INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

MAY/JUNE 2014

Plug Internal Data Leaks with an Effective IG Program

Page 20

Proposing a Charter of Personal Data Rights

Page 27

Leveraging the Principles in Mergers, Acquisitions, and Divestitures

Page 32

MOBILE DEVICES

Surveys: Mobile and Cloud Are Paying Off

Embracing bring your own device (BYOD) and other consumer technologies in the workplace can pay big dividends. The majority – 70%, according to one study – of companies that have deployed mobile and cloud solutions have experienced some sort of return on investment (ROI) from using consumer devices such as tablets and smart phones in the workplace. These devices are giving companies a competitive advantage and contributing to a healthier bottom line.

These conclusions were echoed in two surveys, one conducted by IDG Enterprises involving 1,155 IT decision makers and the other by *Computerworld*, featuring 313 business and IT professionals who influence buying decisions.

The *Computerworld* "2014 State of the Enterprise Survey" found that an increasing number of businesses consider mobility (59%) and collaboration (58%) technologies to be very important or critical to creating a competitive advantage for their organizations' long-term future. Therefore, it's no surprise that the vast majority of the respondents said they are in the process of adopting, have completed deploying, or have optimized their ROI from mobility (74%), collaboration technologies (73%), cloud (58%), and consumer IT (45%) initiatives.

This growing trend translates to increased spending on such devices. Almost half of the IDG respondents to the "2014 Consumerization of IT in the Enterprise" survey plan to invest in tablets and employee training to make the most of this technology; 43% will invest in smart phones. On a business level, this trend is prompting IT leaders to move beyond first-responder status to craft a long-term strategy for success.

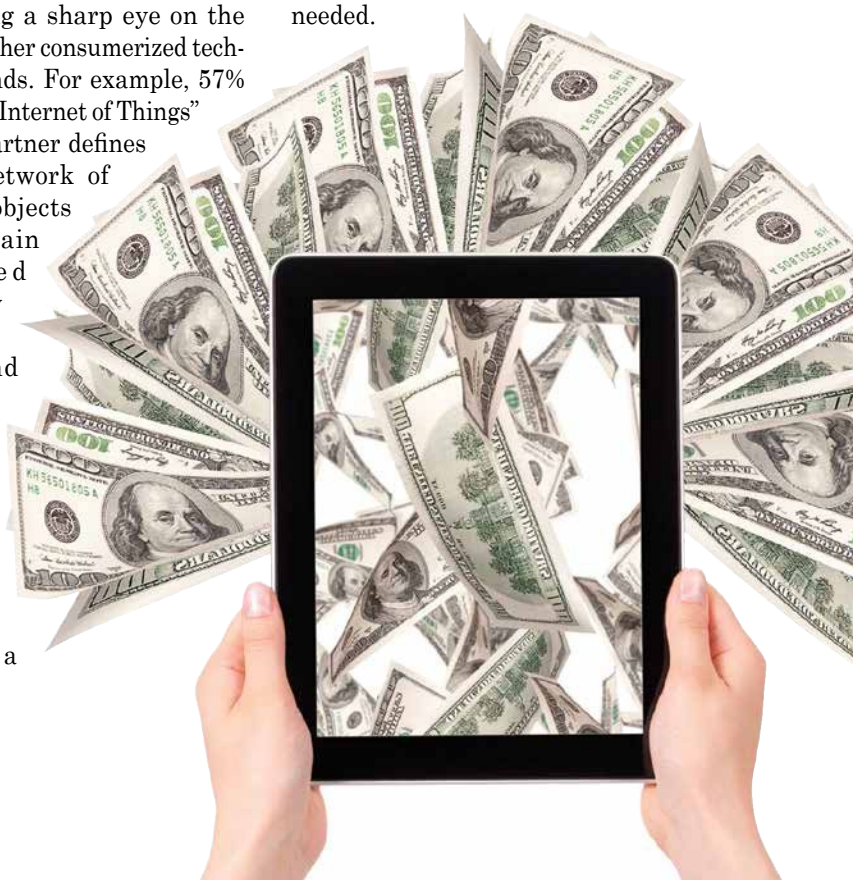
"Driven by widespread mobile device usage, the spread of consumerized technologies such as mobile devices appears poised to move from the mainstream to a transformative technology that will trigger widespread changes in how business users work," the IDG survey report stated.

Indeed, more than 80% of the IDG respondents are making at least one organizational change as the result of the increased use of consumer technology in the workplace, and more than half have implemented formal policies to regulate how corporate data is accessed and shared on consumer technologies such as mobile devices or cloud computing.

IDG respondents reported they are keeping a sharp eye on the impact of other consumerized technology trends. For example, 57% expect the "Internet of Things" – which Gartner defines as "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment" – will have a significant or moderate impact on the business landscape.

