LEGAL

## U.S. Supreme Court Moves Toward Electronic Filing

No one would ever call the U.S. Supreme Court an early adopter of technology. While the rest of the legal community has had to embrace new information technologies, the court has remained a paper-based system, but it is preparing to take some baby steps into the digital age.

On December 31, Chief Justice John Roberts released his "2014 Year-End Report on the Federal Judiciary" in which he announced that the court is developing its own electronic case filing and case management system, which may be operational as early as 2016.

The court's slowness to deploy new technology directly reflects its nature. Roberts described the court's role as "passive and circumscribed," making it only logical that it "focus on those innovations that, first and foremost, advance their primary goal of fairly and efficiently adjudicating cases through the application of law."

According to the report, "The federal courts, including the Supreme Court, must often introduce new technologies at a more measured pace than other institutions, especially those in private industry. They will sometimes seem more guarded in adopting cutting-edge innovations, and for good reason, considering some of the concerns that the judiciary must consider in deploying new technologies." Those concerns include security of information.

"The judiciary has a special duty to ensure, as a fundamental matter of equal access to justice, that its case filing process is readily accessible to the entire population, from the most tech-savvy to the most tech-intimidated," the report asserts.

Once the system is implemented, all filings at the court will be available free to the public and legal community on the Court's website. They also will be available on paper. The court expects that electronic filing eventually will be the official means for parties represented by counsel, but paper copies will also be required, particularly for those parties without counsel.

E-DISCOVERY

## Internet of Things Brings Discovery Challenges

About this time last year, Wintergreen Research estimated there were 9 billion devices (consumer and enterprise) connected to the Internet. Depending on the source, that number will be anywhere between 26 billion and 100 billion by 2020. Either way, it is clear that the Internet of Things (IoT) is growing at a tremendous pace, making it an exciting new frontier for technology vendors but a source of considerable concern for many in the legal community.

As the IoT explodes, so will the amount of data subject to potential federal oversight, e-discovery, and data breaches, pointed out Erik Post, CEO of the litigation support company OmniVere, in a recent *Law Technology News* article. The situation is further complicated by the likelihood that "most IoT devices won't have adequate data storage capacity, making e-discovery of the devices especially time sensitive," according to Post.

"The universe of potentially relevant information will increase geometrically, complicating an already messy collection and review process," predicted Post. "As plaintiffs' attorneys (and government agencies) become educated on the discovery potential for the IoT, organizations will need to proactively plan for a more demanding, invasive EDD [electronic data discovery] environment."

CYBERSECURITY

## DHS Cybersecurity Role Continues to Grow

In December President Obama signed a bill that, among other things, continues to establish the role and authority of the U.S. Department of Homeland Security (DHS) in the nation's efforts to protect its information systems.

The bill – Federal Information Security Modernization Act of 2014 (FISMA 2014) – updates and modernizes FISMA 2002. The purpose of FISMA 2002 was to provide a framework for developing and maintaining minimum security controls to protect federal information systems. It tasked the director of the Office of Management and Budget (OMB) with overseeing the development and implementation of agency information security policies and practices. FISMA 2014 authorizes the DHS to actively assist the OMB in that task.

According to *The National Law Review*, the DHS secretary will be responsible for coordinating information security efforts government-wide, providing operational and technical assistance to agencies, and consulting with the National Institute of Standards and Technology on related standards and guidelines. Furthermore, DHS will oversee agencies' implementation of "binding directives" developed by the OMB.

FISMA 2014 also modifies the scope of "reportable information" to include specific information about threats, security incidents, and compliance with security requirements. In addition, it directs the OMB to clarify what constitutes a "major incident" in the context of agency reporting requirements.

The new law also updates the cyber-breach notification requirements. The OMB director must ensure that agency policies and guidelines are periodically updated and that agencies notify Congress within 30 days of discovering a breach. That notification must include details such as the number of individuals affected, the likely risk of harm to those individuals, and the date by which the individuals would be notified.

