PRIVACY

Study: 75,000 Data Protection Officers Needed by 2019

The EU's General Data Protection Regulation (GDPR) will drive the need for at least 75,000 new data protection officers (DPOs) worldwide over the next two years, according to a recent study conducted by the International Association of Privacy Professionals (IAPP), covered recently by *Computerweekly.com*.

Trevor Hughes, president and CEO of the IAPP, said the data protection profession has been growing steadily for years and such growth should accelerate as a result of the GDPR mandate.

"But good business is also a major driver; organisations today simply must address privacy concerns to succeed in the information economy," he said.

The GDPR governs the privacy practices of any organization that handles EU citizens' data, regardless of its location. Because the EU is the world's largest economy and top trading partner for 80 countries, thousands of organizations around the globe will be subject to the GDPR.

Article 37 of the GDPR requires all processors and controllers of EU citizens' personal information to designate a DPO when the processing is done by a public authority or when core activities require "regular and systematic monitoring of data subjects on a large scale" or consist of "processing on a large scale of special categories of data."

Once an organization has appointed a DPO, the work has only just begun, according to Omer Tene, vice-president of research and education at the IAPP. "Organisations will need to ensure DPOs are well qualified and trained in the growing body of knowledge of the privacy profession, including law, technology and data management best practices," he said.

PRIVACY

Presidential Transition Shouldn't Threaten EU Privacy Agreement

An official from the Department of Commerce believes the United States under the Trump administration will keep its commitment to a trans-Atlantic data transfer pact that organizations around the globe depend on.

"We have a real expectation that a new administration would come in and follow through on" what's been done, said Ted Dean, deputy assistant secretary for services at the Commerce department. His remarks came at a privacy conference in Brussels on November 9.

According to Dean, any move away from the commitments the United States has made after long negotiations with the EU to agree on the EU-U.S. Privacy Shield – which was enacted in July to replace the annulled "safe harbor" accord – would face "tremendous pressure" from industry.

"This whole program was built with very significant ongoing interaction between U.S. and European Commission and data protection authorities," Dean said at the event, which was organized by the International Association of Privacy Professionals. He said the mechanism was designed with the knowledge that a political transition would soon occur.

An American intelligence official is bullish as well on U.S. commitment to the deal. "From the intelligence community's point of view, we're committed to this going forward," said Robert Litt, general counsel for the Office of the Director of National Intelligence. "I think that the intelligence community believes that on the whole we're better off with this, than without it."

RISK MANAGEMENT

Compliance Is Key Demand for Legal Tech Providers

As reported on *Legaltechnews.com*, an AlixPartners survey finds that many U.S. and European organizations are extending their risk management compliance to vendors.

The survey spoke to 300 corporate counsel and legal and compliance officers across North America and Europe.

Nearly all respondents (96%) said their use of new technologies to mitigate internal risks stayed the same over the past year; 38% noted an increase in legal department implementation in 2016.

The survey found that many organizations are holding compliance technology and services to a higher standard, stressing the importance of adhering to data handling and data security compliance regulations, such as the General Data Protection Regulation and Health Insurance Portability and Accountability Act. In fact, roughly one-third of all respondents said they would pay more to store their information at certified data centers. In addition, 40% said they would work only with e-discovery providers who deliver the highest level of compliance.

Michael Prounis of AlixPartners said the demand for certified e-discovery providers is higher for heavily regulated industries such as finance, but even the less-regulated "are still generally becoming savvier in their vendor selection and vetting activities regarding security and privacy assurances."

The survey may have exposed a "disconnect" for some between the concept of information governance (IG) and the reality of it. The responses suggest that more organizations see managing risk as a data security function rather than a broader IG implementation. Around 60% of respondents, for example, called data security important for managing risk, while only 46% said the same of IG.

It is Prounis' hunch that even though many respondents did not highlight the importance of IG, they may be implementing such processes as part of their data security program.

"Information governance as a discipline is still quite young and immature so this disconnect is most likely driven by many varied interpretations of the term 'information governance' by the respondents," he said.

"We all know you can't build a robust data security program without some level of information governance. So, we suspect that the other 54 percent are engaging in many information governance activities, such as updating their records retention programs, cleaning up legacy data stores, mapping information flows and inventorying data assets to address internal risks without calling these information governance programs, per se."

BYOD

Employees Pressured to Use Personal Smartphones at Work

Increasingly, employees are being asked to use their personal devices for workplace purposes, according to a survey from *Syntonic*, a mobile content solutions provider.

As reported on *CIO.com*, the survey found that 87% of the employers it queried expect their employees to use their personal smartphones to access business apps. Likewise, nearly half of the employees said their bosses required them to use their smartphones while on the job, and 23% said they felt pressured to use their personal devices when away from the workplace.

Meanwhile, many organizations have yet to establish bring your own device (BYOD) policies – many, in fact, aren't even sure who should lead the charge. The survey found that 45% of CEOs say they should head an enterprise-wide BYOD program, while 73% of CIOs and half of the CFOs said it falls under the jurisdiction of IT.

Sinan Eren, a vice president with Vast Mobile Enterprise, says organizations should secure their own data that lives on those devices and create policies for what can and cannot go onto a personal device. According to Eren, the security threats mostly lie with the apps that host the corporate data.

Rather than fixate on hardware security features and attempt to micromanage every smartphone in the enterprise, Eren believes an organization should identify the data that would pose the biggest threat and then figure out how to lock it down.

