legal hold on backup tapes lasted only as long as was necessary for Paragon to identify individuals with knowledge, locate their papers and electronic data subject to the preservation duty, and replicate and secure them.

But it was in court that Monolith had its most painful experience. Monolith sought sanctions, claiming Paragon had wrongfully disposed of e-mail. Instead, Paragon convinced the judge it had carefully crafted its records policies with a good faith, ordinary course of business analysis—and presented the business case to prove it. Each of Paragon's actions that led to the purging of e-mail over the years was justified in a litigation-neutral manner, with appropriate consideration of the costs to be saved by proper disposition of electronic data no longer required for legal or business reasons, and of the value a company can gain from effectively managing its records and information resources.

Once the preservation duty actually arose in the dispute with Monolith, Paragon took steps to preserve e-mail and other records that satisfied the judge.

Yet the loss of its spoliation arguments were the least of Monolith's problems now. Paragon demonstrated to the judge how a responsible company should manage its e-mail in the ordinary course of business, and in appropriately preserving and producing it in discovery. This cut the heart out of Monolith's *Rowe* arguments for why it should not bear the high cost of responding to Paragon's e-mail discovery. Suddenly, the attractiveness of Monolith's lawsuit evaporated, leaving Monolith's general counsel with just one question: "I wonder who will take the fall for this one?"

Peter Sloan is a partner at Blackwell Sanders Peper Martin, LLP. Mr. Sloan counsels companies on records and information management. He can be reached at psloan@blackwellsanders.com.

Case Law & Regulation

U.S. Supreme Court: Search and Seizure

High Court Declines to Review Ruling That Computer Passwords Vitiates Consent Search

Freeh v. Trulock, U.S., No. 02-443, cert. denied 12/2/02.

The U.S. Supreme Court Dec. 2 declined to review a lower court ruling that FBI agents violated the Fourth Amendment when they relied on the consent of an individual's roommate to search his password-protected personal computer files.

The Fourth Circuit had held that FBI agents violated a civil rights plaintiff's Fourth Amendment rights when they conducted a warrantless search of his computer files after his roommate consented to the search, 275 F.3d 391 (4th Cir. 2001). The court later declined to rehear the case en banc.

FBI agents searched the personal home computer of Notra Trulock, the former director of the Department of Energy's Office of Intelligence, shortly after the publication in a national magazine of an article by Trulock that alleged the DOE, the FBI, and other government agencies ignored security breaches at U.S. weapons laboratories.

Trulock's roommate had joint access to the home computer but she did not know his passwords. According to the Fourth Circuit, a search of an individual's password-protected computer files is an illegal search under the Fourth Amendment when consent to the search is given by another individual who had joint access to a computer but did not know the passwords and therefore did not have authority to grant access to the files.

The Fourth Circuit also affirmed that the FBI agents had

qualified immunity from civil rights liability in the case, holding that reasonable officers in their position would not have known that the search violated clearly established law.

E.D. Virginia: Search and Seizure/Child Pornography

District Court Holds Hacker's Use of 'Trojan Horse' to Search for Child Porn Violates Fourth Amendment

United States v. Jarrett, — F. Supp.2d —, 2002 WL 31496302 (E.D. Va. Nov. 1, 2002).

Hacking into a home PC without a warrant violates the Fourth Amendment, says the District Court for the Eastern District of Virginia in *United States v. Jarrett*, — F. Supp.2d —, 2002 WL 31496302 (E.D. Va. Nov. 1, 2002). According to Associate Professor Orin Kerr of George Washington University Law School, who writes extensively on computer crime, this is the first case to state that fact clearly.

Professor Kerr explains that law enforcement agents are in occasional contact with hackers who have hacked into computers and found child pornography. "Without identifying themselves, the hackers report that they have found the child porn, and the police then use the 'anonymous tip' to get probable cause to obtain a search warrant and search the target's house and seize the computer," said Kerr. "Under traditional Fourth Amendment doctrine, this doesn't violate the Fourth Amendment so long as the government does not encourage or facilitate the hacker's conduct, because the hacker is a private actor, rather than the government. See, e.g., *United States v. Kennedy*, 81 F. Supp.2d 1103, 1112 (D. Kan. 2000)."

Case Law & Regulation

But in *Jarrett*, the Eastern District of Virginia granted a defendant's motion to suppress in a case in which the government apparently went too far. Because the government knew of and acquiesced in the hacker's searches, the court held, the hacker became a state actor for Fourth Amendment purposes. Accordingly, the hacker's intrusion into the defendant's home computer without a warrant violated the Fourth Amendment.

