CYBERSECURITY

## Data Breaches Shake Consumer Confidence

Most consumers are reluctant to continue to do business with a company that has suffered a financial data breach, according to a recent global survey by SafeNet of more than 4,500 adult consumers. Almost two-thirds (65%) of the respondents said they would never or were very unlikely to do business again with a company whose customers' financial information had been breached.

The SafeNet Breach Level Index for the second quarter of this year reported a total of 237 breaches between April and June, compromising more than 175 million customer records containing personal and financial information. Only two of the 237 incidents were considered secure breaches where encryption protected the stolen data from being used.

Three of the top five breaches were in the United States, the other two in Europe. Additionally, the United States accounted for 85% of the records compromised worldwide, followed by Germany with 10%. At the industry level, retail was the biggest loser with more than 145 million records lost or stolen, followed by government, which accounted for 11% of the records lost or stolen.

CLOUD

## Court on Cloud Computing: Ignorance Is No Excuse

A recent ruling in the case *Brown v. Tellermate Holdings, Ltd.* should serve as an excellent reminder that organizations using cloud computing (and their attorneys) are expected to understand the way cloud computing works, especially during e-discovery.

This became abundantly clear when the plaintiffs requested that Tellermate produce documents from the cloud-based application Salesforce.com. Tellermate objected, stating that it didn't possess or control the data maintained in the cloud database and that the data belonged to Salesforce. Apparently Tellermate and its attorneys failed to check their agreement with Salesforce.com, which clearly stated that Tellermate had access to the data and, in fact, retained ownership of it.

The court not only denied Tellermate's objection, it went on to question whether the data had been properly preserved. It turned out that when an employee separated from the company, Tellermate deactivated or reassigned access to the database account. That meant the data input by the plaintiffs had remained accessible and could have been changed by the employee who took over the account. Thus the reliability of the information that could be produced could not be guaranteed.

The message should be loud and clear: ownership of and responsibility for preservation of data stored in the cloud is the customer's. This holds true regardless of the software application.

"Technology, like cloud-based computing, can be a valuable resource, but it is important to understand its intricacies in order to prevent misrepresentations to the court," concluded attorney Matthew Barley in a posting on the Butler Snow LLP blog. "As the court in *Tellermate* noted, both the failure to produce and failure to preserve the information in salesforce.com was 'premised on the basic inability to appreciate whose information it was and who controlled it.'"

MOBILE DEVICES

## NIST Offers Guidelines for Vetting Mobile Apps

The use of mobile devices at work may improve productivity, but it can also challenge the organization's data security and privacy. Third-party mobile applications need to be thoroughly vetted before they are allowed in the workplace. This is true for all sectors, including government. That's why the National Institute of Standards and Technology (NIST) drafted guidelines for vetting third-party apps.

"Agencies need to know what a mobile app really does and to be aware of its potential privacy and security impact so they can mitigate any potential risks," Tony Karygiannis, a computer scientist in the NIST's Computer Security Division, told *InformationWeek*. "Many apps may access more data than expected and mobile devices have many physical data sensors continuously gathering and sharing information."

For example, individuals could be tracked without their knowledge through a calendar app, a social media app, a Wi-Fi sensor, or other utilities connected to a global positioning system. "Apps with malware can even make a phone call recording and forward conversations without its owner knowing it," Karygiannis said.

The draft offered the following recommendations:

- Understand the security and privacy risks mobile apps present and have a strategy for mitigating them.
- Provide mobile app security and privacy training for your employees.
- Vet all mobile apps and their updates to ensure they remain suitable throughout their life cycle.
- Establish a process for quickly vetting security-related app updates.
- Advise stakeholders what the mobile app vetting does and doesn't provide in terms of security.
- Have a software analyst review mobile app testing results within the context of the organization's mission, security policies, and risk tolerance.

