

# the DIGITAL INVESTIGATOR

NOVEMBER/DECEMBER 2010

## A New Approach to E-Discovery

Appointing a digital forensic investigator to conduct e-discovery and negotiate agreements could improve results and reduce litigation costs.

**D**iscovery has become the most time-consuming — and potentially contentious — aspect of litigation, thanks in large part to requests for electronically stored information (ESI). According to the Sixth Annual Litigation Trends Survey released by international law firm Fulbright & Jaworski, e-discovery accounts for 30 percent to 50 percent of litigation costs, and 16 percent of those surveyed expect to spend more on e-discovery this year.

The explosion of ESI produced and stored by the typical organization has certainly impacted e-discovery, as has a growing body of industry and government regulations mandating long-term data retention. Arguably, however, e-discovery challenges are rooted in common e-discovery practices that are inherently flawed, leading to poor document search results and time-consuming and expensive discovery litigation.

“Parties typically respond to discovery requests by performing keyword searches of their ESI archives. Often, this yields only a small fraction of discoverable documents, leading to disputes over search methodology,” said Tom Smith, a forensic scientist with Ispirian Computer Forensics and a member of the American College of Forensic Examiners Institute (ACFEI). “On the other hand, broad searches can result in ‘document dumps’ that increase costs and headaches on both sides.”

Smith believes that mediated investigative e-discovery\* could help relieve those headaches. In this scenario, a digital



Continued on page 2

# A New Approach to E-Discovery

---

forensic examiner would conduct document searches on behalf of both parties and mediate agreements regarding document production. Utilizing digital forensic techniques rather than keyword searches to conduct e-discovery would maximize results while minimizing disputes.

## Google Isn't the Answer

Everyone who's ever used Google knows how to perform a basic keyword search. However, conducting a Google search is vastly different than finding every electronic record associated with a matter, while weeding out those documents that are irrelevant.

"Keyword searches are within the comfort zone of attorneys and the courts because they are used to searching on Google, Lexis and Westlaw," said Smith. "The problem is that those familiar search tools are designed to aid the user in finding the answer to a particular query. Google's powerful search engine, for example, recommends keywords and uses synonyms to find the most relevant documents, and then ranks and filters the results. The user then employs an iterative process to hone in on the answer. E-discovery, with its requests, responses and objections, simply doesn't work that way."

The shortcomings of keyword searches are demonstrated by litigation over what search terms may be used, and in what combinations. When initial search terms yield limited results, opposing counsel will recommend other search terms, leading to protracted arguments over the precise construction of search parameters, and whether the search will yield relevant documents or an overly burdensome document dump. Increasingly, both sides end up calling in e-discovery experts who also jump into the fray.

"Courts hear these disputes every single day," Smith said. "Judges are very smart people, but are they experts in document searches? And is this an efficient use of judicial resources? I think the answer to both questions has to be 'no.'"

## Bring in the Expert

Digital forensic examiners like Smith are experts in tracking down electronic information using tools that are much more powerful than keyword searches. Widely used forensic tools rapidly scan storage media for potential evidence, then classify the evidence by status (such as deleted, encrypted or duplicate) and category (such as documents, databases, graphics or e-mail). These tools increase the efficiency of an investigation by enabling the examiner to prioritize the files and examine the most relevant evidence first.

"These tools filter out things like system and application files and duplicates so that the examiner can focus on files with the greatest potential evidentiary value. The examiner can then search through the evidence in a variety of ways, not just by

keywords," Smith said. "What's more, digital forensic examiners employ a variety of tools and techniques depending upon the nature of the investigation. There are tools that enable them to find bits of deleted files and reassemble them, for example."

Although the value of this expertise is clear, Smith contends that e-discovery challenges are only exacerbated if each side calls in its own expert.

"You wind up with a battle of the experts," he said. "Experts are paid a lot of money to advocate on behalf of the party that hires them. As a result, the experts are not likely to agree, so the parties still have to litigate search techniques. Sure, the techniques recommended by the experts are likely to be more refined than those that the parties could come up with themselves, but the fundamental problems remain. The costs have just gone up."