Moreover, consumer technologies are driving adoption of related technologies, creating a snowball effect at many companies. For example, more than 60% of respondents said that consumer technology use will increase the use of cloud computing services at their company, while a little more than half expect a similar impact regarding Web 2.0 technologies such as web applications, mashups, and social media, according to the IDG report.

Companies investing in these and other emerging technologies expect to reap financial, operational, and strategic benefits. Consequently, many IT departments, especially in larger companies, are struggling to balance business expectations with the challenges of integrating new technologies with legacy systems that are still needed.



INFO SECURITY

Beware Security Pros: The Wearable Revolution Is Coming

Remember the old Dick Tracy walkie-talkie watch? That was hightech.

Now we have Internet-connected spectacles (Google Glass) and computers on wrist watches (smartwatches), also known as *wearable technologies*. Some predict that 2014 may well be the year wearables will become mainstream.

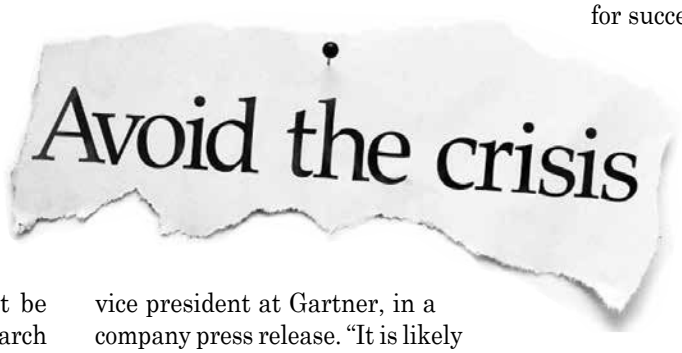
These new technologies are vulnerable to cyber attacks, warned Rashmi Knowles, chief security architect at RSA, EMC's security division, in a recent digital article on *TechRadar Pro*. He pointed out that Google Glass is expected to be commercially available by the end of the year. Although many consumers are skeptical of the technology, Knowles sees significant possibilities for businesses, especially those dealing with advanced engineering or electronic technology. The technology could enhance the capabilities of their staff, but it could also become extremely vulnerable considering there are viruses that can control the microphone and camera of a mobile device.

Knowles also noted that the inherently small screens are designed to make information decipherable at a glance. That means a lack of domain names and graphics, which will make it more difficult to detect phishing e-mails and other "deception-based cyber-attacks."

"…[A]s security professionals we need to be aware that, as wearable technologies make their way into the workplace, they represent a multiplication of potential attack surfaces. This will affect everything from BYOD policy to information infrastructure design, and we would be well advised to prepare now," Knowles said.

INFO GOVERNANCE

Gartner Warns of Information Crisis by 2017



Fortune 100 organizations beware: an information crisis might be looming. Gartner, an IT research and advisory company, predicts that one-third of the Fortune 100 will experience an information crisis because of their inability to "effectively value, govern and trust their enterprise information."

"There is an overall lack of maturity when it comes to governing information as an enterprise asset," said Andrew White, research vice president at Gartner, in a company press release. "It is likely that a number of organizations, unable to organize themselves effectively for 2020, unwilling to focus on capabilities rather than tools, and not ready to revise their information strategy, will suffer the consequences."

Business leaders need to be more proactive and manage information for business advantage rather than just maintain it, emphasized White. IT leaders must design enterprise information management (EIM) initiatives so sharing and reusing information creates business value that contributes to enterprise goals. An EIM program must help an organization identify which information is important to its success – not all information is.

Unfortunately, according to Gartner, more than 75% of an organization's individual information management initiatives are isolated from each other. Consequently, EIM is not being realized, sustained, or fully exploited.

Gartner recommends that "IT leaders identify the crucial business outcomes in need of improvement or that are being hampered by poor information management. Second, they need to determine the business processes and leaders most affected by those outcomes and use their findings to start setting priorities for a new EIM program. Finally, they need to adopt a program management approach for EIM, to identify work efforts, resource commitments, stakeholder expectations, and metrics for success."

As EIM focuses on linking projects, using assets, and aligning organizational efforts, there is also demand for information governance, said White. "With effective information governance, business users will understand the impact of poor quality data on the outcome of desired business processes. This understanding leads to a desire, on behalf of the end user, to assure or 'steward' the data so that it supports their day-to-day business activities."

CYBERSECURITY

Boards Seek Cybersecurity Risk Experience

Experience overseeing cybersecurity risk is increasingly in demand in the boardroom, according to a key finding of the 2014 "What Directors Think" survey report. In fact, the report shows information technology expertise is the fourth most-desired attribute for new corporate board members, following only financial expertise, industry expertise, and CEO experience.

The survey of nearly 600 corporate directors revealed that 20% of directors are not confident their board understands the many facets of cybersecurity risk. According to a press release about the report, "Overall, boards indicated they were confident in their ability to monitor cyber risks; however, about 40% acknowledged there was room to improve knowledge and understanding of risk oversight in general."