E-DISCOVERY

## FRCP Proceeds to U.S. Supreme Court

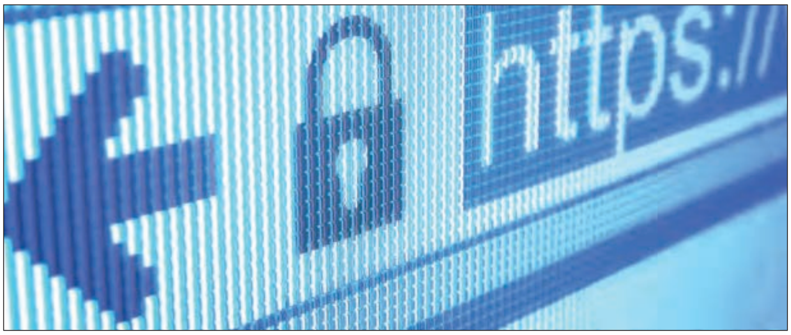
On September 15 the U.S. Judicial Conference approved the proposed changes to the U.S. Federal Rules of Civil Procedure. The revisions, which next will be considered by the U.S. Supreme Court, include language intended to narrow the scope of pretrial discovery to ensure demands are "proportional" to the needs of a particular case.

Proponents contend the proposed changes will help lower the skyrocketing costs of litigation. Opponents, on the other hand, state the changes would benefit big business at the expense of plaintiffs with legitimate claims, reported *LegalTimes*.

If the Supreme Court approves the changes, they will proceed finally to Congress. Unless Congress opposes the amendments or decides to make adjustments, the changes will take effect December 1, 2015.

PRIVACY

## EU Accuses Google of Distorting Privacy Rule



The European Union's Justice Commissioner, Martine Reichert, recently chastised Google and other search engines for intentionally undermining the EU high court's recent right-to-be-forgotten (RTBF) privacy rule. Reichert contends that the search engines are purposely distorting the essence of the law by claiming it will allow anyone to get virtually anything deleted from the web if they deem it unfavorable or inconvenient.

This controversial ruling is part of the EU's effort to reform its data protection laws. It allows individuals to be "forgotten" by petitioning search engines such as Google to remove links to web pages containing personal information that is inaccurate, irrelevant, outdated, etc. Only the links need be removed; the actual web pages remain intact. The search engine can reject the request if it determines the public interest trumps the individual's right to privacy, at which point the applicant can appeal to a national data protection authority.

[Google and others] are "trying to use the recent ruling by the European Court of Justice on the right to be forgotten to undermine our reform," Reichert stated in her recent address to the IFLA World Library and Information Congress. "They have got it wrong. And I will not let them abuse this crucial ruling to stop us from opening the digital single market for our companies and putting in place stronger protection for our citizens."

Reichert pointed out that the court "explicitly ruled that the right to be forgotten is not an absolute, but that it will always need to be balanced against other fundamental rights, such as the freedom of expression and the freedom of the media." Striking that balance may not always be easy, she acknowledged.

INFO SECURITY

## Information Security Costs Rising

Look for worldwide spending on information security to reach $71.1 billion this year, Gartner advised; that's an increase of about 8% over 2013. It's expected to increase another 8% in 2015. Gartner's latest research indicated that data loss prevention is the fastest growing segment.

According to the research analysts, the increasing adoption of mobile, cloud, and social [computing] (often interacting) will drive the use of new security technology and services through 2016.

Gartner Research Director Lawrence Pingree said the bigger trend that emerged in 2013 was the democratization of security threats, driven by the easy availability of malicious software (malware) and infrastructure (via the underground economy) that can be used to launch advanced targeted attacks.

"This has led to increased awareness among organizations that would have traditionally treated security as an IT function and a cost center," he said.

Other trends being forecasted are:

- By 2015, about 10% of IT security will be delivered in the cloud.
- Regulatory pressure in Western Europe and Asia/Pacific will intensify.
- Mobile security will be a higher priority for consumers beginning in 2017.

INFO SECURITY

# Healthcare Industry Battles Breaches

There was a 30% increase in the number of breaches on the Identity Theft Resource Center's 2013 breach list released earlier this year compared to 2012. And the highest percentage occurred in the healthcare industry: 44% compared to 34% for the business sector, which has topped the list since 2005.

One reason for the dramatic increase is the tougher reporting requirements of the final rule of the Health Insurance Portability and Accountability Act (HIPAA) that became effective in 2013. The U.S. Department of Health and Human Services (HHS) recently submitted its annual breach report to Congress for 2012. It showed that theft continues to be the leading cause of breaches of unsecured protected health information; the percentage increased to 52% in 2012 from 49% in 2011.

What happened in 2013? HHS is still compiling the data, but in the meantime, a 2014 benchmarking study of 505 healthcare organizations conducted by Ponemon Institute showed a slight decrease in the number of breaches reported in 2013.