The Facts

A computer hacker, apparently operating out of Istanbul, Turkey, had uploaded a file to a pre-teen erotica group that contained a Subseven Trojan Horse, a program that infects computers by posing as a harmless e-mail attachment. The program allows an attacker to manipulate files from a remote system, including retrieving saved and cached passwords. In the *Jarrett* case, the Trojan Horse allowed the hacker to remotely control the computers of people who had downloaded the file from the group. The hacker would then look for child pornography, and when he found it, send an anonymous e-mail to the law enforcement authorities, tipping them off to the location of the child porn.

According to e-mails from the hacker, who went by the name "unknownuser," he had found child pornography on the home computers of at least 2,000 people, including three known child molesters, one of whom had been convicted of child molestation in Alabama and had received a sentence of 17 years.

The hacker "unknownuser" contacted Alabama law enforcement authorities via an anonymous Hotmail account. The FBI then used the evidence sent to it from the hacker to arrest the defendant. The FBI e-mailed thanks to the hacker for his help, and appeared to leave open the possibility of future assistance.

The Law

The defendant, William Jarrett, moved to suppress all of the evidence against him on the grounds that it was all the fruits of an illegal search. Jarrett argued that the hacker had become a state actor by the time he had contacted law enforcement about his hacking, and that his hacking of the defendant's home computer (even from abroad) violated the Fourth Amendment.

The district court agreed with the defendant and granted his motion to suppress. Noting that a private person becomes a state actor if his conduct is designed to help the government and the government "knew of and acquiesced in" the conduct, the court held that both aspects of the test were satisfied. The government had nurtured a relationship with hacker and seemed to want to rely on his tips in the future, which the court viewed as sufficient to constitute knowledge of and acquiescence in the conduct.

The court also agreed with the defense that the act of hacking into Jarrett's home computer from Turkey was a Fourth Amendment search, stating: "[T]he Court concludes

that the evidence seized from the defendant's computer by Unknown user was the result of an unlawful search in violation of the Fourth Amendment."

Professor Kerr is unsure whether this case is correctly decided, at least on the question of whether the hacker was a state actor. Kerr asks, "At the time that the search occurred, did U.S. law enforcement authorities know of and acquiescence in the search? The Court relies heavily on the fact that the FBI was happy to receive the information when the hacker later gave it to them, and on the fact that afterwards the FBI appeared to want to nurture future contacts with the hacker. But that happened *after* the search, not *before* the search, so I can't see exactly how that is relevant. In fact, at the time the search occurred, it had been seven months since there had been any contact between the hacker and U.S. law enforcement. Did U.S. law enforcement really know about the search, and acquiesce, at the time the search occurred? Maybe, but I'm not so sure. I wouldn't be surprised if the Fourth Circuit would see this case differently."

N.D. Alabama

Absent Showing that Defendant's Production Was Inadequate, Request for All Electronic Documents Was Quashed As Overly Burdensome

Braxton v. Farmer's Ins. Group (N.D. Ala.), 2002 WL 31132933, 203 F.R.D. 651 (Sept. 13, 2002)

A nonparty subpoena issued by the plaintiff to insurance agents for all documents, including e-mail, and all documents in electronic format touching on, relating to or concerning the use of consumer credit reports in setting homeowners insurance premiums, was quashed as overly burdensome. Defendant insurer alleged that it was able to produce e-mail messages and other correspondence sent to its agents regarding use of consumer credit reports in setting premium rates; without a showing by plaintiff that insurers' production would be inadequate, nonparty agents would not be required to comb through e-mail and other electronic records.

Massachusetts: Internet Pornography

Mass. High Court Rules Computer Image Is 'Visual Material' Under Porn Statute

Perry v. Commonwealth of Massachusetts, Mass. Sup. Jud. Ct., No. SJC-08662, 12/18/02.

A digitized image stored on a computer is “visual material” for the purposes of Massachusetts’s child pornography dissemination law, the Massachusetts Supreme Judicial Court ruled Dec. 18. The court concluded that the plain meaning of the term “visual material” encompasses any newly created technology. Furthermore, the court said that the updating of statutory provisions by the Massachusetts General Court to include “depiction by computer” was merely a means of reaffirming the meaning of those statutes, not to contrast them with the definition in force at the time of the alleged infractions.

In 1998, police and prosecutors executed a search warrant at the home of Christopher Perry of New Bedford, Mass. They seized his computer, on which were stored images of unclothed under-aged persons. Perry was charged with dissemination of child pornography, in violation of Mass. Gen. Laws ch. 272, §29B(a), and possession with intent to disseminate child pornography, in violation of Mass. Gen. Laws ch. 272, §§29B(a) and 29B(b).