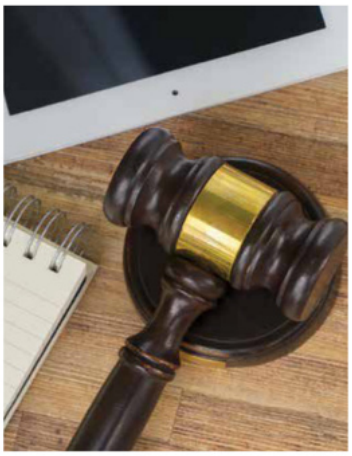
He also believes a BYOD strategy must adapt as technology evolves, and it must focus on employee privacy. "Employees expect their employers will not monitor, inspect, alter or destroy any of their personal content and apps under any circumstance," Eren told *CIO.com.*

CLOUD COMPUTING

Court Compels Defendant to Tap Knowledgeable IT Personnel

A recent South Dakota case highlighted on *ediscovery.com* centered on how well an organization's IT personnel should understand its systems, its data storage practices, and the access to that data.

In *Collins v. St. Paul Fire & Marine Ins. Co.,* the plaintiff, Collins, filed a motion to compel discovery. He claimed the defendants provided an insufficient response to a legal interrogatory that asked for "the person most familiar with [defendants'] electronic claims systems and electronic claims database," such as an IT member.



In response to that interrogatory, St. Paul Fire & Marine had said the persons most familiar with the company's electronic systems and database were the claims adjustors and the supervisors who handled the claims. To locate an IT member would be unduly burdensome and irrelevant, the defendants argued.

The court sided with Collins, saying that IT personnel have knowledge of the systems, of how the company stores data, and of who can access that data – knowledge that is far superior to that of the claims adjustors. Accordingly, the court granted the motion to compel.

CYBERSECURITY

Most Ransomware Attacks Bypass E-mail Filtering

As reported on *esecurityplanet.com,* the results of a recent Barkly survey suggest that ransomware attacks are routinely bypassing e-mail filters.

The survey queried 60 organizations that had been hit by a ransomware attack in the past year. More than three-fourths of the respondents said the attacks bypassed their filters. Additionally, 95% of the attacks bypassed the victims' firewalls as well, and about half of them got past the systems' anti-malware solutions.

Further, about one-third of the attacks succeeded even though the organizations had conducted security awareness training.

In response to the attacks, many companies doubled down on the security measures that had already failed them: about a quarter of them invested in e-mail filters or security awareness training, 20% in antivirus tools, and 17% in firewalls. In contrast, 43% of the respondents did nothing to combat future attacks.

An earlier Barkly survey had revealed that 81% of IT pros believed a data backup mechanism could provide complete recovery from a ransomware attack. Yet, the more recent study found that fewer than half of the organizations were able to recover fully even with a backup plan in place.

Rick Orloff, an executive with Code42, told eSecurity Planet that ransomware is on track to become a billion-dollar business in 2016.

"It's not exactly a surprise that hackers have turned to targeting businesses with ransomware," he said. "Despite its proliferation, ransomware is profitable because many companies don't have the right security solutions or expertise to combat it."

"Despite its proliferation, ransomware is profitable because many companies don't have the right security solutions or expertise to combat it."

Information security expert G. Mark Hardy, who authored the Barkly report, said, "Increasing user awareness, information and intelligence sharing, as well as improving overall risk posture, will be key issues that IT security teams must face sooner rather than later."

It is your life. It is your career. It is your certification.

CRM

In a business world of doing "more with less," your designation as a Certified Records Manager shows that you understand the many facets of the RIM profession.

In a business world that is rapidly changing, your designation as a Certified Records Manager shows you are up to date on the latest technology, the latest rules and regulations, and the techniques of the RIM profession.

In a business world in which new jobs are increasingly competitive, your designation as a Certified Records Manager (CRM) demonstrates that you have the experience and expertise to lead change and deploy best practices as they evolve in the RIM profession.

For more information about becoming a Certified Records Manager, contact (518) 694-5362 or visit www.icrm.org

ICRM®
Institute of Certified Records Managers

INTERNET OF THINGS

In an Internet of Things World, Humans Assist Machines

During the past two years, the number of Internet of Things (IoT) devices in the world has skyrocketed almost 70% to 6.4 billion, according to research firm Gartner. By 2020, Gartner predicts, the IoT population will hit 20.8 billion.

IoT fans say the technology will enable people and systems to live and work smarter, easier, and more efficiently. But critics worry that such networked technologies will be easy prey for hackers. Just like they do for their computers or smartphones, consumers certainly will need to adopt safety precautions for their Internet-connected home appliances, experts say.

"If we want to put networked technologies into more and more things, we also have to find a way to make them safer," Michael Walker, a computer security expert at the Pentagon told the *New York Times*. "It's a challenge for civilization."

Researchers for Level 3 Communications recently announced they had detected several strains of malware that launched attacks on websites from compromised IoT devices, the *Times* reported. The researchers, working with Flashpoint, an Internet risk management firm, found that as many as one million devices, mainly security cameras and video recorders, had been equipped for botnet attacks. They said the discovery marked a "a drastic shift": IoT devices are now being used as hosts for attacks instead of traditional hosts, such as hijacked data center computers and computer routers in homes.

Late last year, researchers at Akamai Technologies said they detected hackers commandeering as many as two million devices, including Wi-Fi hot spots and satellite antennas, to test whether stolen user names and passwords could be deployed to gain access to websites, the *Times* reported.