The cost of data breaches to healthcare organizations continues to average about $2 million over a two-year period. Based on the experiences of the 2014 participants, Ponemon estimates the cost to the healthcare industry could be as much as $5.6 billion annually.

Employee negligence is the greatest security risk, according to the benchmarking study. Three-quarters of the organizations ranked it their greatest worry, followed by use of public cloud services (41%) and mobile device insecurity (40%). Despite that, 88% of the organizations permit employees and medical staff to use their own mobile devices, such as smartphones and tablets, to connect to the organization's networks.

Participants also expressed their lack of confidence in business associates to protect data against breaches. Interestingly, the HHS report revealed that healthcare providers accounted for the majority of breaches in 2011 and 2012, 63% and 68%, respectively; business associates accounted for 27% and 25%, respectively.

One thing is certain: Healthcare organizations are continuing to struggle to comply with the HIPAA final rule.

PRIVACY

# Young Americans Protective of Privacy

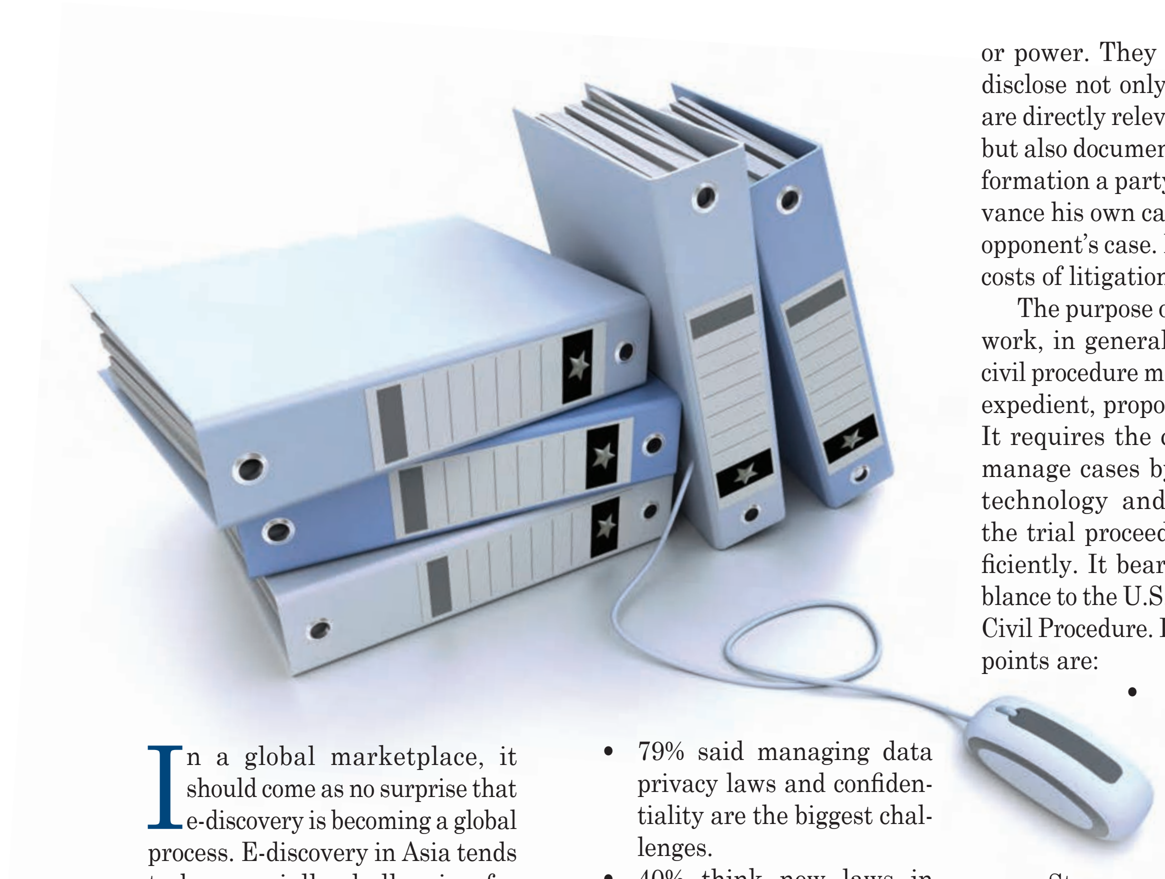
They may live their lives online and share their most intimate secrets with a broad group of "friends," but younger Americans are actually protective of their privacy, according to a study by the Public Affairs Council (PAC).