"Risk oversight has always been a key focus for boards but with developments in technology and the rise of social media, many are reassessing their skillset or partnering with organizations that specialize in risk management," said NYSE Euronext Head of Global Issuer Services Jean-Marc Levy in the press release.

The survey was released by NYSE Governance Services and senior executive search firm Spencer Stuart.

E-DISCOVERY

Can Contract Provisions Reduce Discovery Risks?

The pressure is on. Corporate counsels are looking for ways to reduce the impact of e-discovery and lower its price tag, which are not easy tasks given the tremendous volume of electronically stored information and plaintiffs' growing sophistication in aggressively seeking e-discovery. Add to that the court's willingness to sanction defendants for non-compliance, and it's understandable why corporate defendants are feeling pressured. After all, according to an article in *Law Technology News*, it's estimated that discovery costs now account for up to 50% of total litigation costs.

One approach that may help control costs is the use of contract provisions whereby parties negotiate the terms of e-discovery at the beginning of the relationship. Many issues could be addressed, including specifying when the duty to preserve begins, specifying the types and sources of data to be preserved and searched, determining fee and cost-shifting provisions, and limiting the availability of discovery sanctions.

How successful this approach could be is unknown due to the lack of case law. Corporate counsels should be prepared for the court to override the contract provisions. For example, the Federal Rules of Civil Procedure state that the duty to preserve begins when a party can reasonably anticipate litigation. Regardless of what date the parties agreed the duty to preserve begins, the court could determine a different date and assess sanctions, particularly if it perceives the contractual provisions to be one-sided. Courts are more likely to enforce a provision when it is the result of legitimate arm's-length bargaining between parties of equal bargaining power; thus it's possible that contracts between two corporations are better candidates for such provisions than employment contracts or those between corporations and consumers.

Clearly there are risks associated with this approach; it could increase discovery costs if the court doesn't enforce the provisions, so parties taking this route should beware.

XACT DATA DISCOVERY

Fact: The world is digital.

Fact: Paper hasn't disappeared.

Xact Data Discovery is both

IN-HOUSE FORENSICS	ELECTRONIC DISCOVERY	NO-FEE PROJECT MANAGEMENT	DATA HOSTING & MANAGED REVIEW	PAPER DISCOVERY

XDD delivers EVERYTHING you need to tackle today's complex discovery challenges.

xactdatadiscovery.com
1.877.545.XACT

XACT DATA DISCOVERY
Because you need to know

INFO GOVERNANCE

How Does Your IG Program Measure Up?

Implementing a legally defensible retention schedule is a key component of an organization's data management program. It can speed up the e-discovery process and reduce costs associated with document preservation and reproduction. U.S. companies understand this. Unfortunately, the same can't be said for most companies in other countries, according to a recent *Mondaq* article.

If your CEO asked you to assess the condition of your information governance (IG) program, how would you respond? You might begin at the core of any comprehensive IG program: your records and information management (RIM) practices. If your organization is among the 13% who recently reported they don't have a RIM program, you're already in trouble.

Most (87%) of the organizations that participated in the 2013/2014 Information Governance Benchmarking Survey conducted by Cohasset Associates, ARMA International, and AIIM International confirmed they have a RIM program. That's the good news. The fact that few organizations (12%) fully integrate RIM and the other key IG disciplines – compliance, security, IT, risk management, audit – is the not-so-good news.

Some of the other findings of note are listed here:

- At 78%, the greatest challenge RIM programs face is changing the keep-everything culture.
- 42% said their programs are mature (according to the Information Governance Maturity Model) in protecting private, confidential, and sensitive information.
- 27% gave their programs a mature rating for the handling of electronically stored information as part of the legal hold process.
- 74% reported they have a legal holds process in place, and 72% of them think it is generally efficient and effective.
- The top three IG disciplines RIM is most integrated with are privacy (39%), information security (38%), and legal holds (36%).
- Only 35% train all employees on what information to manage and how to manage it at least every two years; more than 50% basically don't provide any training.
- 45% have either incorporated (18%) or are in the process of adding (27%) RIM compliance to service provider contracts.

CYBERSECURITY

Japan Holds Cybersecurity Drill

Preparations for the 2020 Olympics in Tokyo are underway, including those aimed at strengthening national security. In March, Japan gathered more than 150 cyber defense experts to simulate an attack across 21 state ministries and agencies and 10 industry associations, reported Reuters. The exercise simulated a phishing attack, where government officials or businesses opened up their servers to a computer virus by visiting a fake website.

Britain had employed a similar tactic in preparation for the 2012 London Olympics. It warded off multiple attacks during the event.

"Cyber-attacks are becoming more subtle, sophisticated and international, and strengthening Japan's response to them has become a critical issue," the Japanese government's spokesman, Yoshihide Suga, said during the drill in Tokyo. Suga is the chief cabinet secretary and is in charge of Japan's cybersecurity.