BIG DATA

## Will Big Data Tools Make Proportionality Irrelevant?

It may be hard to believe at first, but there's a real possibility that big data tools could make proportionality a non-issue – or at least less of an issue – in legal matters.

Proportionality has been a factor because the costs of searching for immense amounts of electronically stored information can be crippling. The courts instituted a formula to ensure production expenses didn't exceed a reasonable percentage of the settlement being sought.

The emergence of big data platforms, however, has "so drastically reduced the burden side of the proportionality analysis that it may no longer be credible to limit or preclude discovery in many cases," suggested James Shook, director of e-discovery and compliance legal practice at EMC Corp. in Atlanta, in an article he penned for *Law Technology News*.

"The same proportionality rule that protected us from technology may now be in danger of elimination by technology," he wrote.

Shook was referencing technologies such as the open source platform Hadoop, which allows organizations to store a large number of files and very large files. The software includes Map Reduce capabilities that enable it to quickly analyze huge volumes of data and create a search index. "The computer and network bandwidth requirements that create burdensome proportionality outcomes on normal data sets do not apply to Hadoop platforms," Shook explained.

Some may see these capabilities as a liability, while others will realize they now are able to more efficiently analyze large volumes of data that might be relevant to a matter. Either way, the tools are here today.

At the very least, counsel needs to be aware of when these capabilities are available before suggesting that accessing the data will be burdensome. The courts have made it clear that ignorance is not a defense when it comes to e-discovery-related technologies.

PRIVACY

## Verizon Yields to Pressure

Verizon Wireless has succumbed to pressure regarding its use of a Unique Identifiable Header (UIDH) for tracking customers' web traffic. Although customers could opt out of having their information sold to third-party marketers, Verizon did not offer an opt out of the UIDH until the end of January.

The wireless company started inserting UIDH into the web traffic of its retail customers (not corporate or government contacts) in 2012, reported the *Washington Post*. It was quickly dubbed the "supercookie" as privacy groups and others protested its use, stating the concern that other companies (and even governments) could use the supercookie to track an individual's online activities.

In November, AT&T abandoned its plans to implement a similar program. But Verizon brushed off the critics until a privacy researcher revealed that a third-party advertising tracker company was using the UIDH to bring back its own cookies, even if consumers had tried to remove them. According to the *Washington Post*, the tracking company has since stated it was discontinuing the practice. Verizon announced it would allow customers to opt out of having supercookies inserted into their web traffic.

The privacy watchdog group Electronic Frontier Foundation has meanwhile petitioned the Federal Communications Commission and Federal Trade Commission to investigate Verizon for "unfair and deceptive" practices related to the UIDH. A few Congressional members are also looking into it.

Verizon's decision to allow customers to opt out is not enough for some critics. The Center for Digital Democracy reportedly has stated opting out should be the default – that users should have to choose to opt in.

GOVERNMENT RECORDS

## New Coalition to Help NARA Meet E-Records Management Order

ARMA International has pulled together a group of related organizations to support the federal government's efforts to modernize its records management infrastructure and implement proven information governance practices. The group will provide training and resources to help the federal agencies' practitioners meet President Obama's 2011 Managing Government Records Memorandum and the implementation directives issued by the National Archives and Records Administration (NARA) and the Office of Management and Budget. It will also provide a forum for the practitioners to learn more about the private sector best practices from industry leaders.

In addition to ARMA International, the coalition includes the American Health Information Management Association; AIIM; the Information Governance Initiative; the National Association for Information Destruction; and PRISM International.

"Since the issuance of the Managing Government Records Directive in August of 2012, we have consistently reached out to the private sector for input and support. With the recent enactment of the Presidential and Federal Records Act Amendments of 2014 calling on all agencies to transfer permanent electronic records to NARA in electronic form to the greatest extent possible, we will need continued assistance from non-governmental organizations like those in this coalition," Paul Wester, NARA's chief records officer, told *Government Executive*.