Section 29B(a) makes it a crime to “disseminat[] any visual material that contains a representation or reproduction of any posture or exhibition in a state of nudity involving the use of a child.” Similarly, Section 29B(b) prohibits “the disseminat[ion of] any visual material that contains a representation or reproduction of any act that depicts, describes, or represents sexual conduct participated or engaged in by a child.”

No Explicit Mention of Computer Images

At the time of the alleged offenses, Mass. Gen. Laws Ch. 272, §31, defined “visual material” as “any motion picture film, picture, photograph, videotape, any book, magazine, or pamphlet that contains pictures, photographs or similar visual representations or reproductions. Undeveloped photographs, pictures, motion picture films, videotapes, and similar visual representations or reproductions may be visual materials notwithstanding that processing, development or similar acts may be required to make the contents thereof apparent.”

In an opinion authored by Justice Judith A. Cowin, the court rejected the defendant’s argument that this definition did not encompass the image files stored in digitized format on his computer.

It was irrelevant that the digitized images were in a medium different from traditional film photography, the court said. A digitized image is still a “photograph” in the broad sense.

“The phrase ‘any ... photograph’ means what it says, any photograph without limitation. A ‘photograph’ is ‘a picture, image, or likeness obtained by photography.’ ... In modern parlance, an image produced by a digital camera is considered ‘photography,’ i.e., it is ‘characterized by great truth

of representation or minute detail in reproduction,’ “ the court said, quoting from the dictionary. “It matters not that the scene is captured in bytes rather than on conventional film.”

Furthermore, the court pointed to the statute’s use of the word “picture” in the definition, which, it said, indicated “that the Legislature intended the section to reach images produced by any method of photography: conventional, ‘instant,’ electronic, digital, or some means as not yet invented.”

Additionally, unprocessed images, which are also included in the definition, can be likened to digital files that must be interpreted by a computer in order to be viewed.

The court rejected the defendant’s argument that the General Court’s 1997 amending of the child pornography purchase and possession provision, Mass. Gen. Laws Ch. 272, §29C, to explicitly include “depiction by computer,” should be interpreted to mean that “depiction by computer” was not covered by the definition of the dissemination law.

“Section 29C has its own terms, to which the definitions of [Section] 31 do not apply,” the court said. “In other words, ‘the use of the term “depiction by computer” [in 29C] adds a meaning unnecessary’ in the context of [Section] 31. ... If anything, the legislative ‘findings’ that accompanied the enactment of 29C indicate that the Legislature did not place any significance on the distinction. It is absurd to believe that the Legislature intended that computer-stored pornography could not be purchased or possessed but could be disseminated freely.”

Recent Amendments to Statutory Definitions

Similarly, the court said that the insertion of “videotape” into the definition of “visual material” did not mean that digitized images were excluded from the definition.

“We do not read into that amendment an intent to update, or the necessity of updating, the wording of the statute each time new technology emerges,” the court said. “To hold otherwise would allow child pornographers to evade prosecution simply by upgrading the technology employed.”

Indeed, in 2002, the General Court inserted “depiction by computer” into the provision in question. In doing so, the court said, the legislature was “reaffirm[ing] what was already evident.”

Joining in the court’s opinion were Chief Justice Margaret H. Marshall and Justices John M. Greaney, Francis X. Spina, Martha B. Sosman, and Robert J. Cordy. The plaintiff was represented by Richard J. Fallon of Acton, Mass. The state was represented by William J. Meade and Julie B. Ross of the Office of the Massachusetts Attorney General, Boston. Amicus curiae was represented by Timothy J. Cruz and Mary Lee of the Plymouth County District Attorney’s Office, Brockton, Mass.

Texas: Breadth of Discovery/ECPA

Texas Supreme Court Orders All Backup Tapes Produced

In re CI Host, Inc., 2001 WL 34047373 (Tex. Sup. Ct. Nov. 21, 2002).

Customers brought a breach of contract class action against the company hosting their web services. During discovery, the trial court ordered the defendant to preserve and produce computer backup tapes containing potentially relevant evidence. The defendant objected that the request was overbroad, demanded confidential information, and was in violation of the federal Electronic Communications Privacy Act. The appellate

court held that in light of the defendant's failure to produce evidence supporting its objections as required by Texas Rule of Civil Procedure 193.4(a), the trial court did not abuse its discretion in ordering the contents of the tapes to be produced.

Virginia: Discovery of Public Records

E-Mail Exchanges Between Councilmen Constitute 'Meeting' Under Virginia FOIA

Shelton v. Beck, Va. Cir. Ct., No. CH02-428, 12/13/02.