The survey asked participants if they would be willing to sacrifice their privacy "to protect national security" or obtain "lower-cost products and services." Surprisingly, the answer to both was generally "no," said PAC's Alan Crawford. Regarding the question of national security, 42% said they would give up "some privacy in order to help protect national security," while 56% would not. Almost three-quarters (72%) said they would not trade their privacy to save money on goods and services.

In both instances, younger Americans were more concerned about preserving their personal privacy. In matters of national security, millennials (born 1981-1996) were the most vocal (61%), followed by Gen X-ers (1965-80) (57%), and then Baby Boomers (1946-64) (55%). Age was less of a factor in the second question: 71% of millennials would opt to preserve their privacy, as would 76% of Gen X-ers and 73% of Baby Boomers.

E-DISCOVERY

# Study Highlights Implications of E-Discovery in Asia



In a global marketplace, it should come as no surprise that e-discovery is becoming a global process. E-discovery in Asia tends to be especially challenging for multinational enterprises because of growing data privacy concerns, new regulations, and Chinese state secrecy laws.

"E-discovery is an increasingly global process, whereas the challenges become less about data volume and more about jurisdiction," said Rod Sutton, senior managing director and regional chairman for FTI Consulting in Hong Kong.

FTI recently released the findings of a study that highlights more than 20 factors encountered in dispute resolution unique to Asia. FTI queried 70 Asia-based law firm and corporate e-discovery professionals about the evolving e-discovery trends in this complex region. Key findings of the study included:

- 67% of respondents cited regulatory investigations as the biggest driver of e-discovery.
- 79% said managing data privacy laws and confidentiality are the biggest challenges.
- 40% think new laws in China will have a large impact on managing electronic data in legal review – particularly the Law of the People's Republic of China on Guarding State Secrets, which broadly requires documents to be reviewed and cleared of secrecy concerns before leaving China.

### *Discovery in Hong Kong*

To facilitate the discovery process in Hong Kong, the Hong Kong judiciary recently introduced a "framework for reasonable, proportionate, and economical discovery of electronic documents."

Hong Kong's current discovery rules do not distinguish between paper and electronically stored information (ESI). Both parties are expected to disclose all documents within their possession, custody, or power. They are obligated to disclose not only documents that are directly relevant to the issues, but also documents containing information a party could use to advance his own case or damage his opponent's case. Hence, the rising costs of litigation.

The purpose of the new framework, in general, is to make the civil procedure more cost-effective, expedient, proportional, and fair. It requires the court to actively manage cases by making use of technology and directing that the trial proceed quickly and efficiently. It bears a clear resemblance to the U.S. Federal Rules of Civil Procedure. Its key take-away points are:

- Discovery issues should be considered as soon as litigation is contemplated.
- Steps must be taken to preserve documents, including ESI, including any scheduled for destruction in accordance with a document retention policy or in the "ordinary course of business"; ESI should be preserved in its native formats.
- The parties and their legal representatives should be technically competent and discuss the use of technology in facilitating the discovery of ESI.
- The parties should agree among themselves how the costs of discovery will be shared.

While these concepts sound familiar, they represent a cultural shift away from the practice of adversarial discovery that has been pervasive in Hong Kong, explained Sidley Austin LLP.

MOBILE DEVICES

# Get Ready for Wearable Technology in the Office

First it was the personal computer, then the notebook computer, smartphones, and tablets. What's next? It may well be wearable technologies, most notably smart glasses, smart watches, and fitness bands. Deloitte predicts that in 2014, more than 10 million units of wearables will be sold, totaling about $3 billion in sales. Analysts further estimate that wearables will eventually be able to handle two-thirds of what we currently do on smartphones.

Of course, wearable technology is just emerging, but if it catches on as quickly as smartphones, tablets, and other performance-enhancing technology, it won't be long before we see a new fashion trend in the workplace. Now is a good time to prepare for that eventuality.