To address these challenges, Walker and the Defense Advanced Research Projects Agency (DARPA) created a contest called the Cyber Grand Challenge and offered millions in prize money. To win, contestants had to create automated digital defense systems that could identify and repair software vulnerabilities on their own.

The contest demonstrated how machine automation and human expertise might be combined in computer security. Currently, automation in the security industry applies to one element of security, such as finding software vulnerabilities, monitoring networks, or deploying software patches.

For the DARPA test, however, the attack code was new, created for the event. The teams played both offense and defense and could not get human help. The software was on its own to find and exploit flaws in opponents' software, scan networks for incoming assaults, and write code to tighten its defenses, according to the *Times*.

The winners integrated different software techniques, in ways not done before, into automated "cybersecurity systems.

INFO SECURITY

Survey Shows More than Half of Companies Use Biometric Authentication

Advanced user authentication methods are becoming more popular among businesses because the traditional password no longer provides enterprise security, according to a *PwC* survey.

"The Global State of Information Security Survey 2017" found that 57% of respondents are using some form of biometrics for authenticating users, including fingerprints, retina scans, and facial recognition.

More than 10,000 CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security practices from 133 countries responded to the *PwC* survey.

David Burg, PwC's U.S. and global leader of cybersecurity and privacy, told *Legaltech News* that the use of advanced authentication is being spurred by companies' increasing awareness that employees aren't following proper password policies.

"By utilizing this technology, it allows companies to offset this potential weakness while also adding an extra layer of security and improving trust among customers and business partners," Burg explained. "In the past, advanced authentication was primarily the technological domain of government systems and large financial institutions or, more recently, social media and consumer email providers. But now a broader range of sectors are adopting multifactor authentication across a range of transactions."

INFO SECURITY

Directors, Executives Careless with Sensitive Data, Survey Finds

When it comes to safeguarding sensitive company data, lower-level employees appear to be more careful than directors and C-level executives, a recent survey has revealed.

According to the survey of more than 4,000 employees in North America and Europe, 49% of mid-market managing directors (MDs) and C-level executives (CxOs) have used their personal e-mail accounts to send sensitive business information.

The survey, conducted by Opinion Matters and commissioned by Iron Mountain, also found that:

- 57% have left business-sensitive or confidential information in the printer.
- 40% have sent information over an insecure wireless network.
- 43% have disposed of documents in a potentially insecure trash bin.
- 39% have lost business information in a public place.

Interestingly, the survey revealed that lower-level employees are more security-conscious – only 29% of administrative staff said they have left confidential information in the printer, and just 15% said they have lost business documents in a public place.

When asked about processes in place to protect sensitive data, 21% of CxOs said such processes are too complex and so they look for a way to evade them. Also according to the survey, another 14% said they don't follow company policies regarding data security because they consider the policies too complicated, and 6% are unaware of any such policies at all.

"Our research shows that business leaders in the mid-market are more likely to put sensitive information at risk than any other employee," Iron Mountain UK Commercial Director Elizabeth Bramwell said in a statement. "They tend to bypass the very protocols designed to keep information secure. Given the potential consequences, this is concerning.

According to eSecurityPlanet, another survey conducted in 2016 of 1,022 U.S. respondents found that 13% of employees have allowed colleagues to use devices that can access their employer's network, 9% have allowed their partners to do so, and 1% have even allowed their children to do so – despite the fact that one in five employees had no security software on their work devices.

That survey, conducted by Arlington Research on behalf of OneLogin, also found that 20% of employees share their company e-mail passwords, and 12% share passwords to other work applications.

Remarkably, almost half of all employees surveyed said they were not aware of any company policies concerning the sharing of passwords, according to the survey.

GOVERNMENT RECORDS

Former Contractor Stole More Than 50TBs of Government Data

In what is being called the biggest case of classified document mishandling in U.S. history, FBI agents recently seized more than 50 terabytes of classified documents from the Maryland home of a former National Security Agency (NSA) contractor.

According to a recent federal court filing, Harold Martin spent 20 years working for multiple government agencies, including the NSA. He was arrested in August but it may take months before agents finish combing through the classified material he had accumulated. According to *PC Magazine*, it is unclear whether all the files are classified, but prosecutors said much of it is likely "national defense information."

Martin was arrested less than a week after federal authorities announced they were investigating a leak of the NSA's hacking tools. The leak included a 31-page document describing tools for tracking surveillance targets and appears to have come from two hacker groups.

Investigators are trying to prove that Martin gave the documents to the groups, the *New York Times* reported. They found some forensic clues that he might be the source, but the evidence is not conclusive, officials told the *Times*.

According to the filing, prosecutors said Martin was careless in how he stored some of the information, with many of the hard-copy documents found scattered around his home office and in the trunk of his car. But he was careful with the digital records.

CYBERSECURITY

How E-Discovery Is Safer with Cloud Providers

According to *The Wall Street Journal,* the number of breaches tracked by the national Identity Theft Resources Center was up in 2016, and the FBI reported a notable increase in ransomware. In New York, State Attorney General Eric T. Schneiderman said data breaches in his state rose 40% last year.

A 2016 study of data breach costs by the Ponemon Institute found that the average cost of a data breach is $4 million. But for any business, the damage could extend far beyond just financial loss, including damage to its reputation and loss of customers. In addition, a company loses data that may be needed for litigation, the damage could be profound.