## Focus on Results

Mediated investigative e-discovery has unique features that promise to reduce those costs. The skilled digital forensic examiner can preserve data and find relevant ESI more effectively and efficiently than, say, an in-house IT expert. Armed with knowledge of the discoverable ESI of both sides, the neutral, third-party examiner is well-positioned to mediate solutions to any problems that arise. As a result, document production costs go down and attorneys spend less time filing motions to compel and litigating e-discovery disputes.

"After the so-called '26(f) conference,' when the parties lay the initial ground rules for discovery, the examiner would establish the chain of custody and forensically copy the data, as in any investigation," Smith said. "The examiner would then meet with each party to gain an understanding of their 'theory of the case.' Those theories would form the basis for the initial investigation, but the examiner would develop hypotheses about the data itself, and test those hypotheses in an iterative process."

The whole process would proceed under the direction of counsel. The examiner would give counsel the retrieved data to produce if appropriate or withhold if it is privileged, irrelevant or attorney work-product.

"This concept would solve a whole host of problems, including questions about data spoliation and 'hide the ball' activities," Smith said. "Forensics is all about bringing truth to the forum. Mediated investigative e-discovery promises to do that at lower cost and with greater success than current techniques."

---

\* This term was used in an article by Marian Riedy, Suman Beros, and Kim Sperduto in a 2010 issue of *The Federal Courts Law Review*.

## BRIEFS

### Social Media Good for Business

**B**usinesses that are not using social networking sites or adopting enterprise 2.0 tools fast enough may be putting themselves at risk of lost opportunities, according to a survey conducted by the technology analyst firm Yankee Group for Siemens Enterprise Communications, a business software company.

Seventy percent of the consumers surveyed said they are increasingly seeking information about businesses on social networks such as Facebook and Twitter. However, only 30 percent of the businesses surveyed say they are prepared to interact with consumers over such networks. Researchers also noted that 50 percent of consumers surveyed said that they use social media at least once a day, and 65 percent reported they were satisfied with their business interactions on social networks.

"Social media is changing the way businesses, customers and employees interact, and this creates significant opportunities for contact centers and the enterprise as a whole to leverage the integration of these tools into business processes," Yankee Group analyst Zeus Kervavala said in a statement. "As integration of social media improves within the contact center and with unified communications and collaboration, businesses can improve customer interactions and positively impact employee productivity and collaboration."

### Mobile Phones Replacing Memory?

**A**n increased reliance on information stored on mobile phones and online has led to a phenomena British researchers are calling "numerical amnesia." A recent study conducted by the British firm CPP Group found that millions of people can't recall important phone numbers due to an increased dependence on mobile phones over memories.

In the study, 23 million Britons could not remember their partner's mobile number, 30 million couldn't recall their best friend's number and 22 million couldn't remember their parents' mobile number. The study shows that it's not just mobile phone numbers that we are failing to remember. More than half of UK adults (53 percent) struggle to memorize their bank account number and 44 percent can't remember their national insurance number.

"As technology gets more sophisticated, our own memories are on the decline as we increasingly rely on information stored on phones and online," said psychologist Dr. Glenn Wilson. "While this reliance can be problematic if people are totally dependent on an external memory store that is lost or becomes temporarily unavailable, it can also affect an individual's mental agility later in life. Like many other skills, memory needs exercising if the capacity is not to be lost."

### The Digital Investigator

Copyright © 2010 CMS Special Interest Publications.  
All rights reserved.

#### Editorial Correspondence:

4941 S. 78th E. Ave., Tulsa, OK 74145  
Phone (800) 726-7667  
Fax (918) 270-7134

#### Change of Address:

Send updated address label information to the above address.

Some parts of this publication may be reprinted or reproduced in nonprofit or internal-use publications with advance written permission.

The Digital Investigator is published by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.



## GET A CLUE

With issues regarding electronic discovery becoming a central aspect of civil and domestic litigation, legal and paralegal professionals increasingly require the ability to identify, collect, preserve and examine data found on computer hard drives and digital storage media.