Members of the Fredericksburg, Va., city council violated the state's Freedom of Information Act when they used electronic mail to discuss matters of public business, the Virginia Circuit Court for the City of Fredericksburg ruled Dec. 13. This ruling was based on a previous holding that e-mail communications between council members were "meetings" that the FOIA requires to be held in public when the subject of the e-mails constituted "public business."

The court's ruling relied on an amendment to the statute that clarified that e-mail messages, telephone calls, and personal contacts among public officials are permissible so long as they are not "meetings" under the FOIA.

The statute, Va. Code §2.2-3700, et seq., mandates that all meetings of public bodies, excepting certain specific matters concerning personnel and the acquisition of real property, be conducted in public.

The defendants were the mayor of Fredericksburg, the vice mayor, and three members of the city council. The plaintiffs, a former mayor of Fredericksburg and two citizens, alleged that over a period of months, beginning in May 2002, the defendants had on several occasions met privately to discuss public business in violation of the FOIA. Several of these instances involved the exchange of e-mail messages among the defendants rather than face-to-face meetings.

In determining whether the alleged instances were meetings subject to the statute's requirements, Judge John W. Scott Jr. rejected the defendants' argument that e-mails are not communications subject to the statute.

Legislature Amended Law to Clarify

The court pointed to an amendment to Section 2.2-3710.B of the statute, which clarified that "nothing contained herein shall be construed to prohibit ... separately contacting the membership, or any part thereof, of any public body for the purpose of ascertaining a member's position with respect to the transaction of public business, whether such contact is done in person, by telephone or by electronic communication, provided the contact is done on a basis that does not constitute a meeting."

"Meetings" are defined as "the meetings including work sessions, when sitting physically, or through telephonic or video equipment ... as a body or entity, or as an informal assemblage of (i) as many as three members or (ii) a quorum, if less than three, of the constituent membership, wherever held, with or without minutes being taken, whether or not votes are cast, of any public body."

The court concluded without further analysis that under this definition, exchanges between the defendants of e-mail messages whose subjects constituted public business were subject to the FOIA.

The plaintiffs were represented by David Zachary Kaufman of Fairfax, Va., and Michael Barnsback of DiMuro, Ginsburg & Mook, Alexandria, Va. The defendants were represented by William M. Sokol of Fredericksburg, Va., and Howard Stahl, Steven K. Davidson, and John F. O'Connor of Steptoe & Johnson, Washington, D.C.

Indiana: Jury Selection

Computer Glitches in System for Selecting Jury Pool Require Reversal of Death Sentence

Azania v. State, Ind., No. 02S00-0009-SC-538, 11/22/02.

Rounding of numbers and alphabetization made African-American jurors half as likely to be called for jury service. Problems with the computer program that a county used to select its master jury pool resulted in the exclusion of jurors from the township where 75 percent of the county's African-American residents lived and require reversal of a defendant's death sentence, a majority of the Indiana Supreme Court held Nov. 22, 2002.

The defendant was convicted in Allen County, the site of the state's second largest city, Fort Wayne, of the murder of a police officer and was sentenced to death. The death sentence

was later overturned, and a new penalty phase proceeding was conducted in 1996. In a post-conviction petition challenging the second death sentence, the defendant presented evidence that the computer program the county used since 1980 to select the master jury pool was flawed and resulted in disproportionately fewer African-Americans being called for jury service.

Some of the problems with the computer program had to do with the way it rounded off numbers and attempted to select jurors in proportion to the sizes of the townships. In 1996, county officials estimated that they needed 14,364 jurors, but the program identified only 10,000. Because the program worked through lists of the voters in alphabetical order by the name of the township, all of the 4364 excluded jurors were from Wayne Township, where 75 percent of the county's African-American residents lived. The 4364 jurors represented 87 percent of the voters in Wayne Township. The result was that African-Americans made up only 4.4 percent of the jurors in the county's 1996 master pool, whereas census figures showed that African-Americans made up 8.5 percent of the county's population.

Census Data

In an opinion by Justice Theodore Boehm, the majority based its ruling on a statutory requirement that county jury selection systems be "impartial and random," Ind. Code Section 33-4-5-2(c). However, the majority decided that the appropriate statutory analysis, like Sixth Amendment analysis, inquires into "whether the flaws in a jury selection system are so minor as to be inconsequential or are material enough that a segment of the population has been materially excluded."

Other state and federal courts have held that criminal defendants relying on gross census data cannot establish a prima facie case of discrimination against Hispanics in view of evidence that the percentage of Hispanics who are U.S. citizens—and thus eligible for jury service—is significantly lower than the total adult Hispanic population.