So how does a business best protect its data, especially in light of e-discovery considerations? According to *Legaltech News,* cloud service providers provide the highest level of data security for e-discovery, delivering:

- **Sophisticated encryption:** There are different ways to handle encryption, including methods that protect data in storage, in transit, and while moving from one application to another. Most data centers and businesses storing data onsite often don't have such technologies because they are typically expensive and complex. Also, they aren't able to make data available on demand while ensuring it is fully encrypted and widely accessible. However, some cloud providers offer all these options as part of their standard plan, meaning that they protect sensitive business data while ensuring compliance with regulations such as HIPAA, HITECH, and others that protect personally identifiable information.
- **Constant security expertise:** Cloud service providers typically have a large team of security experts because their business depends on reliable, dependable security. These experts monitor their cloud environment 24 hours a day, 365 days a year. They also constantly implement improved security technologies and the latest best practices. Businesses and data centers cannot afford to maintain such scrutiny.
- **Early access to new technology:** Emerging technologies are often implemented in the cloud first because that's where ever-increasing amounts of data are stored and processed. The world is shifting to a software-as-a-service model, and most programs used today, including smartphone apps and business software, are served from the cloud. Security experts say cloud services providers will likely be the first adopters of fully homomorphic encryption, an emerging technique that allows data to remain encrypted even during processing.

GOVERNMENT RECORDS

NARA Announces New FOIA Ombudsman

Alina Semo, the U.S. National Archives and Records Administration's (NARA) director of litigation in the Office of General Counsel, has been tapped as the new director of the Office of Government Information Services (OGIS), which oversees Freedom of Information Act (FOIA) activities across government.

OGIS was created under the OPEN Government Act of 2007 to serve as an ombudsman between FOIA requesters and federal agencies. The OGIS director's responsibilities include leading the FOIA Advisory Committee, providing policy guidance for agencies, ensuring open government law compliance, and mediating disputes between requesters and agencies, according to *FCW.com.*

FCW.com said Semo brings 25 years of federal litigation experience to the role. As NARA's director of litigation, she provided legal advice to agencies, helped revise NARA's FOIA regulations, and worked with the FOIA Advisory Committee. Before joining NARA, Semo worked as chief of the FOIA Litigation Unit for the Federal Bureau of Investigation's general counsel, where she helped establish litigation tracking systems and streamline legal and clerical processes.

"Ms. Semo is a dedicated public servant who is uniquely qualified for this position," National Archivist David Ferriero said in a statement. "Her extensive experience with FOIA at both the administrative stage and in federal court litigation, knowledge of National Archives and commitment to open government will serve her well in her position as director of OGIS."

PRIVACY

FCC Approves Rules to Protect Internet User Data

In a landmark vote that will create new protections for Internet users, the Federal Communications Commission (FCC) approved new privacy rules that prevent broadband providers from collecting and sharing digital information about individuals.

Federal officials voted 3-2 to require companies such as AT&T and Comcast to get subscriber permission before gathering and giving out data on their web browsing, app use, and location and financial details, the *New York Times* reported. At present, providers are able to track users unless those individuals ask them to stop doing so.

The FCC has enacted privacy rules for phone and cable providers before, but this is the first time it has decided to require high-speed Internet providers to follow privacy restrictions.

"There is a basic truth: It is the consumer's information," Tom Wheeler, FCC chairman, said of the need to protect Internet users who want more control over what companies do with their private information. "It is not the information of the network the consumer hires to deliver that information."

Privacy groups praised the new rules, saying that they will move the United States closer in line with European online privacy protections.

"For the first time, the public will be guaranteed that when they use broadband to connect to the Internet, whether on a mobile device or personal computer, they will have the ability to decide whether and how much of their information can be gathered," said Jeffrey Chester, executive director of the Center for Digital Democracy.

Industries that rely on online user data to collect targeted advertising, however, were not pleased by the passage of the new rules, the *Times* said. The Association of National

Advertisers has called the regulations "unprecedented, misguided, counterproductive, and potentially extremely harmful."

The FCC rules are not all-encompassing. The FCC does not have jurisdiction over Internet companies, so they are not required to follow the new rules, according to the *Times*. That means online web companies like Google and Facebook instead are required to follow general consumer protection rules enforced by the FCC and do not have to explicitly ask users' permission before gathering web browsing information.

The FCC rules apply only to broadband businesses, so AT&T, Verizon, and Comcast can still gather consumers' digital data, as well, just not as easily as before. According to the *Times*, data on the habits of AT&T's wireless and home broadband customers would be subject to the regulations, but not data about AT&T's DirecTV users or users of the HBO Now app.

The companies also can collect information about people in other ways, such as by purchasing data from brokers.

The new rules give major broadband providers about one year to make the changes, and companies must notify users of their new privacy options via e-mail or dialogue boxes on websites. After the rules are enacted, broadband providers must immediately stop collecting data that the FCC deems sensitive, including Social Security numbers and health data, unless a customer gives permission.

"Hopefully, this is the end of what has been the race to the bottom for online privacy, and hopefully the beginning of a race to the top," said Harold Feld, senior vice president at nonprofit public interest group Public Knowledge.

E-DISCOVERY

Study: Best E-Discovery Review Requires Humans and Technology

Before choosing technology-assisted review (TAR) over human review, consider that the best systems for e-discovery include a combination of people and software, new research has revealed.

The joint project by nonprofit Electronic Discovery Institute (EDI) and Oracle Corp. found that TAR is often faster and cheaper when identifying relevant documents. However, when it comes to identifying privileged or sensitive information, human reviewers outperform machines, the research shows.