"It's not that we haven't put effort into cybersecurity, but we are certainly behind the U.S.," said Ichita Yamamoto, the cabinet minister in charge of IT policy.

The drill marked the first time Japan's government and businesses have worked together to counter the threat of cyber attacks. The test is expected to help break down some of the current silos.

Also in March, IT minister Yamamoto convened the first meeting of cybersecurity officials from the ministries and police agency, joined by outside experts, to create a unified approach to Japan's online security. The group is expected to make its recommendations by summer.

E-DISCOVERY

India Lags in E-Discovery

Finding e-discovery services in India is extremely difficult, to say the least. According to a recent *CJNews India* blog posting, only a handful or more of law firms provide e-discovery services in India, and only one or two cyber law firms do. The deficit is due largely to a lack of the necessary techno-legal experience in the law firms and in law enforcement. India's law enforcement and revenue authorities have failed to take advantage of e-discovery and cyber forensics in their investigations, despite the fact that cyber laws were broken in several notable cases.

One high-profile example noted in the news posting was the Target Corp. breach, which exposed the personal information of up to 70 million customers. The company is facing litigation threats from around the world, including from India, for failing to comply with techno-legal requirements of applicable Indian laws.

According to the post by Priyanka Sharma, owner of the "Cyber Laws in India" portal, clearly needed are e-discovery and cyber forensics best practices that national and international companies operating in India would be required to adopt.

"In the absence of various techno legal compliance on the part of Indian and foreign companies operating in India, there is an urgent need to formulate effective and robust techno-legal e-discovery and cyber forensics regulatory regimes for India," Sharma posted.

Cyber forensics and cyber crimes investigation capabilities also need to be seriously strengthened, Sharma stressed.

E-DISCOVERY

More Companies Strive to Emulate U.S.-Style Retention Policies

Implementing a legally defensible retention schedule is a key component of an organization's data management program. It can speed up the e-discovery process and reduce costs associated with document preservation and reproduction. U.S. companies understand this. Unfortunately, the same can't be said for most companies in other countries, according to a recent *Mondaq* article.

"Except for truly global companies that have plenty of experience in U.S. litigation, many non-U.S. companies do not know how broad and burdensome the discovery process can be," said Masahiro Tanabe, an attorney who focuses on cross-border business transactions and disputes in the Tokyo office of Foley & Lardner LLP, in the article. "Similarly, many of them do not know that there is an obligation to preserve relevant documents pre-litigation. Accordingly, they are not always fully aware of the importance of a defensible document retention policy."

Tanabe said many companies typically have retention schedules that were developed in accordance with their home country standards. The more business they do with the United States, the more prepared they must be for U.S. litigation. That's why many Japanese and other non-U.S. companies are trying to implement U.S.-style, company-wide document retention policies. Unfortunately, some practices that are unique to a country become obstacles. For example, in Japanese companies, it is common for each business department to have its own information system or encryption method.

Likewise, U.S. companies need to review their retention policies concerning their operations outside the United States. Privacy is an excellent example of a facet of information retention that trips up some U.S. companies. Google and other organizations have faced sanctions in European countries that have more stringent privacy policies than the United States has.

CYBERSECURITY

NIST Presents Cybersecurity Standard

The U.S. Commerce Department's National Institute of Standards and Technology (NIST) released the first version of the "Framework for Improving Critical Infrastructure Cybersecurity" in February. It was presented exactly one year after President Obama issued an executive order directing the agency to collaborate with industry to create a voluntary framework for managing cybersecurity-related risk based on existing standards, guidelines, and practices.

According to NIST, the framework uses a common language to address and manage cybersecurity risk in a cost-effective way, based on business needs without adding regulations. It focuses on using business drivers to guide cybersecurity activities and on considering cybersecurity risks as part of the organization's risk-management processes. Furthermore, because it references globally recognized standards on cybersecurity, it "can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity."

Per the executive order, the framework also provides guidance on how organizations can incorporate the protection of individual privacy and civil liberties into a comprehensive cybersecurity program.

NIST has stressed that the framework is not a one-size-fits-all approach to managing cybersecurity risk. "Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the framework will vary."

The agency recommends that companies begin by prioritizing their business objectives and identifying the digital threats to those priorities; then determine how they would identify, protect against, detect, respond to, and recover from a cyber attack. The next steps should be to conduct a risk assessment and define their cybersecurity objectives. Once they've identified the gaps between their current and desired cybersecurity profiles, they should be ready to develop an action plan.

The framework is generally regarded as a good first step, but some don't think it goes far enough. Ann M. Beauchesne, vice president of national security and emergency preparedness for the U.S. Chamber of Commerce, stated: "[T]he Chamber believes that the framework will be fundamentally incomplete without the enactment of information-sharing legislation. Businesses need policies that foster public-private partnerships – unencumbered by legal and regulatory penalties – so that individuals can experiment freely and quickly to counter evolving threats to U.S. companies."