CYBERSECURITY

## China's New Cybersecurity Rules Rile Western Tech Companies

Regulations adopted by China at the end of last year have many Western businesses – particularly technology companies that sell in China – seriously concerned. One of the new rules states that companies that sell computer equipment to Chinese banks will be required to turn over their source code, submit to invasive audits, and build back doors into hardware and software, according to the *New York Times*.

Many foreign companies are concerned that this is a concerted effort by China to shut them out of one of the world's largest and fastest-growing markets. Indeed, as a related article by Reuters pointed out, China has long considered its reliance on foreign technology a national weakness.

The U.S. Chamber of Commerce in China and 17 other U.S. business lobbies have written to China's top cybersecurity policy group asking to postpone the implementation of the policies, stating the new rules would require "intrusive" security testing and the disclosure of sensitive intellectual property.

The new rules are the first in a series of policies Beijing says will strengthen cybersecurity in critical Chinese industries, the article stated.

MOBILE DEVICES

## The Life-Changing Side of Mobile Communications

Most of us take the conveniences of mobile computing for granted, oblivious to how it has changed lives in developing countries.

"Twenty years ago connectivity was a rarity. Today Internet access is so central to how people interact with one another, create and share information, and conduct business that the United Nations has called broadband connectivity a basic human right on par with food, shelter, and education," noted Juniper Networks in its recent Global Bandwidth Index. The report was based on findings from a survey of how people in developed and developing countries use the mobile Internet in their daily lives and what they hope to achieve using their devices in the future.

Although researchers found commonalities, the differences they observed were most revealing. First and foremost, they found that consumers in emerging markets see mobile connectivity as a catalyst for progress and change, while those in developed countries tend to regard it as a tool for accomplishing daily tasks more easily.

According to the study, 97% of people in emerging markets believe that connectivity has transformed their lives by changing "how they complete a wide range of essential and everyday tasks."

Not surprising, almost twice as many users in developed countries use their mobile devices for business purposes than those in emerging markets (53% vs. 26%). Yet, 40% of respondents in emerging markets said that connectivity has improved their earning power, compared to only 17% in developed markets.

Education is another area where there is a dramatic difference. Nearly twice as many people in developing countries reported regularly using their mobile devices for educational purposes than in developed countries. Overall, 39% of people in the developing countries said they have experienced a significant transformation in their access to education.

Network speed, network capacity, mobile device quality, and the ability to find a connection were almost twice as likely to be cited as issues by respondents in developing countries. More specifically, 60% considered connection speed the greatest problem, and 30% said finding a connection remained an issue.

PRIVACY

## Google and UK Call a Truce on Privacy Policy

The U.K.'s Information Commissioner's Office (ICO) and Google have signed an agreement that may finally begin to lay to rest the long battle over Google's privacy policy. By signing the agreement, Google has agreed to make numerous changes to its policy by June 30. In return, the ICO agreed to close its investigation.

The battle over Google's privacy policy gained momentum in 2012 when the Internet giant combined the 70 policies it had used for its individual products – such as You Tube and Gmail – into one. Privacy watchdogs contended the change led to confusion among users and ultimately eroded their privacy. The new agreement does not require Google to unbundle its privacy policies for different services, reported *ZDNet*. The company has implemented a "multi-layered approach" to its privacy policy, which it will continue to enhance.

Other changes that Google agreed to include:

- Making the privacy policy easier to find
- Disclosing in the policy its data processing activities, including the types and purposes for which it processes users' information and guidance on how users can exercise their rights
- Clarifying the entities that may collect anonymous identifiers through Google products and for what purposes

These changes should bring Google's privacy policy into compliance with not only U.K. laws but those of the European Union, thereby potentially settling similar investigations in Italy, Spain, France, the Netherlands, and Germany.