#### Ispirian's digital forensic investigators can help.

Our focus on the digital forensics discipline gives us the training, litigation support experience, report-writing skills and professional involvement necessary to support the e-discovery process and deliver quality, defensible results.

Ispirian's comprehensive case management solution streamlines communication and provides attorneys and support staff with real-time updates as your cases progress. Using a secure Internet portal, Ispirian investigators and their clients can exchange information, update schedules and view key evidence with 24-hour access to budgets, documents, photos and reports.

When it comes to making sense of digital evidence, it makes sense to call Ispirian Computer Forensics: (636) 736-2180.



*Ispirian is a member of the High Technology Crime Investigation Association (HTCIA).*



Ispirian Incorporated  
Chesterfield, MO 63017  
Ph: 636.736.2180  
Fax: 636.736.2181

Ispirian Computer Forensics is a licensed Missouri professional investigative agency (MO PI Agency License #2010008265) specializing in digital forensics, data recovery and computer misuse investigations. Our headquarters is located in Chesterfield, Missouri USA. Copyright 2010, All Rights Reserved.

# Taking Chances



Studies indicate even savvy computer users take unnecessary risks online.

**W**hile most computer users consider online privacy to be of extreme importance, many do little or nothing to protect themselves, according to a recent study from the Ponemon Institute. Meanwhile, another recent study shows some of the most tech-savvy cities in America also rank among the riskiest for cybercrime.

The Ponemon study reveals that Americans are particularly lax when it comes to the amount and type of personal information they share on social media sites. Although more than 80 percent of respondents expressed concern about their security while using social media, more than half of these same individuals admitted they do not take any steps to actively protect themselves.

Remarkably, 90 percent of respondents were under the impression that using social media sites posed no risk,



and 60 percent weren't even sure if the social media provider was able to protect their identity. Approximately 40 percent admitted sharing their physical home address through social media applications.

"The study results are extremely telling, especially about measures that users take, or fail to take, in order to protect their identity while using social networks," said Dr. Larry Ponemon, chairman and founder of the Ponemon Institute.

## Techs and the City

Online risk is particularly high in some cities regarded as hotspots of technology innovation and knowledge, according to a separate study from Symantec's Norton product group. Seattle, Boston and Washington D.C. ranked as the riskiest cities in America for cybercrime, with San Francisco; Raleigh, N.C.; Atlanta; Minneapolis; Denver, Austin, Texas; and Portland, Ore., rounding out the top 10.

Symantec, which partnered with Sperling's BestPlaces to come up with rankings for the nation's 50 largest metro areas, said the survey demonstrates that even skilled and experienced Internet users are at risk when it comes to cybercrime and online insecurity. Norton Internet safety advocate Marian Merritt noted that cybercrime is generally on the rise everywhere, affecting one in five online shoppers and costing Americans \$560 million in 2009 due to online fraud.

"With more people than ever relying on the Internet to stay in touch, shop and pay their bills, feeling confident and secure in our information-driven world is vital," Merritt said. "This study highlights the cities most at risk of cybercrime and reminds individuals, families and businesses across the country of the hazards they face each time they go online."

The rankings relied on data from Symantec's Security Response team for factors such as the number of malicious attacks, infected machines and spam-

“Despite people’s familiarity with technology and the Internet, this study shows that everyone is exposed to a certain level of risk when they are online ... it’s important to be vigilant in everyday online behavior in order to protect yourself against cybercrime of all types.”

generating zombie computers per capita. Sperling's contributed data on the prevalence of computer ownership, Internet use and potentially risky online activities, including online banking and online shopping.

## The Wi-Fi Factor

The report noted a clear correlation between the number of public Wi-Fi hotspots and the incidence of cybercrime. San Francisco tops the list for riskiest online behavior and highest number of Wi-Fi hotspots per capita. Atlanta residents experience the most cyber attacks and potential infections. Minneapolis and Portland are near the top for risky online behavior, while Denver and Austin score high across the board.