Just as personal mobile devices have challenged organizations, so too will wearable data devices (WDDs). Forbes reported this summer that insurance giant USAA had prohibited WDDs in the workplace until it had fully researched the potential advantages and disadvantages of the new technology. Some of the concerns USAA had were:

- Employees inadvertently recording inappropriate audio in the workplace
- Employees capturing sensitive images in the workplace
- Potential safety hazards while driving or walking on company property
- Infringement on employee privacy

*Forbes's* Jeanne Meister offered the following advice to companies that are forming their policies on wearable devices: Remember what happened when companies tried to ban the use of Facebook and YouTube on desktops in early social media policies? Employees accessed the sites anyway on their smartphones, which affected their on-the-job productivity. The same could easily happen with wearables.

"Smart employers will put policies in place now to manage the integration of WDDs into the workplace and adjust them as needs dictate," said Mintz Levin attorney Jonathan Cain in a recent privacy and security advisory. "Less prepared employers will be deeply exposed to liability for data breaches, privacy and workplace discrimination complaints, and other disruptions as they try to catch up."

He added that human resources and IT policies should address at least the following concerns:

- **Detection:** WDDs may not be readily detectable, unlike smartphones and tablets. Therefore, "[w]orkplace policies should set out the circumstances under which various categories of devices may be used, and what notice is required to co-workers and customers when they are brought into the workplace."
- **Security:** Most WDDs will have wireless capability, which could challenge the security of corporate data. Policies need to clarify where and under what circumstances that wireless capability may be used.
- **Privacy:** Co-workers' and customers' reasonable privacy expectations may be challenged when employees are allowed to use WDDs to record their interactions. The employee's privacy expectation for the data collected by the WDDs may also be inconsistent with the employer's views about its right to monitor and record data broadcast within its workspaces.
- **Productivity:** As with smartphones, balancing the use of smartphones to access personal e-mail or web browsing with productivity will likely become even more challenging with WDDs. It may be necessary to modify workplace policies to address the use of company resources and company time with the "pursuit of personal interests using WDDs."
- **Support:** As more WDDs are brought into the workplace, demands on IT to support those devices will increase. "Employers need to consider whether and how they will integrate these new classes of devices into their IT environments."
- **Liability:** "Policies should address the circumstances under which interactions with third parties may be recorded. Employers also should consider how they are going to limit their employees' expectations that data transmitted from a WDD over a company network will remain private."

CLOUD

## Microsoft Privacy Case Has Cloud Industry on Edge

Who owns data stored in the cloud? Where are the legal boundaries? These are issues at the core of a Microsoft privacy case. Microsoft has been ordered by a U.S. federal court to turn over a customer's e-mail stored on servers in Ireland in compliance with a U.S. government-issued search warrant. Microsoft is fighting the ruling, contending that the e-mails belong to the customer. As for the search warrant, Microsoft says there is well-established case law that it cannot reach beyond U.S. shores. U.S. District Judge Loretta Preska ruled the location of the e-mail was irrelevant because Microsoft controls it from the United States.

Many see this as the latest hit to the cloud computing industry and, particularly, to U.S. cloud providers still dealing with trust issues because of the National Security Agency surveillance scandal. But that's just one piece – this case could also have far-reaching ramifications for international law. In an interview with *InformationWeek*, Morgan Reed, executive director of the Association for Competitive Technology, pointed out that if the U.S. government can force Microsoft to turn over data in an Irish data center, European governments could decide they can extract data from U.S. citizens anywhere in the world.

Elad Yoran, CEO of cloud security vendor Vaultive, told *InformationWeek* that businesses should not resist the cloud but should ensure they control their data. He stressed the importance of encrypting data before moving it to the cloud and holding on to the encryption key. Kate Westmoreland, a lawyer and fellow at Stanford Law School, concurred: "It means power is back with the user. There are limitations on being able to compel users to give up those keys."

Preska's verdict wasn't immediately applied because she unexpectedly issued a bench ruling that stayed her decision so Microsoft could appeal.

"Either way this decision unfolds in the end, the important thing is to have some business certainty," Westmoreland said.

CYBERSECURITY

## FDA Focuses on Cybersecurity, Medical Devices

October was National Cybersecurity Awareness month. To celebrate, the Food and Drug Administration (FDA), in collaboration with the National Institutes of Health and Homeland Security, was to host a public workshop and webcast to engage the healthcare and public health sectors in promoting medical device security.