CLOUD COMPUTING

## IBM Sets Its Eyes on the Cloud

IBM is in the midst of a massive structural reorganization to make it a serious player in the cloud. It has shifted its focus onto software, letting hardware take the back seat.

In December IBM announced it was partnering with Apple to launch 10 IBM Mobile First for iOS apps. The apps range in capabilities to benefit governments as well as businesses in the banking, retail, insurance, financial services, telecom, and airline industries.

In mid-January, it unveiled the z13 mainframe, which it calls the most powerful and secure system ever built. The new system's scalability and reliability make it "the ideal private or hybrid cloud architecture," IBM stated. In fact, it can run up to 8,000 virtual servers. IBM further estimated that a cloud system on the z13 could lower the total cost of ownership between 32% and 60% over three years.

The z13 is being heralded as the first system that can process 2.5 billion transactions a day, the "equivalent of 100 Cyber Mondays every day of the year." It's also the first system to make practical real-time encryption of all mobile transactions at any scale. Plus, it's the first mainframe system with embedded analytics.

At the same time it announced the new mainframe, IBM previewed its new z/OS software, which is supposed to help further extend mainframe enterprise applications to mobile users.

Restructuring clearly hasn't slowed down innovation at IBM. In 2014 it received 7,500 patents, more than any other company. Online publisher Seeking Alpha noted that 2014 was the 22nd consecutive year that IBM topped the patent list.

Despite these advancements, IBM does not appear to be growing sales in these new markets fast enough to offset the decline in traditional enterprise hardware and services, which still account for the bulk of its business, noted the *International Business Times*. This was borne out by the company's fourth quarter earnings report. Analysts such as Credit Suisse's Kulbinder Gulcha expect IBM stock will continue to underperform as it weathers a painful multi-year transition, reported *Investors.com*.

In the meantime, IBM continues to forge ahead in its plans to become a key player in the cloud. It has opened SoftLayer data centers in Paris, Mexico City, Tokyo, and Frankfurt.

PRIVACY

## Proposed Customer Data Retention Sounds Alarm in Australia

Industry and privacy advocates are up in arms over legislation before the Australian Parliament that they say threatens all Australians' privacy.

The proposed legislation would require Australian telecommunications companies to retain a set of customer data – including, but not limited to, e-mail records, IP addresses, call records, and address information – for two years, reported *ZDNet*. Australian law enforcement agencies have voiced support for the bill and for the need to access that data without a warrant in criminal investigations.

AIMIA, the Digital Industry Association of Australia, whose members include Google, eBay, Twitter, Microsoft, and Facebook, has raised concerns that the legislation not only increases the risk of interference with fundamental rights, but also carries with it heightened security risks.

"The increased security risk of unnecessarily requiring businesses to retain data for two years should also not be underestimated, especially in light of the recent Sony hack. Businesses of all sizes that do not have a strong internal security engineering department will be particularly vulnerable to external threats when storing large volumes of data for long periods of time," the group said, according to the *ZDNet* article.

The Victorian Commissioner for Privacy and Data Protection has also spoken out against the proposed legislation, stating that "[B]y requiring retention of such sweeping categories of data, and by allowing potentially numerous agencies to have access, the scheme significantly interferes with the fundamental right to privacy in a manner that is not proportionate to the objectives of the Bill."

The Australian Human Rights Commission also stated that the legislation reaches "beyond what can be reasonably justified." It went on to suggest that the data set be defined in legislation and that a one-year retention period be tried first.

PRIVACY

## Privacy, Data Security on M&A Radar Screens

Dykema's 10th annual M&A survey revealed that privacy and data security are showing up on the radar screen for a third of mergers and acquisitions (M&A) professionals.

It shouldn't be surprising given the increased attention from regulators and customers affected by data breaches in recent years. *Inside Counsel's* Ed Silverstein predicts there will be an even higher volume of M&A transactions this year than there were in 2014.