However, the Indiana majority brushed aside a lower court's criticisms of the defendant's use of census figures in this case. "The post-conviction court may be correct that African-American citizens do not necessarily register to vote in proportion to their population, but Allen County did not maintain racial information about the voter list and we have nothing to go by except the census," the majority said. It noted that the U.S. Supreme Court and lower federal courts have repeatedly upheld the use of census figures in constitutional assaults on jury selection procedures.

Half the Chance of Being Called

The majority explained that federal courts have developed two competing tests under the Sixth Amendment to determine if a jury pool adequately represents the community. The "absolute disparity test" looks to the difference between the percentage of the distinctive group eligible for

jury duty and the percentage represented in the pool. In this case, the absolute disparity is 4.1 percent (8.5 percent minus 4.4 percent.)

Under the comparative disparity test, the disparity is calculated by dividing the absolute disparity by the percentage of the group eligible for jury duty, which in this case is 4.1 percent divided by 8.5 percent, or 48.2 percent. The majority emphasized that this meant that "as the result of flaws in Allen County's system, African-Americans as a group had roughly half the chance of being included on a jury panel than a truly random system would have produced."

Noting that the U.S. Supreme Court has called for heightened reliability in death penalty proceedings when evaluating Eighth Amendment claims, the majority said that—although the disparities in Allen County jury selection system might be deemed to substantially comply with the statute in a non-death-penalty case—the system was not sufficiently impartial or random to support a jury recommendation of the death penalty.

The majority explained:

"[T]he system's programming error excluded 4364 people—roughly one-third of the jury pool—from possible service, and reduced by nearly one-half the odds that an African-American would appear on the jury panel. Every one of the excluded jury pool members was from Wayne Township, the township in which three-fourths of Allen County's African-Americans over age 18 resided. The net result was that the flaws inherent in the selection system materially reduced the probability that African-Americans would serve on [defendant] Azania's penalty phase jury."

Accordingly, the system did not substantially comply with the statute, and a new penalty phase is required, the court held.

In dissenting opinions, Chief Justice Randall T. Shepard and Justice Brent E. Dickson argued that the inadvertent exclusion of the jurors from Wayne Township did not keep the county's selection system from substantially complying with the statute and that any error was harmless.

The defendant was represented by Jesse A. Cook, of the Public Defender's Office, Terre Haute, Ind., and Michael E. Deutsch, of the Public Defender's Office, Chicago. The state was represented by Steve Carter and Christopher L. Lafuse, of the Indiana Attorney General's Office, Indianapolis.

Securities Regulation

Five Broker-Dealers Settle Case Involving Storage of E-Mails; \$8.25 Million in Fines

In re Deutsche Bank Securities Inc., SEC, Admin. Proc. File No. 3-10957, 12/3/02.

Five Wall Street broker-dealers agreed Dec. 3 to pay fines totaling more than \$8 million resolving charges by the Securities and Exchange Commission and state and industry regulators that they violated recordkeeping requirements concerning their e-mail communications. Firms are required under the Securities Exchange Act of 1934 to preserve e-mails that relate to their business for at least three years, and to store them in an accessible place for two years.

In a joint statement, the SEC, the New York Stock Exchange, and NASD said the firms—Deutsche Bank Securities Inc., Goldman Sachs & Co., Morgan Stanley & Co., Salomon Smith Barney Inc., and U.S. Bancorp Piper Jaffray Inc.—agreed to fines of \$1.65 million per company, censures, and future reviews of their procedures.

The respondents consented without admitting or denying misconduct to cease and desist from future violations, the regulators said. The fines will be paid to the Treasury Department, NYSE, and NASD.

Inadequate Procedures

The regulators said the firms had “inadequate procedures and systems to retain and make accessible e-mail communications.” Without singling out the companies, they said some of the firms counted on employees to preserve copies of

their e-mails on computer hard drives, while others backed up their electronic mail on tape or other materials as part of their disaster-recovery plans.

The regulators said, however, that the firms that relied on individuals to copy their missives did so without having a system to ensure that the task was done. Such a procedure also led to files being erased when individuals left the firms. The concerns that backed up their electronic mail as part of their business-continuity measures, meanwhile, often recycled and overwrote the materials within a year.

Separate Investigations

Regulators said the violations came to light during investigations into separate enforcement matters in which e-mails constituted important evidence. The three regulators, along with numerous state securities regulators, have been probing allegations that Wall Street investment banks are operating under conflicts of interest in which analysts are pressured to give investors bullish advice in order to appease issuers. Critics say the issuers are more likely to give their investment banking business to firms that recommend their stocks.