One theme for discussion was identifying cybersecurity gaps and challenges, especially end-of-life support for legacy devices and interconnectivity of medical devices. The goal was to bring together the stakeholders to identify those challenges and to discuss strategies and best practices, including how to adapt and implement the FDA's guidelines for managing these risks, "Framework for Improving Critical Infrastructure Cybersecurity."

The vulnerabilities of medical devices continue to increase as more and more devices are connected to the Internet, hospital networks, and other devices. For example, connected devices could be threatened by malware or unauthorized access to configuration settings in medical devices and hospital networks. It's up to manufacturers to remain vigilant in identifying risks associated with their medical devices, and it's up to hospitals and healthcare facilities to evaluate their network security and adequately protect the hospital system, the FDA said. The agency recommends that medical device manufacturers and healthcare facilities work together to address those weaknesses and implement safeguards necessary to protect medical devices from these and other potential security risks.

PRESERVATION

## Using Technology to Preserve Space Age History

The challenge: preserve national historic landmarks that are falling into decay. One answer: laser scanning.

Funding limitations for major preservation projects have prompted the U.S. Air Force to take a high-tech approach to the challenge. The Air Force has turned to laser technology to document and preserve Cape Canaveral Air Force Station's historic launch structures that launched the United States' first manned spacecraft to orbit the earth in 1962.

The Air Force's 45th Space Wing partnered with the University of South Florida's (USF) Alliance for Integrated Spatial Technologies (AIST) to use a laser scanner "to survey, map, and create virtual-model videos of six of the highest priority historic launch complexes."

"We consider many of these structures to be endangered species, meaning that they are unique and sometimes the last of their kind, and we are looking at ways to preserve them digitally and holistically, as well as improve chances for effective stabilization and maintenance," said Lori Collins, Ph.D., the co-director of the AIST program.

"Digital documentation will, in this case, not only be used for preservation and archival recording efforts, but for visualization through online, classroom and other applications, promoting education and outreach," she explained. "Already, data from this project has been used in courses at USF on heritage preservation, museum visualizations and field method applications, and much more is planned in the way of teaching and training using heritage as a theme."

The scanning and field operations are complete and the project is now focusing on modeling, visualization, and other digital products for possible future maintenance and stabilization of the structures. The Air Force said the next phase of the project is scheduled to begin in 2015 and will include terrestrial laser scanning and 3-D spatial technologies to identify, evaluate, and document baseline conditions at the launch complexes so researchers can evaluate condition changes and deterioration.

INFO SECURITY

## Home Depot Security Breach Fallout Begins

Move over, Target; Home Depot is now in the hot spot. In September, Home Depot finally confirmed a breach of its payment security systems that affected 56 million customers in its U.S. and Canadian stores. Within a matter of days, the first class action suit was filed in the Northern District of Georgia; Home Depot is based in Atlanta. Attorneys general in three other states have launched investigations.

The lawsuits accuse Home Depot of negligence in failing to secure customers' personal and financial information. While most of the cases were filed on behalf of customers, two credit unions and a bank also have filed suit.

KrebsOnSecurity reported the breach September 2, stating it could extend back to April and affect all of Home Depot's 2,200 U.S. stores, according to Reuters. A variation of the malware that compromised Target's systems last year was used on the Home Depot systems, according to Krebs.

As of September 25, Home Depot had incurred $62 million in expenses, including legal costs, associated with the breach, reported *The National Law Journal.* But this is just the beginning. Home Depot was due to respond to the court by October 10.

On a side note, Target, which had 40 million customer records breached in December 2013, currently faces about 100 lawsuits. The company has moved to dismiss the litigation brought by financial institutions, contending it has no "special relationship" with them that requires a duty of care.

DATA PRESERVATION

## Automated Data Preservation on the Rise

Organizations are increasingly seeing the benefits of automating their litigation hold process. According to the 2014 Legal Hold and Data Preservation Benchmark Survey, 44% of organizations have automated their legal hold process, compared to 34% last year, and they have reported higher confidence in their data preservations process should they need to defend it. In fact, 70% of automated users were satisfied to very satisfied with their litigation hold processes, while only 35% of manual users said they were satisfied or very satisfied.