Greg Nojeim, director of the Center for Democracy and Technology's Project on Freedom, Security and Technology, said, "The framework will be useful to companies and their privacy officers, because it will remind them that processes should be put in place to deal with the privacy issues that arise in the cybersecurity context. However, we are concerned that the privacy provisions in the framework were watered down from the original draft. We would have preferred a framework that requires more measurable privacy protections as opposed to the privacy processes that were recommended."

NIST noted that the framework "is a living document and will continue to be updated and improved as industry provides feedback on implementation. As the framework is put into practice, lessons learned will be integrated into future versions."

In conjunction with the release of the framework, the U.S. Department of Homeland Security launched the Critical Infrastructure Cyber Community C^3 (pronounced "C cubed") Voluntary Program to encourage use of the framework and serve as the coordination point within the federal government for critical infrastructure owners and operators interested in improving their cyber-risk management processes. Initially the program is focused on working with sector-specific agencies and organizations to develop guidance on how to implement the framework.

Compliance monitoring is just a click away

Data protection regulations require organizations to monitor the qualifications and compliance of service providers that process sensitive information.

NAID just made this a lot easier!

Select the "**NAID AAA Notification**" link in NAID's member directory to receive emails announcing status changes to that member's certification and compliance qualifications.

Data Destruction Co.

John Smith
123 S. 1st Ave.
Smalltown, AZ 85011
234-567-8901
www.123destruction.com

NAID CERTIFIED: Mobile and Plant-Based Operations Endorsed for Paper/Printed Media, Computer Hard Drive and Non-Paper Media Destruction

Original Date: January 16, 2008
Expiration Date: August 31, 2014

NAID AAA Notification

Visit **bit.ly/AAAnotification** to sign up. This simple act will go a long way in establishing your organization's compliance.

PRIVACY

What's Posted to the Internet Stays on the Internet – or Does It?

The European Parliament passed new online privacy rules in March that could shorten the Internet's memory, so to speak. One of the measures, the so-called "right-to-be-forgotten" rule, would allow consumers to request that companies delete selective data from their systems. If they have no legitimate grounds for keeping the data, the companies would have to comply.

While this is an idea that seems to be growing in popularity (as evidenced by the growing popularity of apps like Snapchat, whose messages automatically disappear within a few seconds), particularly in Europe, it has some in the technology world concerned. They fear, Felix Gillette wrote in a recent *Bloomberg Businessweek* article, that it would turn providers such as Google and Facebook into "global censors" as they are bombarded with requests to edit, alter, or delete consumers' information.

The impact of the new measures, if approved by the 28 member states, would be felt by companies outside of Europe as well. The measures are not expected to progress until after the May elections.

CLOUD

Cisco to Build Global 'Intercloud'

Network giant Cisco announced in March that it will spend $1 billion over the next two years to create the world's largest global, open, hybrid cloud, a network of clouds it is calling an "intercloud."

"…[W]e saw an opportunity, by building an Intercloud with more national cloud nodes than any rival, to address rising data sovereignty concerns," Robert Lloyd, Ciscos's president of development and sales, wrote on the Cicsco blog "The Platform."

"Our cloud will be the world's first truly open, hybrid cloud," said Lloyd. "[It] will be built upon industry-leading Cisco cloud technologies and leverage OpenStack for its open standards-based global infrastructure. We plan to support any workload, on any hypervisor and interoperate with any cloud."

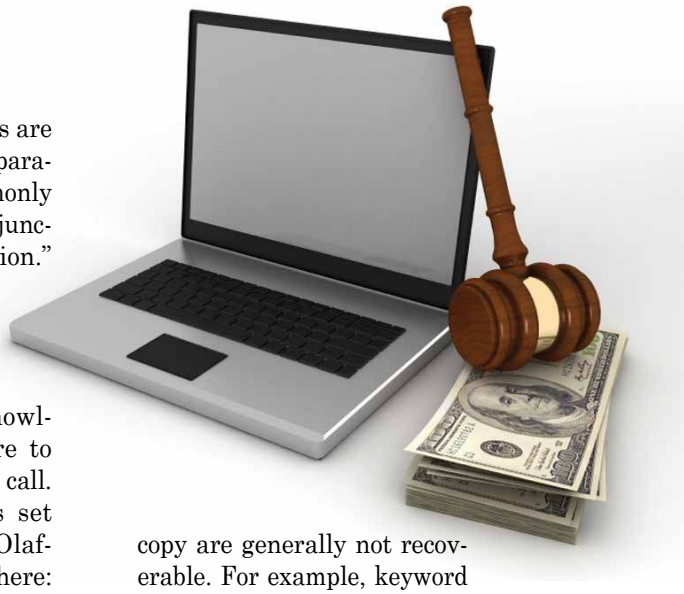
Lloyd said the intercloud is being built for the Internet of Everything – which Cisco defines as "bringing together people, process, data, and things to make networked connections more relevant and valuable than ever before – turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for businesses, individuals, and countries." It will be, according to Lloyd, "capable of scaling to billions of connections, and trillions of events, all supported by real-time analytics to help customers get the insights they need from the connections of people, processes, data and things, as they happen."