At the other end of the spectrum, Detroit residents were less likely to participate in risky online behavior compared to other cities in the study, and it also ranked low in cybercrime, access to the Internet, expenditures on computer equipment, and wireless Internet access.

"Despite people's familiarity with technology and the Internet, this study shows that everyone is exposed to a certain level of risk when they are online," said Bert Sperling, founder and researcher of Sperling's Best Places. "No matter where you live — be it Seattle or Detroit — it's important to be vigilant in everyday online behavior in order to protect yourself against cybercrime of all types."

ProtectMyID.com, which sponsored the Ponemon Institute study, offers these suggestions to help users guard their personal information and reduce their exposure to cybercrime:

- **Log off when you leave.** Always log off or enable a secure screen saver when away from the computer or it is not in use. More than 80 percent of respondents leave their computers unsecured.
- **Install and update antivirus software.** Keep antivirus software up-to-date in order to maximize protection against keystroke loggers and other malware commonly used for identity theft. Nearly 70 percent of respondents stated that they do not use any form of antivirus protection on their computer.
- **Make sure your wireless network connection is secure.** If you are operating on a wireless network, always make sure that the network is secure to avoid exposing your personal information while it is in transmission. Approximately 75 percent of individuals said they use an unsecured network.
- **Review and customize security settings.** Research the default account settings when visiting social media sites and make sure to customize personal privacy settings in order to only share information with people you choose.
- **Pick a password that can't be cracked.** Do not choose a password that incorporates common information, such as a pet's name or your hometown. Approximately 40 percent of those surveyed said they use a password known to individuals other than themselves.



# Clearing the Air

*Industry alliance seeks standards to eliminate the security concerns impeding cloud computing adoption.*

**C**loud computing offers enticing advantages such as reduced maintenance costs, increased flexibility and extreme scalability, yet many IT professionals remain fearful that sensitive data will fall into the wrong hands if their organizations rush into the cloud.

Their fears aren't unfounded. For all its benefits, cloud computing has unique attributes that require risk assessment in areas such as data integrity, recovery and privacy. Cloud platforms can also have an impact on legal issues in areas such as e-discovery, regulatory compliance and auditing.

In a recent survey of hundreds of IT professionals, the Cloud Security

Alliance (CSA) found near-unanimous agreement that security is the principal concern impeding the widespread adoption of cloud computing. Ninety-three percent of respondents said the need for cloud computing security standards is important, and 82 percent said the need is urgent.

## **Standards Needed**

"It's clear from the survey's findings that enterprises across sectors are eager to adopt cloud computing — but that security standards are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers," said Jim Reavis, founder and executive director of CSA, a not-for-profit organization formed to promote

best-practice security measures in the cloud. "Cloud computing is shaping the future of IT but, as this study shows in a variety of ways, the absence of a compliance environment is having dramatic impact on cloud computing's growth."

Among the survey's findings:

- Forty-four percent of respondents said they are already involved in development of cloud computing standards, and 81 percent said they are somewhat or very likely to participate in development of cloud security standards in the next 12 months.

- Data privacy, security and encryption comprise the most urgent areas of need for standards development.

- The ISO 27001/27002 Information Security Management Standard is a key regulatory driver of standards compliance, as are Data Breach Notification, the Payment Card Industry Data Security Standard (PCI DSS), EU Data Privacy Legislation, Sarbanes-Oxley (SOX) and the Health Insurance Portability and Accountability Act (HIPAA).

While most organizations are experimenting with cloud computing, executives said they are still in the early stages of adoption. Security and management issues are leading many organizations to keep their cloud initiatives within their own firewalls. According to the CSA survey, private and hybrid cloud implementations are quickly gaining in popularity and will see increasing adoption over the next 12 months.

"Cloud services are clearly the next generation of information technology that enterprises must master," said Reavis. "We have a shared responsibility to understand the security threats that accompany the cloud and apply the necessary best practices to mitigate them."

## **Chief Threats**

The CSA also recently announced findings that detail the chief potential threats surrounding the use of cloud services. Specific security threats include exploits such as the Zeus botnet and

InfoStealing Trojan horses, malicious software that has proven especially effective in compromising sensitive private resources in cloud environments.