In a recent issue of *Inside Counsel*, Stephen Tupper, leader of Dykema's privacy, data security, and e-commerce practice, highlighted some issues that could become major problems if not addressed early and well. If the deal includes the transfer of personally identifiable information (PII), it matters what the parties have promised customers. If the acquisition target has promised its customers it will not transfer their PII to a third party, the Federal Trade Commission would likely hold up the deal.

Transferring PII across national borders becomes even more problematic. Foreign regulators, particularly those in the European Economic Area, strictly prohibit the movement of their citizens' PII across borders to countries where local law does not provide comparable data protection. This doesn't have to be a deal breaker, but it does require research and advance planning.

"Consumers and others are beginning to care more about who has their data," Tupper added. He pointed to Google's recent acquisition of Nest Labs as an example. The deal prompted discussion in public forums about what combinations of data mean for privacy.

The best strategy for now, advised Tupper, "is to make room in the due diligence process and deal planning to identify any PII involved in any transaction and be prepared to take into account the evolving regulatory environment and likely consumer reaction."

INFO GOVERNANCE

## CIGO May Be Next Step in Information Governance

Big data is one thing, but what about the quality of that data? Information governance (IG) professionals voiced concern about such matters at the 2015 LegalTech held in early February in New York, according to a report in *Law Technology News*. In an attempt to leverage big data, many organizations are holding on to more information than they may need. According to one panel of IG experts, almost 70% of retained data is unnecessarily kept.

"We are living in a post-Sony, post-Snowden world. We are in 2015, the 'year of the data breach,'" said Jason Baron, Esq., of counsel at Drinker Biddle and Reath. "If you secure the borders, you are doing something that is necessary, but that is not sufficient."

Jordan Lawrence's Marty Provins suggested organizations start with their e-mail. "If an organization did nothing but get better control over e-mail, they would be starting on a path to success," he said. "They tend to make arbitrary decisions over time limits on saving e-mail; the secret to making something work is to understand how they are using it, not having a one-size-fits-all model."

According to the panelists, some organizations are beginning to wonder if a chief IG officer (CIGO) is a necessity or a luxury. Baron said he could envision a scenario in which there was a need for a CIGO.

"I think the moment has come for one of two things," Baron said. "A designated head of info governance as a subfunction of legal … or a fully mature model where you have a C-suite person who stands as a peer of the CIO of an organization."

This need could materialize soon if 2015 does indeed shape up to be "the year of the data breach," as some have predicted.

"I think the job got a lot easier with the Sony Pictures breach," said Gareth Evans, a partner at Gibson, Dunn, and Crutcher. He added that data security is increasingly being addressed at the board level.

INFO SECURITY

## Finland Cracks Down on Social Media Companies

On January 1, Finland's new Information Society Code went into effect. The umbrella act simplifies the country's electronic communications legislation in an effort to improve consumer protection, boost information security, and strengthen competition among telecommunications markets.

The law fulfilled the first goal by consolidating 10 laws into one. Most notable is the new requirement that all electronic communication distributors – including social media companies – ensure the confidentiality of communications, reported *ZDNet*.

Olli-Pekka Rantala, director of the communications market at the Finnish Ministry of Transport and Communications, explained that this "is a small step towards a level playing field between traditional telecom operators and new internet players but it was a big change in principle."

In practice, the new law means that companies such as Apple, Facebook, and Twitter must ensure that users of their messaging services get the same standards of privacy and security as other already-regulated sectors such as telecoms, the article stated. The scope of the legislation also extends to companies based outside the EU but offering services in Finland.

The new code is in line with current EU legislation, but Finland is the first to extend its scope.

PRIVACY

## EU Data Protection Rules Hit a Snag

Creating a data protection law for the European Union (EU) as a whole is proving to be a grand challenge. Hopes for a law being passed this year are already dwindling.