The goal is a "Star Alliance" of technology companies, Cisco Senior Vice President for Cloud Sales Nick Earle told *The New York Times*. Star Alliance is a global network of 28 major airlines, the article explained.

At the time of the announcement, Telstra, a telecommunications and information services company in Australia, had signed on as Cisco's first partner. Cisco will deploy and run a cloud infrastructure on Telstra's behalf, and Telstra will provide both Cisco-specific and Telstra-specific solutions to customers. Several other companies have also announced their support for the Intercloud.

E-DISCOVERY

Court Clarifies Standard for Recovery of E-Discovery Costs



The costs of producing documents for litigation have become a significant burden for the parties involved. In fact, e-discovery costs often reach into the hundreds of thousands of dollars. A recent decision by the U.S. Court of Appeals for the Federal Circuit (*CBT Flint Partners, LLC v. Return Path Inc.*) provides a guideline for determining the recoverability of those costs.

28 U.S.C. § 1920 states that among the recoverable expenses are "the costs of making copies of any materials where the copies are necessarily obtained for use in the case," according to Shane Olafson, a partner at Lewis Roca Rothberger LLP, in a recent *The National Law Review* article. "District courts have been all over the map when deciding what constitutes 'making copies' for purposes of recovering taxable costs associated with e-discovery," Olafson wrote.

The federal circuit court reviewed the history of Federal Rules section 1920, The Sedona Conference® principles, and other federal court decisions in concluding that section 1920 applies only to documents produced in accordance with Rule 26 or other discovery rules and does not apply to documents a party creates for its own litigation or other use.

Stated the federal circuit: "[R]ecoverable costs under section 1920(4) are those costs necessary to duplicate an electronic document in as faithful and complete a manner as required by rule, by court order, by agreement of the parties, or otherwise. . . . But only the costs of creating the produced duplicates are included, not a number of preparatory or ancillary costs commonly incurred leading up to, in conjunction with, or after duplication."

In its final opinion, the federal circuit focused on whether various tasks were necessary to fulfill a party's discovery obligation, acknowledging that deciding where to draw the line is a judgment call.

Some of the guidelines set forth in the opinion that Olafson summarized are listed here:

- If a party must convert electronic documents to a uniform production format (e.g., TIFF or with metadata included), those steps are considered "making copies" for purposes of recovery. If such processing steps are unnecessary, they are not recoverable. For example, if metadata can be preserved without first using imaging and extraction techniques, those additional steps are not recoverable.
- If a vendor works on a large volume of documents before culling to produce only a subset, awarded costs must be confined to the subset actually produced.
- Costs incurred in *preparing* to copy are generally not recoverable. For example, keyword searching, reviewing documents for responsiveness and privilege, and training to use review software are not recoverable. Rather, they are part of "the large body of discovery obligations, mostly related to the document-review process, that Congress has not included in section 1920(4)."
- Deduplication and decryption costs are not recoverable.
- The creation of "load files" is covered to the extent those files contain information required by the requested production.
- The costs of slip sheets are recoverable.
- The costs of copying responsive documents to production media are recoverable.

PRIVACY

Privacy Groups Try to Stop Facebook's Purchase of WhatsApp

Facebook's recent announcement that it was purchasing the instant messaging app WhatsApp met with mixed responses. Privacy advocates promptly petitioned the Federal Trade Commission (FTC) to stop the $19 billion sale until it was clear how Facebook would use the personal data of WhatsApp's 450 million users. The app has long been committed to not collecting personal data for advertising purposes. The question is: Will Facebook (which does collect personal data for advertising purposes) honor that commitment?

Facebook responded that "WhatsApp will operate as a separate company and will honor its commitments to privacy and security."

Despite such assurances, Reuters reported, the privacy groups behind the FTC filing noted that Facebook has in the past amended an acquired company's privacy policies, such as the Instagram photo-sharing service that Facebook acquired in 2012. The groups asked regulators to require Facebook to "insulate" WhatsApp user information from access by Facebook's data collection practices.

CLOUD

What NOT to Do When Adopting the Cloud

Before deciding to make the leap to the cloud, you may want to read Mike Kavis's new book, *Architecting the Cloud: Design Decisions for Cloud Computing Service Models*, which explores the key steps IT and business leaders need to first consider.

Joe Kendrick previewed the book in a recent *Forbes.com* article, summarizing the nine "worst practices" Kavis has observed that have derailed cloud deployment.