At this rate, software provider Zapproved, which conducted the survey, predicts that the majority of all legal data preservation will be automated by 2015. This is especially relevant given that it has become common practice in commercial litigation for opposing sides to challenge each other's preservation efforts, noted Brad Harris, vice president of legal products for Zapproved. Almost one-third (31%) of the survey respondents had to defend their preservation practices this year, up from 22% last year.

The number of litigation holds issued per month is also on the rise. The "Power Preservers" category identified by the survey – those organizations that issue six or more holds a month – jumped 30% from last year. Predictably, this group is more likely to be using an automated system given the benefits of streamlined processes and higher return on investment. Still, only 60% of power preservers are automated.

One area that continues to be of concern is employee training. While 64% of the respondents reported they train employees, fewer than half said that employees are "tuned into their obligations."

Harris concluded the report by offering steps organizations could take to improve their processes:

- Audit current preservation processes to measure their effectiveness and whether they meet the threshold of current legal standards.
- Prepare to defend preservation. The goals should include process consistency, maintaining a detailed audit trail, and identifying potential points of failure.
- Emphasize training and a culture of compliance.
- Educate yourself continuously – this is a fast-moving area of the law.

LEG/REG

## U.S. Companies Charged with Violating Safe Harbor

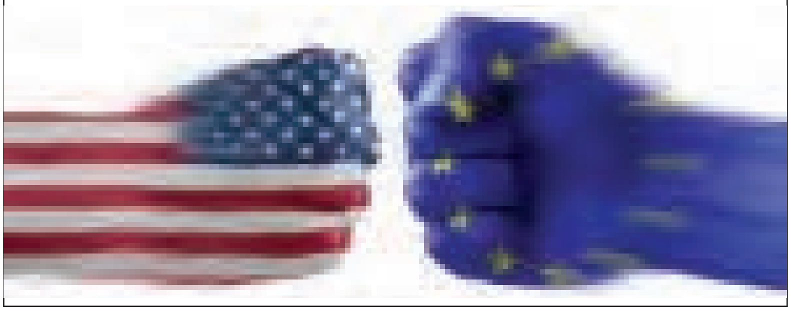
Thirty U.S. companies have been called out by the Center for Digital Democracy (CDD) for allegedly violating the Safe Harbor agreement between the EU and the United States.

CDD recently filed a complaint with the Federal Trade Commission (FTC) asking it to investigate the data brokers and data management firms for collecting, using, and sharing data about European residents in a manner inconsistent with the Safe Harbor framework.

"[The] companies are relying on exceedingly brief, vague, or obtuse descriptions of their data collection practices, even though Safe Harbor requires meaningful transparency and candor," asserted CDD Executive Director Jeff Chester.

Some of the broad concerns CDD cited included 1) failure to provide "accurate and meaningful information" to EU consumers; 2) lack of candor about how the data is collected; 3) failure to provide "meaningful" opt-out mechanisms; and 4) the "myth of 'anonymity,'" considering that companies collect enough details that a user's name is almost irrelevant for marketing.

*Forbes* contributor Emma Woollacott pointed out that the European Parliament voted some time ago to suspend the Safe Harbor but the European Commission has not done so, "preferring instead to hold the threat of suspension over the United States' head."



E-DISCOVERY

## Notable Trends in E-Discovery

The intent of the Federal Rules of Civil Procedure is to ensure a "just, speedy, and inexpensive determination of every action and proceeding." That's a pretty tall order in a time when the amount of electronically stored information (ESI) is exploding. In an effort to meet that challenge, three trends have emerged that in-house counsel cannot afford to ignore, according to Benedict Hur and Matthew Werdegar, partners in Keker & Van Nest, in a recent article.

First, the sanctions for e-discovery violations are growing. There are indications that the number of violations may have leveled off, the authors said, but the courts are also much quicker to impose monetary penalties and issue sanctions for e-discovery misconduct. For example, in 2013 a federal judge levied a $1 million sanction for e-discovery mismanagement and warned that more could follow.

Second, more courts are using their local rule-making powers to enact new e-discovery model orders and guidelines. These new rules typically "call for phased discovery of ESI, limits on e-mail discovery, limits on the obligation to preserve and collect certain categories of ESI, increased cooperation between litigants on e-discovery issues and enhanced cost-shifting provisions to discourage e-discovery overreaching," the authors explained.

"Now more than ever, courts are willing to entertain creative proposals for reigning in e-discovery, provided that they are tailored to the circumstances of the case and transparently describe what will be covered and why," they wrote.