The EU published a legislative package in January 2012 that would replace the existing rules (passed in 1995 when the Internet was still fledgling) and provide more protection to personal data across the EU. It was voted in during its first reading at the European Parliament in March 2014, before the elections, at which point it contained one directive and one regulation. The scope of the reform expanded following the scandal surrounding the U.S. cyber-espionage program PRISM.

Now it contains "an arsenal of measures" to protect European citizens' personal data, reported *EurActiv.com*. Companies that send personal data outside the EU without permission could face stiff fines. On that there is consensus. What may keep the law from being passed this year is a debate between Parliament and EU member states on the issues of informed consent for the use of data, sanctions, and privacy by design, according to German Green Parliament Member Jan Philipp Albrecht, the vice-chairman of the Parliament's civil liberties committee.

One of the most contentious points is the provision that citizens could complain to their local data protection authority regarding a breach anywhere throughout the EU. Albrecht told *EurActiv.com* that Germany, France, and the United Kingdom were all holding up the negotiations. The Germans are concerned the data protection rule would erode the sovereignty of the country's powerful regions. Both Germany and France worry that data issues could be decided in smaller member states that have less-established data traditions. The United Kingdom, Albrecht said, opposes the data protection regulation altogether, preferring instead that the EU adopt a directive.

EHR

## Feds to Ease EHR Certification Schedule

The medical community and electronic health records (EHR) vendors have been asking U.S. regulators for some time to slow down on the final implementation stages of EHR certification. A petition from a coalition of 35 medical societies, led by the American Medical Association, got a response.

"Among physicians there are documented challenges and growing frustration with the way EHRs are performing. Many physicians find these systems cumbersome, do not meet their workflow needs, decrease efficiency, and have limited, if any, interoperability. Most importantly, certified EHR technology (CEHRT) can present safety concerns for patients," the coalition stressed in its January 21 letter to the national coordinator for health information technology.

The group specifically asked that the regulators, among other things:

- Decouple EHR certification from the Meaningful Use program
- Consider alternative software testing methods
- Incorporate exception handling into EHR certification
- Develop guidance and tests to support exchange of data

On January 29, the Centers for Medicare and Medicaid Services (CMS) announced that it would be updating the EHR Incentive Program this year.

"The new rule, expected this spring, would respond to provider concerns about software implementation, information exchange readiness, and other related concerns in 2015," wrote Patrick Conway, M.D., the agency's deputy administrator of innovation and quality, in a CMS blog posting.

CMS is considering proposals to:

- Realign hospital EHR reporting periods to the calendar year to allow eligible hospitals more time to incorporate 2014 edition software into their workflows and to better align with other CMS quality programs
- Modify other aspects of the program to match long-term goals, reduce complexity, and lessen providers' reporting burdens
- Shorten the EHR reporting period in 2015 to 90 days to accommodate these changes

On January 30, the Office of the National Coordinator for Health IT (ONC) released for public comment a draft Interoperability Roadmap, which focuses on actions that will enable consumers and healthcare providers to send, receive, find, and use a core set of electronic health information nationwide by 2017. That core set of information would include standardized data such as demographics that would facilitate matching and linking the information across all systems and platforms, the ONC said in the draft.

The Roadmap identifies three "critical pathways" that need to be addressed to achieve this level of interoperability: 1) requiring standards; 2) incentivizing use of those standards; and 3) creating a "trusted environment" for collecting, sharing, and using electronic health information.

According to ONC, the four most important actions the public and private sectors need to take to make interoperability a reality in the near-term are:

1. Establish a coordinated governance framework and process for nationwide health IT interoperability.
2. Improve technical standards and implementation guidance for sharing and using a common clinical data set.
3. Enhance incentives for sharing electronic health information according to common technical standards, starting with a common clinical data set.
4. Clarify privacy and security requirements that enable interoperability.