In a prepared statement, Piper Jaffray Chief Executive Officer Andrew Duff said, “We are confident that our current e-mail procedures and enhanced software fully meet[s] all of the regulatory requirements for e-mail retention.” The company also said that it did store large volumes of e-mail, but not to the satisfaction of the regulators.

The other firms could not be reached or did not return calls for comment.

The text of the complaint is available at the web site of the Securities and Exchange Commission, <http://www.sec.gov/litigation/admin/34-46937.htm>.

Best Practices

Best Practices: Online Banking

Content on Bank Web Site Constitutes ‘Pattern or Practice,’ Fed Examiner Says

Content on a bank’s Internet site automatically amounts to a “pattern or practice” for purposes of federal law, a bank examiner for the Federal Reserve Bank of Atlanta said Dec. 3.

Senior Examiner Gary Louis, during a telephone seminar sponsored by the American Bankers Association, said that web sites instantly communicate the same content to a global audience.

By definition, content on a web site can never be considered an isolated occurrence, according to Louis.

“Anything on a web site is a pattern or practice,” Louis

said during a teleconference, *Auditing Your Bank’s Website for Compliance*.

Isolated violations of law or regulation—such as allegations of lending discrimination—are not viewed as seriously as a recognizable pattern or practice of discriminatory conduct.

Avoid ‘Weblining,’ Louis Says

In other remarks, Louis said financial institutions that offer certain products and services only through the Internet sites may be setting themselves up for the digital version of “redlining” claims.

Shortchanging customers who lack Internet access may be similar to practices of years past, when some financial services providers used red markers and maps to mark off and exclude whole communities, Louis said.

“You don’t want to cut somebody out because you’re only offering it on your web site,” Louis told participants in

the teleconference.

In addition to warnings about weblining claims, Louis urged bankers to judge content on their web sites with an eye toward the regulatory impact of that content, saying regulators tend to view a bank's Web site as a kind of examination in miniature.

"It's almost like looking at your entire bank through a different medium," Louis said.

International News: How Much Data Should an ISP Retain?

ICC Recommends Harmonized, Limited Approach to Law Enforcement Data Needs

Governments should adopt a uniform and limited standard for law enforcement needs for traffic data from communications service providers, according to a policy statement by the Paris-based International Chamber of Commerce (ICC) issued in late 2002.

According to the ICC, governments should limit what kind of data is covered by traffic data retention rules and tie them specifically to the purpose of the legislation mandat-

ing retention. Furthermore, providers should not be required to store anonymous data.

The policy statement makes a point to define "data preservation" as being preferable to "data retention." Data preservation, as defined by the ICC, relates to the storage of a particular subset of data at the specific request of a law enforcement agency. This is to be preferred over rules that generally require retention of traffic data on a routine basis, the statement said.

Furthermore, private service providers, which might have limited means and resources, should be excluded from requirements to retain data, according to the ICC. The statement also asks governments to bear the costs of infrastructure that would be required to comply with mandatory data retention, and asks that law enforcement agencies bear the marginal costs of complying with specific requests. Service providers should also be protected from liability resulting from compliance with mandatory data retention.

The ICC also urged governments to train law enforcement officials so that they would understand the technical limitations and capabilities of service providers to retain and turn over data.

The text of the policy statement is available at the web site of the International Chamber of Commerce, http://www.iccwbo.org/home/news_archives/2002/stories/traffic%20data.pdf.

Talking Tech

South Carolina Opens Nation's First Cybercrime Center

In late December 2002, the Columbia, S.C.-based Computer Crime Center, the first of its kind in the nation, opened its doors. The center will focus on forensic examination of evidence related to computer-based crimes, including Internet fraud, child exploitation, computer intrusions, child pornography, denial of service, and various telecommunications crimes. The FBI and Secret Service will staff the center, thus providing local law enforcement officers with subpoena

power, federal prosecution of cases, and expertise in electronic investigation. The center, paid for by a \$5.6 million federal grant, will also work with the South Carolina Law Enforcement Division, the U.S. Customs Service, the Postal Service, high-tech firms, and utilities. Financial institutions are encouraged to participate as well.

South Carolina sheriffs and police chiefs will be able to tap into the center's resources, while the facility's investigative team will make digital evidence recovery tools available to local law enforcement. The FBI is working to open similar facilities in Los Angeles and Minneapolis in the near future.

'Explosive' E-mails Allowed Into Evidence in Enron Loan Trial

Manhattan Federal District Court Judge Jed S. Rakoff ruled on Dec. 23 that e-mails written over the course of nine months will be allowed into evidence in the trial over J.P. Morgan Chase & Co.'s financing of Enron. The judge characterized the e-mails as potentially "explosive" in the billion-dollar insurance trial, in which 11 insurance companies are suing Chase for payment, since a central question in the trial is whether or not J.P. Morgan knew the future contracts for oil and gas were actually loans. A senior Chase official allegedly called the transaction a "disguised loan" in one of the e-mails. The decision is *J.P. Morgan Chase Bank v. Liberty Mutual Insurance Co.*, 01 Civ. 11523 (law.com).