However, not all threats in this category are rooted in malicious intent. As the social Web evolves, more sites are relying on application programming interfaces (APIs), a set of operations that enable interaction between software programs, to present data from disparate sources. Sites that rely on multiple APIs often suffer from “weakest link security” in which one insecure API can adversely affect a larger set of participants. Together, these threats comprise a combination of existing vulnerabilities that are magnified in severity in cloud environments as well as new, cloud-specific techniques that put data and systems at risk.

Rounding out the list of common cloud threats covered in the report are malicious insiders, shared technology vulnerabilities, data loss and leakage and account/service and traffic hijacking.

### Cooperative Effort

To help cloud providers develop industry-recommended, secure and interoperable identity, access and compliance management configurations, CSA has announced a vendor-neutral initiative to deliver the industry’s first cloud security certification, education and outreach program. Known as the “Trusted Cloud Initiative,” it is a cooperative effort of CSA’s membership, which represents a cross section of industry stakeholders, end-user organizations, cloud services, SaaS and technology providers. These include Novell, Microsoft, Dell, Rackspace, Qualys, HP, Intel, Cisco, McAfee, Google, ISACA, DMTF and Symantec, as well as individual representatives from Global 2000 organizations and the world’s governments.

The certification criteria, seal and roadmap will be defined by members of the CSA. The educational outreach components of the program will be geared toward helping information security, IT audit and software development professionals within enterprises and cloud providers better understand the security, identity and access, compliance, data governance, portability and interoperability requirements organizations must maintain to demonstrate compliance and mitigate risk in the cloud.

“How identities are managed either in the cloud, or federated with the cloud, create significant barriers for enterprise adoption of cloud services,” said Alan Boehme, SVP IT Strategy and Enterprise Architecture, ING Americas, and current CSA board member. “By building a consensus security reference guide and certification roadmap, we are creating common ground for both enterprises and cloud providers, and expect to accelerate cloud adoption.”



## Funny, it doesn't look like a smoking gun.

Cell phones, GPSs, PDAs and other handheld devices have become practically indispensable as business and personal productivity tools these days. In many cases, they can also be repositories of a variety of dirty little secrets in the form of data, text messages and photographs. As such, they have become increasingly important in a broad range of criminal and civil investigations.

Handheld devices are really tiny computers with their own operating systems, file systems, file formats and methods of communication. Performing a forensic examination on one of these devices takes special software and special knowledge of the way they work, as well as where possible evidence could be stored.

Ispirian Incorporated’s computer forensic experts have the specialized tools, training and expertise to properly identify, collect and protect evidentiary data from handheld devices. Call us today to learn more.



*Ispirian is a member of the High Technology Crime Investigation Association (HTCIA).*



Ispirian Incorporated  
Chesterfield, MO 63017  
Ph: 636.736.2180  
Fax: 636.736.2181

Ispirian Computer Forensics is a licensed Missouri professional investigative agency (MO PI Agency License #2010008265) specializing in digital forensics, data recovery and computer misuse investigations. Our headquarters is located in Chesterfield, Missouri USA. Copyright 2010, All Rights Reserved.



You see bits  
and bytes

We see  
**EVIDENCE**

Let us show you what you've been missing

**ISPIRIAN**  
COMPUTER FORENSICS

It is estimated that 90 percent of the world's information is now created and stored in electronic format. Ispirian's computer forensic experts have the tools, training and expertise to find the needles in any digital haystacks. Ispirian understands how data is stored, where to look for digital evidence and how to recover that evidence from various types of file systems while ensuring that it is not altered in any way. We also understand the unique case management demands and processes legal professionals require during litigation. This allows us to identify, locate, extract and preserve data from computer systems and media for proceedings that range from intellectual property theft to cybercrimes to criminal investigations. Call us today to learn more.

Ispirian Incorporated

◆ Chesterfield, MO 63017 ◆

Ph: 636.736.2180

◆ Fax: 636.736.2181

MO PI Agency License #2010008265