- *Worst Practice #1: Migrating applications to the cloud solely to drive down costs.* Kavis says companies that want the cloud to reduce the costs of managing current applications should consider moving their applications to a managed hosting provider.
- *Worst Practice #2: Having inflated expectations of suddenly becoming a digital enterprise.* Kavis advises that companies should use the cloud for smaller deliverables that can provide business value sooner and in smaller increments.
- *Worst Practice #3: Not fully understanding cloud security.* The lack of standards and enterprise experience with the cloud make it vulnerable to abuse. Cloud security understanding needs to be a top priority for architects, product teams, and other IT professional, says Kavis.
- *Worst Practice #4: Selecting a favorite vendor, not an appropriate one.* Kavis advises to select a vendor who is experienced in cloud and understands the different business circumstances it may present. He also advises IT professionals to learn about the three cloud service models.
- *Worst Practice #5: Failing to plan for outages.* He says organizations must understand the providers' service level agreements and data ownership policies and must thoroughly examine all legal binding documents and agreements.
- *Worst Practice #6: Not understanding the impacts of organizational change.* Starting with smaller, less risky initiatives can help minimize or diffuse resistance to change, Kavis believes. He also recommends bringing a change leader into the process.
- *Worst Practice #7: Not bringing in enough of the right skills.* Operating in the cloud often requires new or different skills. Kavis suggests organizations help employees get the experience they need to manage in the cloud.
- *Worst Practice #8: Misunderstanding customer requirements.* Kavis advises creating a list of frequently asked questions to help customers navigate the cloud.
- *Worst Practice #9: Not preparing for unexpected costs.* Kavis notes that "the most expensive part of cloud computing usually has nothing to do with the cloud at all. Often companies underestimate the effort it takes to build software in the cloud."

INFO TECHNOLOGY

Predictive Coding: Not Just for E-Discovery

Relying on employees to appropriately label and manage records is a flawed approach, according to experts who spoke at the recent LegalTech New York. *Law Technology News* reported that one of the experts, Warwick Sharp, vice president of marketing and business development at Equivio, equated this approach to a game of telephone in which the retention officer "is responsible for sending a company's record policy all the way down the chain to a company's last user employee (who is ostensibly responsible for labeling files in his own email with up to 300 categories)."

The impracticality of this approach is obvious, especially when a company has thousands of employees and hundreds of policies, Sharp said. In his opinion, predictive coding could be a much better solution considering that a records retention expert can train software to label documents with categories. The goal: an automated process that is consistent, and defensible.

Panelist Laura Kibbe, managing director of expert and professional services at Epiq, related a case study that demonstrated the usefulness of predictive coding to one of Epiq's clients. Kibbe said they were able to clean up the company's e-mail repository by categorizing 40% of 1.4 million stored documents as simply junk e-mails, with 80% accuracy – a rate that has been accepted as legally defensible in court, according to the panelists. This approach yielded substantial savings in storage and e-discovery costs for that material alone, persuading the company to further analyze and categorize the not-junk category.

The experts were quick to remind their audience that the goal of predictive coding isn't perfection, but that perfection wasn't possible in the days of paper either. It is, however, a more defensible process than relying on 20,000 employees to follow a detailed schedule.

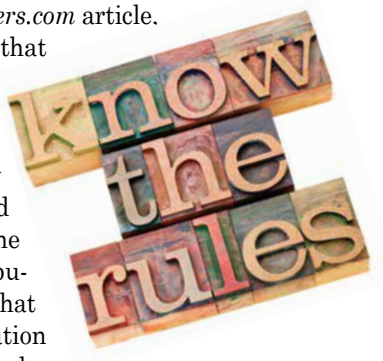
E-DISCOVERY

FRCP Comments Under Review

The proposed changes to the Federal Rules of Civil Procedure would require a party seeking discovery to establish that the requests are justified by the value and "importance" of the case; and they would limit the number of depositions, interrogatories, and requests for admissions.

A brief review of the comments received via hearings and written submissions didn't uncover any surprises. According to Alison Frankel in a *Reuters.com* posting, the comments revealed that defense lawyers and business groups praise the Judicial Conference (which presented the amendments) for attempting to reduce the burdens of discovery in civil litigation in the federal courts, while plaintiffs' lawyers expressed serious concern that proposed limits on depositions, interrogatories, and other discovery tools will exacerbate the challenge of acquiring legitimate information from defendants who don't want to surrender it.

In a Jan. 13 letter to the Committee on Rules of Practice and Procedures, U.S. District Judge Shira Scheindlin of the Southern District of New York questioned the need for and impact of some of the proposed changes. She wrote that a change to Proposed Rule 26(b)(1) adds a proportionality assessment that "invites producing parties to withhold information based on a unilateral determination…. This could become a common practice, requiring requesting parties to routinely move to compel the production of the withheld materials. This, in turn, will increase costs and engender delay."



In the *Reuters.com* article, Frankel wrote that Scheindlin, who is a noted authority on e-discovery sanctions and the author of the influential Zubulake decisions that are the foundation for the current rules, has expressed opposition to the proposed new rule for e-discovery sanctions, particularly the rule's "willful or in bad faith" language. Frankel reported that Scheindlin "is of the view that requiring a showing of bad faith to impose sanctions will encourage parties to handle their e-discovery preservation sloppily."