While software programmed to identify responsive documents could cut up to 80% from firms' discovery expenses, researchers found that privileged and "hot" documents that require conceptual knowledge rather than keyword searches or predictive coding are better reviewed by humans skilled in the practice area.

"It's not a magic bullet. Nobody says that predictive coding is a good way of finding privileged documents, but it's a good supplement if you're using it for quality control," TAR proponent U.S. Magistrate Judge Andrew J. Peck of the Southern District of New York told *Legaltech News*. "It's a combination of the technology, the people involved, and the workflow process."

"Nobody says that predictive coding is a good way of finding privileged documents, but it's a good supplement …for quality control."

According to *Legaltech News*, EDI's research is the most comprehensive evaluation of document review in e-discovery ever conducted in the United States. The project, which began in 2012 and lasted four years, studied how effective technology is at complying with Rule 26(g) of the U.S. Federal Rules of Civil Procedure. It involved more than 1.6 million documents created by Oracle's response to a federal government probe of Sun Microsystems. Documents from the settled case provided a real-life data sample.

John Rosenthal, a partner at firm Winston & Strawn, assisted as a quality-control check. "For those of us steeped in how the algorithms work, it really was not a surprise," he said. "TAR is somewhat faster, somewhat less expensive, but not as dramatic as what the vendors would lead you to believe. I'm a proponent of it in that perspective, but if you're choosing TAR because you think it will be better than human review, I don't think the study substantiates that."

INFO GOVERNANCE

Tensions Prompt Changes to England's NHS IG Toolkit

DigitalHealth.net reports that NHS England has launched a new information governance (IG) network with the goals of simplifying IG, challenging IG myths, and holding national bodies to account when their IG requirements are "outdated and unwieldy."

The network is part of the IG Toolkit (IGT), an online tool that permits health and social care organizations in England to assess themselves against government standards.

Rob Shaw of NHS Digital, recently – prematurely – announced the organization was scrapping the IGT in its current form.

"We are looking to make it more meaningful, looking to make it light-touch," he said at a November event.

Later, NHS Digital said the toolkit would not be scrapped and organizations were still expected to adhere to it.

In July, a national data guardian review had announced an initiative to improve the IGT. In part, the statement said the following: "There is a programme of work underway to improve the IGT, to increase its relevance for senior managers, its accessibility for small organisations and its focus on the new data security standards recommended by the national data guardian."

That review also said the IGT was just a "tick-box exercise" and that it would require simplification to "support rather than inhibit data sharing."

In a blog, Geraint Lewis, NHS England's chief data officer, wrote "there is a widespread view that [IG] in England has become too Byzantine in its complexity and that, in practice, it is too risk averse and too inflexible to meet the modern needs of patients and clinicians."

Lewis called for the NHS to move to models of care that require greater sharing of patient information and of best practices.

Congratulations

to the IGP Class of 2016

Angela Akpapunam
Xavier Alabart
Anthony Allen
Wendy Austin
Robert Bailey
Bruce Bailey
Tina Baker
Scott Barnes
Charles Barth
Jayne Bellyk
Shawn Belovich
Mike Biancaniello
Deanna Brouillette
Stephanie Buholz
Patrick Butts
Karen Campbell
Elizabeth Carrera
Elizabeth Causey
Melody Christofferson
Steven Coates
Mary Coffee-Sevald
Marshall Commons
Charlene Cunniffe
Ingvild Daasvand
Ilya Davidovich
James Dawson
Ayala Deasey
Suzanne DiCicco
Dondi Duffy
Susan Emery
Sarah Emes
Frank Fazzio III
Clinton Field
Mariel Fox
Audrey Gaines
Claire Galloway Jenkins
Celine Gerin-Roze
Frank Girello
Sophia Hani
Julie Harvey
Janet Hodges
Wayne Hoff
Constance Jamu
Elizabeth Johnson
Kurt Johnson
Mark MacFarlane
Felecia McKnight
Robert McLauchlin
Julia Mewbourne
Lee Michael
David Mills
Shanna O'Donnell
Anita Paul
Scott Procter
Jason Schulz
Jason Scott
James Sherer
Robert Smallwood
Kathleen Smith
Kirke Snyder
Courtney Stone
Kathleen Story
Edward Sumcad
Alexander Webb
Katherine Weisenreder
Christopher Whitaker
Darla White
Natausha Wilson
Dorothy Wood

Spring 2017 Testing Dates: March 20 - May 19 *www.arma.org/igp*

GOVERNMENT RECORDS

CIA to Post Millions of Declassified Documents Online

The CIA is moving more than 11 million pages of previously declassified documents to its public *CIA.gov* website, according to *fcw.com*.

In 2000, the agency created the CIA Records Search Tool (CREST), an electronic database of documents declassified under a Clinton administration executive order calling for the declassification of historically valuable records that are 25 years old or older.

CREST was quickly criticized, however, because although the documents had been publicly released, they could be accessed and searched only at the National Archives and Records Administration (NARA) facility in College Park, Md., where it was housed.

"The migration is certainly a welcome move, especially if the existing search functionality – which is quite good – is retained on the new site," said Steven Aftergood, director of the Federation of American Scientists' Project on Government Secrecy and a longtime critic of CREST being kept offline.

CIA spokesman Jonathan Liu said putting the documents online will "dramatically increase" the public's ability to access them. "When loaded on the website, the documents will be full-text searchable and have the same features currently available on the CREST system at NARA," he said.