ONC will accept public comments on the draft version of the Roadmap until 5 p.m. (ET) on April 3 via its website *www.healthit.gov/interoperability*. The draft is available at *www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf*.

INFO GOVERNANCE

## Study: Content Management Needs More than Technology

A new study revealed that most companies are dropping the ball when it comes to managing content enterprise-wide. Less than one-quarter of the participants in a study conducted by the APQC rated their content management practices as effective; 43% said their programs were minimally or not at all effective. Interestingly, the culprit was not the lack of technology. The vast majority said the biggest challenges were change management, organizational structure, and accountability.

"In short, employees weren't following processes in place to manage content or the organizations had not defined sufficient ownership models for the tools and approaches," according to the study conducted by APQC, a member-based association and proponent of best practices and business research.

These results prompted the benchmarking association to launch its second comprehensive best practices study. It focused on content management practices at five best-practice organizations and found that the one unifying characteristic was how attuned the content teams were to the needs of content stakeholders and end users inside their organizations.

"The best-practice organizations thoroughly understand their target audiences for content, and the result is that their tools and processes align with how people want to contribute, access, share, and reuse organizational knowledge," the research team observed.

As part of the research, the study team identified 20 best practices within the following general topic areas:

- Developing a strategy to connect people to content
- Creating content people want
- Managing the end-to-end lifecycle
- Ensuring content is findable and accessible in the flow of work
- Integrating content and social challenges
- Managing change and evaluating success

E-DISCOVERY

## IG, E-Discovery Pros to Win with FRCP Changes

There will be two big winners should the proposed amendments to the Federal Rules of Civil Procedure (FRCP) clear the U.S. Supreme Court as expected: information governance professionals and e-discovery consultants. That is a prediction made by Helen Geib, general counsel and practice support consultant for QDiscovery, in a recent article in *Law Technology News.*

The proposed changes emphasize the need to 1) know what electronically stored information (ESI) the client has; 2) know it early in the case; and 3) understand the technology for handling the data.

"The amendments' focus on preservation is a strong argument for better information governance," reasoned Geib. "In-house counsel must know the what, where, why, who, and how of their company's ESI to effectively implement and manage a litigation hold." Improved information governance, she noted, not only increases the company's ability to defend against preservation-compliance challenges, it helps in controlling costs.

That doesn't mean litigators will be off the hook. The pressure will continue to be on them to become more familiar with ESI and IT systems. "Even if the actual work of data mapping the client's ESI is delegated to others, lawyers must still be able to effectively communicate about ESI in the meet and confer, discovery plan, written discovery, and so on," said Geib.

CLOUD COMPUTING

## The Power of the Cloud

They came to the cloud to save money; they stay because of its potential to change their business. More precisely, almost half (49%) of the enterprise executives who participated in the 2014 Cloud Computing Survey conducted by KPMG, "Elevating Business in the Cloud," said the biggest benefit of using the cloud is its cost efficiency. However, an increasing number are using it to enact large-scale change at the business-unit level as well as enterprise-wide.

The transformative effect of the cloud is being realized by using it to better enable a flexible and mobile workforce; improve alignment and interaction with customers, suppliers, and business partners; and better leverage data for more "insightful" decision-making.

"Cloud has become almost a business imperative because the benefits seem to outweigh the risks," said KPMG's Rick Wright, principal and global cloud enablement leader. The survey participants reported that the cloud has helped them improve business performance (73%), improve levels of service automation (72%), and reduce costs (70%). These enhancements come at a price, however. More than half (53%) cited data loss and privacy risks as the most significant challenges of doing business in the cloud, followed by intellectual property theft. The high costs of implementation and the challenge of integrating the cloud with existing architecture are also notable stressors.

KPMG's survey report included five tips to help companies succeed with their cloud transformations:

1. Make cloud transformation a continuous process.
2. Drive cloud transformation from the top.
3. Focus on strong leadership and engagement.
4. Avoid silos.
5. Measure success. END