Lawyers Accused of Hack Attack

On December 16, occupational illness expert David Egilman sued corporate defense attorneys at Jones, Day, Reavis & Pogue and others for illegally hacking into his web site and using the information to discredit him at trial. W. Kelly Stewart, of Jones Day's Dallas office, admitted he had accessed the site after a co-counsel had guessed the passwords. The unauthorized access might be a violation of the Computer Fraud and Abuse Act, say some experts (washingtonpost.com).

Lawyers Ordered to Disclose E-mails in Legal Malpractice Case

On December 13, Federal District Judge Harvey Bartle III in the Eastern District of Pennsylvania ordered lawyers being sued by their client for malpractice to turn over e-mails written during a 35-day period—after the firm had been threatened with suit but before the firm had retained separate counsel. In *Koen Book Distributors v. Powell Trachtman Logan Carrle Bowman & Lombardo*, No. 02-971, Judge Bartle, after reviewing all the e-mails, found that the messages were not privileged since they concerned "if and how to continue to represent the clients and how to respond to the clients' communications," which showed a clear conflict of interest. Further, the judge concluded that the e-mails were not protected by the work-product doctrine, since that "shelters the mental processes of the attorney, providing a privilege area within which he can analyze and prepare his client's case," and cannot be invoked when those "mental impressions and opinions are directly at issue." The doctrine also does not apply when the client, as opposed to some other party, seeks discovery of those mental impressions (*New Jersey Law Journal*, December 23, 2002, page 6, 170 N.J.L.J. 1006).

SEC Wants Web Disclosure of Insider Deals

The Securities and Exchange Commission proposed in late December that rules require web posting of corporate insiders' stock transactions. The move would make it easier and quicker to see who's buying and selling.

Chief executive officers, board directors and anyone holding 10 percent or more will be affected by the proposal, regulators said.

Companies currently have two business days to report with the SEC whenever an insider buys or sells stock in his company. At the moment, the information can be reported either in paper form or electronically, but this proposal seeks to do away with the paper option.

The proposal, however, will require electronic distribution and the data will be made available on the commission's web site, www.sec.gov, and on companies' sites. "Many investors believe that these reports provide useful information regarding management's views on the performance or prospects of a company," said exiting SEC Chairman Harvey Pitt at the final public meeting of 2002. SEC officials hope to have the requirement in place by the spring of 2003. (www.sec.gov)

Companies Share Information to Fight Cybercrime, Survey Says

Nearly half of security executives responding to an online survey said they have supplied data on customers, employees, or business partners to government or law enforcement agencies.

The survey results, released Dec. 18, suggest that businesses are more willing than in the past to share information that could help reduce cybercrime, according to *CSO* magazine, which conducted the study. Nearly a quarter of respondents said their organizations would supply information without a court order. In cases involving national security, 41 percent said their companies would do so.

"As cybercrime activity and concerns continue to mount, chief information officers are becoming more willing to part with information they normally would hold close to the vest," said Lew McCreary, editor-in-chief of *CSO* magazine.

Privacy Concerns Posed

While this increase in information sharing could help deter cybercrime, it also poses privacy concerns, according to McCreary.

"If standards loosen on what businesses do with customer information, how will customers protect themselves from mistakes and possible abuses?" McCreary said. "Law-

suits are sure to arise in this area.”

Chris Hoofnagle, legislative counsel for the Electronic Privacy Information Center, said companies put themselves in legal trouble when they divulge consumer information in violation of privacy policies or state or federal laws.

“There is a duty among data stewards to protect information from disclosure,” Hoofnagle said. “Companies are not supposed to become agents of the police. Unfortunately, many are willing to do so.”

Hoofnagle said he was not surprised that companies seemed so willing to share information with the government

and law enforcement.

“We had heard from industry lawyers after Sept. 11 that many companies were sharing information in violation of privacy policies and without informing their customers,” he said.

About 800 individuals, representing organizations with 500 or more employees, responded to *CSO* magazine’s online survey. It was conducted in late November and early December.

The survey results are available online at http://www.csoonline.com/releases/12180247_release.html.