Liu added that "the CREST database housed at NARA will remain up and running at least until the website is fully functioning." He did not provide a time frame for when the new website would be available, saying only that the agency is "moving out on the plan to make the transition."

The move will appease Aftergood and others who have been pressing the agency to make the documents more accessible.

"There has been a drumbeat of public demand for access to these soft-copy records for a decade or longer," he said.

PRIVACY

Japan, U.S. Agree on Cross-Border Privacy System

Representatives of Japan's Personal Information Protection Commission (PPC) and the U.S. Department of Commerce have announced their joint commitment to implement and expand the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) system.

According to the announcement, Japan's decision to recognize the CBPR system "as a mechanism for international data transfers in the implementing guidelines for Japan's amended privacy law marks an important milestone" for the development of the system in Japan.

The PPC "has resolved to advocate for further cooperation with foreign counterparts to enable cross-border transfer of personal information while ensuring the protection thereof," said PPC Secretary General Mari Sonoda. "The commission will work strenuously to ensure the reciprocal and smooth transfer of data, including by promoting the APEC CBPR system."

Currently, only four countries are participating in the APEC CBPR system: the United States, Mexico, Japan, and Canada, although more are expected to join soon. The system requires participating countries to have their privacy policies and practices evaluated by an independent accountability agent, which works with companies, consumers, and governments to ensure that cross-border personal data transfers meet the standards required by the APEC Privacy Framework and to resolve any disputes that arise.

According to the Privacy and Information Security Law Blog at the law firm of Hutton and Williams, a draft report conducted by the Vietnam e-Commerce and Information Technology Agency titled "Survey on the Readiness for Joining CBPRs" shows that Korea, Singapore, and the Philippines plan to join, while Australia, Hong Kong, Russia, Taiwan, and Vietnam are considering joining. The blog states that several unresolved issues need to be resolved first, including "which government agency would lead the application process or be responsible for enforcement of the CBPR, and how to structure the certification process to ensure its scalability to companies of all sizes."

MOBILE DEVICES

Smartphones Sent User Data to China, Security Contractors Say

Text messages sent by international smartphone customers and those who use disposable or prepaid phones have been sent to China every 72 hours, thanks to preinstalled software in some Android phones.

According to the *New York Times*, security contractors recently discovered the software, which monitors where users go, to whom they talk, and the content of their text messages. The Chinese company that created the software, Shanghai Adups Technology Co., said its code runs on more than 700 million phones, cars, and other smart devices. One American phone manufacturer, BLU Products, said that 120,000 of its phones had been affected and that it had updated the software to eliminate the feature.

Kryptowire, the security firm that discovered the issue, said the Adups software sent the full contents of text messages, contact lists, call logs, location data, and more to a Chinese server. The code comes preinstalled on phones and users are not warned about the surveillance, Tom Karygiannis, a vice president of Kryptowire, told the *Times.*

In fact, a document provided by Adups to BLU executives revealed that Adups purposefully designed the software to help a Chinese phone manufacturer monitor user behavior. However, that version of the software was not intended for American phones, the company said.

The software, known as firmware, tells phones how to operate, the *Times* said. Adups provides the code that enables companies to remotely update their firmware. Usually, when that happens, the company tells customers what it is doing and whether it will use any personal information. But that did not happen with the Adups software, Kryptowire said.

Adups' website says that it provides software to two of the largest cellphone manufacturers in the world, ZTE and Huawei – both located in China. Adups also provides what it calls "big data" services to help companies study their customers, "to know better about them, about what they like and what they use and where they come from and what they prefer to provide better service," its websites states.

Lily Lim, a lawyer who represents Adups, said the software was written to help a Chinese manufacturer identify junk text messages and calls. She said she did not know how many phones were affected, and told the *Times* that phone companies, not Adups, were responsible for disclosing privacy policies to users. "Adups was just there to provide functionality that the phone distributor asked for," she said.

According to the *Times*, Android phones use software that is developed by Google and distributed free for phone manufacturers to customize. A Google official said the company told Adups to remove the surveillance ability from phones that run services such as the Google Play store. But because Google does not do business in China due to censorship issues, Adups did not have to follow that dictate for devices in China, where hundreds of millions of people use Android phones.

Executives of the Florida-based BLU Products have assured customers that the company moved quickly to correct the problem and today "there is no BLU device that is collecting that information." Samuel Ohev-Zion, BLU chief executive, added that Adups had assured him that all of the information taken from BLU customers had been destroyed.

International customers, however, are left to guess. Adups has not published a list of affected phones, so it's not clear how users can find out whether their phones are affected. "People who have some technical skills could," Karygiannis said. "But the average consumer? No."

Lim also told the *Times* that she did not know how phone users could determine whether their data was vulnerable.

CYBERSECURITY

Lessons from the Yahoo Breach

When Yahoo recently announced that at least 500 million Yahoo users' account information was stolen by hackers in 2014, the biggest surprise was not that it was the largest data breach to date, but that it took Yahoo nearly two years to discover and make it public.

In a statement, Yahoo said user information – including names, e-mail addresses, telephone numbers, birth dates, encrypted passwords, and, in some cases, security questions – was compromised in 2014 by what it believes was a "state-sponsored actor."

According to the *New York Times,* Yahoo is one of the Internet's busiest sites, with one billion monthly users. Many users have used it to build their digital identities, from their bank accounts to photo albums and even medical data.

Upon discovering the breach, Yahoo instructed users to change their passwords and remain vigilant over all of their online accounts. Yahoo said it was working with law enforcement and encouraged people to change the security on other online accounts and monitor those accounts for suspicious activity as well.