Counsel needs to do their homework at the outset of a case if they are going to take advantage of the new rules. They need to know where the relevant data resides, how much there is, and how difficult it will be to collect it. Only then can they hope to craft a comprehensive, justifiable e-discovery plan.

The third trend is the proliferation of new tools to assist in finding, collecting, and producing the data required for e-discovery. Predictive coding is one of the hottest e-discovery tools. In short, predictive coding uses computer algorithms to identify relevant documents based on a human review of test documents. Despite the up-front effort required, many believe it has the potential of dramatically decreasing e-discovery costs.

The law governing the use of predictive coding and other emerging tools is still being written. The authors recommend that anyone considering using predictive coding read U.S. Magistrate Judge Andrew Peck's order in 2012's *Moore v. Publicis Group*.

DATA PRESERVATION

## New Technology Said to Preserve Data for 1,000 Years

Hitachi Data Systems Federal (HDS) has introduced a digital preservation platform it says will enable federal agencies to comply with the Presidential Memorandum – Managing Government Records' requirements to preserve and archive mission-critical data indefinitely.

The new platform allows long-term storage of 50 years using Blu-ray, and eventually up to 1,000 years using M-DISC media, according to the HDS announcement of the new solution. "These optical media solutions ensure compatibility as data formats continue to evolve, longevity across generations of technology, and continued retrieval and use."

The release went on to explain, "In addition to alleviating pain points caused by forced data migrations, enterprise-quality optical discs ensure that agencies can safely preserve data for decades because of their proven survivability, including resistance to water, dust, electromagnetic events, and storage environments that have high heat and humidity."

E-DISCOVERY

## UK Businesses Re-Think Data Protection Strategy

Recent high-profile data breaches such as those involving eBay, Adobe, and Kickstarter, for example, have prompted many UK organizations to re-think their data protection strategies. Trend Micro's EU Data Protection Regulation report found that 68% of UK organizations are reconsidering their strategy.

The greatest threats to their data, reported UK organizations, come from accidental loss by employees (36%) and cyber attacks (29%). Many have responded by training staff to raise their awareness about data security (72%), using encrypted passwords (60%), and implementing technology for remotely wiping lost devices (47%) and for identifying network intruders (32%).

Organizations reported increasing user demand for transparency: 37% have had more requests to know what user data is being kept and where. Surprisingly, though, only 26% have a formal process for notifying customers in case of a breach and, in fact, always notify them. Almost one-third (32%) have no formal policy for notifying customers.

The impending EU General Data Protection Regulation will require all organizations that do business in EU states to immediately notify customers in the event of a data breach and to notify the applicable regulator in as few as 24 hours.

"The majority of UK organizations don't have this capability, and this is a perfect example of how organizations will need to upscale their readiness against tough new standards," said Vinod Bange, partner at the international law firm Taylor Wessing.

Bange added that organizations also need to be able to comply with the new right-to-be-forgotten ruling handed down by the European Court of Justice (the highest court in the EU). "[The ruling] established that EU data laws apply in a context that was not previously envisaged, so organizations need to ensure that they have processes in place to address compliance with EU data laws which they may have previously considered as not applicable to them."

"Awareness is growing among companies that the new EU data legislation will have a significant impact on their businesses, but there is still some way to go," said Ferguson. "It's frightening considering how close it is and how little some organizations know." **END**

E-DISCOVERY

## Cloud Providers Unprepared for New EU Regs

Businesses aren't the only ones not ready for the impending EU General Data Protection Regulation. Cloud services providers are far from prepared.

The first thing to note is that the new regulation will affect any organization based in Europe, operating in Europe, or handling data pertaining to EU residents. Liability for data breaches and violations of the law will be shared between data controllers (organizations that own the data) and data processors (such as cloud providers that store the data) – and the penalties can be severe. Yet only one in 10 cloud service providers is prepared to meet the new requirements, according to a study by security provider Skyhigh Networks.

Some areas of specific concern are as follows:

- 23% of cloud providers maintain the right to share data with another third party, which could make complying with the right-to-be-forgotten requirements difficult.
- Only 1% offer encryption using customer-managed encryption keys.
- Only 3% enforce secure passwords.

Clearly there's a great deal of work to do before the regulations go into effect, which is likely to be in 2015.