Calendar

The Fifth Annual Sedona Conference on Complex Litigation to Critique White Paper on Guidelines for Electronic Document Production

The Fifth Annual Sedona Conference on Complex Litigation, to be held in Sedona, Arizona on Thursday-Friday, April 24-25, will be 50 percent devoted to an advanced discussion of issues relating to electronic document production. The other 50 percent of the conference will deal with issues relating to courtroom technology. The full agenda and faculty bios will be posted on The Sedona Conference web site by the end of January, at www.thesecondonaconference.org.

The dialogue will include a critique of the white paper containing guidelines for electronic discovery currently being developed by a Working Group of The Sedona Conference. The faculty of 15, co-chaired by **Prof. Stephen Saltzburg** (George Washington University Law School) and **Dennis Suplee** (Schnader), includes **Mary Boies** (Boies & McInnis), **James J. Brosnahan** (Morrison & Foerster), **Francis J. Burke** (Steptoe & Johnson), **Bryan G. Harston** (DecisionQuest), **The Hon. Jacob P. Hart** (Magistrate, U.S. District Court for the Eastern District of Pennsylvania), **Carol Heckman** (Harter Secrest & Emery), **Monica Wiseman Latin** (Carrington Coleman Sloman & Blumenthal), **Vance K. Opperman** (Key Investments), **Jonathan Redgrave** (Jones Day Reavis & Pogue), **The Hon. James M. Rosenbaum** (U.S. District Court Judge, District of Minnesota), **Kenneth Shear** (Electronic Evidence Discovery), Stephen Snyder (Gray Plant Mooty), and **Kenneth J. Withers** (Federal Judicial Center).

Thus, the critique of the guidelines on electronic document production and the dialogue exploring issues relating, *inter alia*, to discovery of backup tapes, e-mail, meta data

and deleted documents, will benefit from the views of the bench and both sides of the bar.

The first 10 readers of this newsletter who register for the April 24-25 Sedona Conference on Complex Litigation will receive a \$100 discount off their tuition—please write “newsletter registration” on the registration form to be eligible for the discount!

The Sedona Conference Working Group on Electronic Document Retention and Production was convened on October 17-18, 2002 in Phoenix Arizona, and its first output—a set of guidelines on electronic document production—will be available for review and comment in about a month. It is the intent of The Sedona Conference to solicit the views of any organization and individual who is interested and experienced in the topic, as well as subjecting the guidelines to critique at the April 24-25 conference on complex litigation before review, revision and republication of the guidelines later in the year. Through a combination of its new Working Group Series and regular season conferences The Sedona Conference hopes to be able to develop peer-reviewed guidelines on difficult issues confronted by our legal system. A second set of guidelines dealing with electronic document retention will be published later in 2003 and also subject to review and commentary.

Participation in The Sedona Conference on Complex Litigation is strictly limited to 40 registrants in addition to the 15-person faculty for an intimate conference conducive to stimulating, advanced dialogue. You can find further information on the conference, the new Sedona Conference Working Group Series, and how to register on The Sedona Conference web site (see above for address).

EVIDENCE ISSUES IN EMPLOYMENT CASES: A View from the Bench

March 27-28, 2003

• The Yale Club •
New York City.

Register

phone: 1-800-255-8131,
online: [http://conferences.pf.com/
employment/](http://conferences.pf.com/employment/)

Why You Should Attend:

■ As jury trials of employment disputes proliferate, attorneys on both sides of the aisle in these cases are encountering new and complex evidentiary issues. Judges are intensifying their scrutiny of expert evidence. Violations of the *ex parte* rule are an ever-present risk. And vast, often overwhelming forms of computer-based records become evidence that can make or break your case.

■ Attend this state-of-the-art course to learn new strategies that can help you handle this

evidence to your advantage in discovery, summary judgment proceedings, in limine motions, at trial, and in appellate proceedings. You'll see a distinguished faculty of plaintiff and defense attorneys present dicey evidentiary disputes to panels of federal judges, who will analyze and discuss the application of the evidence rules to the disputes. And you'll receive a course book that contains comprehensive analyses of each topic, as well as forms and checklists of indispensable use in your practice.

For More Information:

Pike & Fischer, Inc. • 1010 Wayne Avenue • Suite 1400 • Silver Spring, MD 20910

To register or inquire about CLE:

Telephone Jill Adler at 631-368-2082, ext. 21

Fax her at 631-368-2948

Or e-mail her at jill-adler@meeting-matters.com

<http://conferences.pf.com/employment/>

Pike & Fischer, Inc. has produced leading conferences for its parent company BNA, Inc. since 1999, and publishes *Digital Discovery and e-Evidence*. Pike & Fischer is the nation's chief private publisher of FCC Rules materials and is the leading source for information in the rapidly developing field of communications law and regulation. For more information and the conference agenda and faculty, please visit <http://www.pf.com>.