Yahoo said it learned of the data breach this past summer after hackers posted to underground forums and online marketplaces what they claimed was stolen Yahoo data, the *Times* reported. A Yahoo security team was unable to verify those claims, but eventually found a breach by what the team believes was a state-sponsored actor that dated back to 2014.

Two years is a long delay for identifying a hacking incident. According to Ponemon Institute, which tracks data breaches, the average time it takes organizations to identify such an attack is 191 days, and the average time to contain a breach is 58 days after discovery.

Security experts told the *Times* the breach could result in class-action lawsuits on top of other costs. An annual report by the Ponemon Institute released in July found that the average cost to remediate a data breach is $221 per stolen record. In Yahoo's case, that would total more than $4.8 billion – the price Verizon Communications is in the process of purchasing Yahoo for at present. The *Times* said it was not clear how the breach would affect the acquisition.

Sen. Mark R. Warner (D-VA), a former technology executive, has called for a federal "breach notification standard" to replace data notification laws that vary by state. Warner said he was "most troubled" that the public was only learning of the incident two years after it happened.

INFO SECURITY

Survey: Firms Look to Counsel, IT to Handle Data Breaches

Which internal players do companies rely on to handle compliance and data breach issues? According to a recent survey, the general counsel and IT staffs win.

The survey, from insurance analytics company Advisen and insurer Zurich North America, asked more than 300 risk management professionals which department in their organization is responsible for ensuring compliance with all privacy laws, including data breach notification laws..

Respondents said they look to the office of the general counsel (24%) and IT (23%), followed by the chief privacy officer/chief information security officer (17%).

Interestingly, in the 2015 version of the same survey, Advisen and Zurich asked the same question and found that IT was the top response, garnering 31% of the vote. In that survey, general counsel registered only 21% of the vote.

The 2016 survey also revealed that:

- A technology interruption due to a cyber threat would have a "moderate-to-significant" impact on the business of 87% of respondents.
- About 65% of companies have purchased security and privacy insurance, which marks a 7% increase from 2015.
- The top reason for buying a security and privacy policy is the cost of a customer information breach.

CYBERSECURITY

What *FTC v. LabMD* Means for Cybersecurity

An old case may help define the Federal Trade Commission's (FTC) regulatory role in overseeing cybersecurity and indirectly creating a federal cybersecurity law.

It began in May 2008, when Michael Daugherty, CEO of LabMD, was informed that Robert Boback of the cybersecurity firm Tiversa claimed to have found sensitive LabMD files on the peer-to-peer file-sharing network LimeWire. As proof, Boback e-mailed Daugherty a LabMD billing file with the names, birth dates, addresses, and Social Security numbers of 9,300 company patients. LabMD traced the file to a billing manager who had violated company policy by downloading LimeWire on her computer.

When LabMD searched online for the file, it found nothing. But in January 2010, Daugherty received an 11-page notice of investigation from the FTC in the mail – a notice that began an ongoing battle for LabMD as well as a redefining of the FTC's authority to oversee and govern cybersecurity.

According to a *Legaltech News* report, the legal interpretation of the unfairness standard of Section 5 of the FTC Act is at the center of the case. It gives the commission authority over an "act or practice [that] causes or is likely to cause substantial injury to consumers."

The courts must determine whether the exposure of LabMD's billing file – copies of which apparently neither traveled far outside the company's network, nor were picked up and used for any obvious malicious purpose – was likely to cause harm. But the opinion will send shock waves far beyond LabMD, all the way to company boards that direct enterprise data security, courtrooms that litigate injury caused by cyber incidents, and regulatory agencies that fight harmful data practices, according to legal experts.

In November 2015, D. Michael Chappell, FTC chief administrative law judge (ALJ), ruled the commission had failed to prove that anyone had been harmed by LabMD's data security practices. In his 95-page opinion, Chappell wrote that "[a]t best, complaint counsel has proven the 'possibility' of harm, but not any 'probability' or likelihood of harm. Fundamental fairness dictates that demonstration of actual or likely substantial consumer injury under Section 5(n) requires proof of more than the hypothetical or theoretical harm that has been submitted by the government in this case."

But the FTC disagreed. In July 2016, the commission unanimously overturned Chappell's decision, finding that LabMD's data security practices lacked even basic precautions and were unreasonable under Section 5 of the FTC Act. FTC Chair Edith Ramirez wrote that "contrary to the ALJ's holding that 'likely to cause' necessarily means that the injury was 'probable,' a practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low."

Still, while LabMD certainly mishandled sensitive information, no evidence ever surfaced to prove that anyone suffered. "Nobody spoke up and said their medical information had been exposed. Nobody spoke up and said they were embarrassed by that or it violated their privacy – there was no evidence of medical identity theft," said Julie O'Neill, a former FTC staffer. The basis for the FTC's action, she said, is the belief that personal data "was exposed is an injury unto itself, even if nothing further comes of it."

Legal critics say the FTC's action against LabMD means the commission is widening its scope to regulate potential and intangible cybersecurity risk, regardless of any evidence of harm. And by doing so, many fear the commission may be over-reaching.

As of September 2016, *Legaltech News* reported that LabMD's legal team was weighing where it would file the appeal and which arguments it would raise. Under the FTC's rules, LabMD can appeal to any federal appeals court.