INFO TECHNOLOGY

New Study: Are State and Local Agencies Ready to Deploy the 'Big Five' IT Initiatives?

Manufacturing and distribution executives have become more aware of the risks associated with business information and data, especially as social media becomes more widespread. Yet more than two-thirds believe their data is at little or no risk, according to a research report from the consulting firm McGladrey. Given that their controls are often insufficient or ineffective, this raises the question of whether the executives fully understand their exposure.

U.S. government agencies are looking to the "Big Five of IT" to help them respond to increasing responsibilities and decreasing funding, according to the new study "Big Five in Overdrive: Are State and Local Networks Ready?" by MeriTalk. In fact, most of the agencies said they plan to deploy over the next three years the "big five" IT initiatives:

1. Data center consolidation
2. Mobility
3. Security
4. Big data
5. Cloud computing

However, 94% also said their agency's IT network is not fully prepared for the resulting demands.

Government IT professionals generally buy into the promise of these initiatives to improve performance, productivity, and service, yet two-thirds (63%) admitted they would face moderate to significant network bottleneck risks, and 89% said they would need additional network capacity just to maintain current service levels.

These aren't the only likely ramifications of the infrastructure imbalance created by unsynchronized adoption of these technologies, according to the report. Additionally, the IT professionals said their agencies will face security risks (59%), bandwidth limitations (55%), storage limitations (44%), and network latency (40%).

Surprisingly, the respondents aren't asking for new budget or policy changes to overcome these challenges. They want better coordination, which they believe would result in increased efficiencies (72%), shared best practices (59%), and better decision making (58%). Only two of five agencies reported they are currently coordinating efforts across these initiatives.

As always, executive support is critical. More than half (52%) believe their organization's senior leaders do not understand the combined impact of these five initiatives on IT. When asked what they most need from their senior leaders, 54% of respondents said clear prioritization from leadership, 47% asked for regular coordination across all initiatives, and 44% cited the need for standardized documentation of infrastructure requirements.

"If agencies don't align their plans to the major IT trends driving our industry, both cost and risk will increase," said Anthony Robbins, vice president public sector for Brocade, which underwrote the study. "The Big Five will fundamentally reshape how state and local governments can deliver services to citizens – better services at a lower total cost. Agencies can't afford to wait, but without coordination and planning, network capacity will choke off any chance at delivering benefits."

The good news is that some agencies are laying the groundwork now. Almost half (45%) reported they have already taken steps to improve security measures. Many have also taken steps to improve network policies, reduce network latency, improve scalability, and add bandwidth.

CLOUD

U.S. Agencies Embrace the Cloud

Four years ago the U.S. government took a major step toward modernizing its IT system by issuing a cloud-first mandate and identifying funds to support the effort. Agencies were directed to adopt cloud computing in some capacity and were advised on how to select services appropriate for migration to the cloud, such as e-mail systems. Some agencies have moved beyond the cloud-first mandate and are looking at using the cloud strategically to support their missions.

Executives from the Interior and Treasury Departments recently described some of the more strategic cloud initiatives they've deployed; their comments came during a forum sponsored by the University of Maryland's Center for Digital Innovation, Technology and Strategy. Those initiatives include cloud platforms that support the geospatial community, develop-and-test-as-a-service, and extranet services, reported *InformationWeek*.

Regardless of how they embrace the cloud, many agencies are not adequately considering the electronic recordkeeping requirements, which could lead to legal problems, warn former and current officials at the National Archives and Records Administration (NARA).

"It doesn't surprise me that the issue of recordkeeping doesn't come up much in discussions about going to the cloud," Jason R. Baron, a lawyer at the Washington law firm Drinker Biddle and former director of litigation at NARA, recently told *InformationWeek*. "When people think about the cloud, the first issues that come to mind are security and privacy. Of course, those are extremely important, but from an information governance perspective, one needs a more holistic picture."

NARA launched the Capstone Project to help agencies better manage their e-mail by automation so the agencies can meet some of the key deadlines. For example, agencies must be managing their permanent and temporary e-mail records in an electronic format by the end of 2016 and all permanent records by December 31, 2019.

These deadlines will be especially difficult for those agencies that aren't spending enough time on electronic records management requirements at the beginning of the migration process. Explained Baron: "Otherwise you're building what amounts to a slow-motion train wreck, where you've got this cloud and you've got a million e-mails somewhere in there and that's all very good. But at the end of the day, when the agency wants [to forward e-mail records] to NARA, it may not have deleted any email or differentiated between what's permanent and what's temporary."

Agencies can look to NARA as a best-practices model for integrating electronic records requirements into a cloud-based e-mail migration. Last year NARA successfully moved more than 3,000 of its e-mail users to the cloud. The migration took only six months, but officials had spent several years carefully planning it. **END**