E-DISCOVERY

Court Doesn't Punish Plaintiff for Losing Texts

In a recent North Carolina case, *Shaffer v. Gaither,* the court ruled that even though the plaintiff failed to preserve her text messages, the requisite intent under FRCP 37 (e)(2) did not exist, and so it did not sanction her.

The defendant had asked the court to dismiss the case for evidence destruction. The plaintiff admitted to accidentally dropping her phone, which resulted in the loss of relevenet text messages The plaintiff filed the litigation in June 2014, one month after dropping the phone.

The plaintiff contended she was "constructively discharged" when she quit as an assistant district attorney due to sexual harassment by the defendant, and she claimed the defendant defamed her by telling others she was fired for having a relationship with a married member of the defense bar (which she admitted to, but contended was a falsely given reason for termination).

In arguing against dismissal, the plaintiff claimed these texts were not relevant because the defendant did not read them until after he decided to fire her. He admitted as much, but claimed his decision came after the affair partner's spouse told him about the texts and the alleged affair.

In her affidavit, the plaintiff said she no longer had the phone or the SIM card because her insurer required her to turn in both. The texts were not available from the phone service provider.

The court determined the plaintiff had a duty to take reasonable steps to preserve the evidence, as the plaintiff had threatened litigation almost a year before this incident. However, the court found the plaintiff acted without the requisite intent and so denied the motion to dismiss. It did allow the defendant to call as witnesses anyone who had read the destroyed text messages. The court denounced the lack of reasonable steps taken by the plaintiff and explained that when litigation is anticipated, "steps should be taken to preserve that material, such as printing out the texts, making an electronic copy of such texts, cloning the phone, or even taking possession of the phone and instructing the client to simply get another one."

In considering the defendant's motion for dismissal, North Carolina District Judge Max O. Cogburn Jr. stated that "[u]nder recently revised Rule 37(e), the duty of a party to preserve ESI arises when litigation is 'reasonably anticipated' and the loss of ESI is sanctionable when 'reasonable steps to preserve' are not taken and such information cannot be restored or replaced through additional discovery." However, he also noted that the "sanction of dismissal is not, however, a sanction of first resort" with Rule 37(e)(1) and Rule 37(e)(2), allowing the court "to take action no greater than necessary to cure the prejudice resulting from the loss" and that "Rule 37(e)(2) allows treatment of loss under spoliation only where party acted with an intent to deprive."

INFORMATION PRIVACY

LinkedIn Blocked in Russia

Professional networking site LinkedIn will be blocked in Russia after a court ruled it had breached the country's data protection rules. The ruling is part of a push by Russia to gain greater control over its Internet users, the *New York Times* reported. From China's blocking of entire portions of the Internet to Europe's efforts to regulate what can be viewed online, governments worldwide are attempting to dictate how citizens use digital services.

But Russia is a rare occasion of LinkedIn being blocked in a country, according to the *Times*. Russia imposed the ban after lawmakers passed rules requiring any personal digital data on Russian citizens collected by companies to be stored the country. Russian officials said the rules were meant to protect online privacy from hackers, but critics say the law could allow Russia to force companies to turn over sensitive data.

Many tech firms, including Facebook and Twitter, do not store data within Russia, but Roskomnadzor, the country's telecom watchdog agency, has targeted LinkedIn for failing to comply with the new rules. Some analysts think Russia is using LinkedIn as an example.

The Moscow court ruling, which upheld a previous decision against LinkedIn, means the company is blocked from operating across Russia. LinkedIn, which counts five million Russian users, could appeal. A spokesperson said the company is interested in meeting with Roskomnadzor.

Other social media firms have had difficulties in Russia as well. Facebook last year rejected all five requests from that government for access to data, the *Times* reported.

FOIA

NARA Announces New FOIA Ombudsman

Alina Semo, the U.S. National Archives and Records Administration's (NARA) director of litigation in the Office of General Counsel, has been tapped as the new director of the Office of Government Information Services (OGIS), which oversees Freedom of Information Act (FOIA) activities across government.

OGIS was created under the OPEN Government Act of 2007 to serve as an ombudsman between FOIA requesters and federal agencies. The OGIS director's responsibilities include leading the FOIA Advisory Committee, reviewing and providing policy guidance for agencies, ensuring open government law compliance, and mediating disputes between requesters and agencies, according to FCW.com.

Additionally, the OGIS director is authorized to issue advisory opinions in the event of an unresolved dispute and collaborates with Congress and the president to improve FOIA implementation.

FCW.com said Semo brings 25 years of federal litigation experience to the role. As NARA's director of litigation, she provided legal advice to agencies, helped revise NARA's FOIA regulations, and worked with the FOIA Advisory Committee. Before joining NARA, Semo worked as chief of the FOIA Litigation Unit for the Federal Bureau of Investigation's general counsel, where she helped establish litigation tracking systems and streamline legal and clerical processes.

She also spent eight years as a trial attorney in the Federal Programs Branch of the Department of Justice's Civil Division.

"Ms. Semo is a dedicated public servant who is uniquely qualified for this position," National Archivist David Ferriero said in a statement. "Her extensive experience with FOIA at both the administrative stage and in federal court litigation, knowledge of National Archives and commitment to open government will serve her well in her position as director of OGIS."

Previous director James Holzer resigned in May 2016.

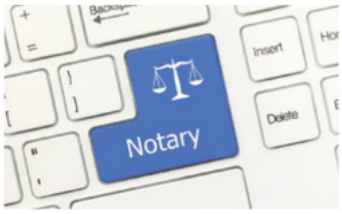
ELECTRONIC RECORDS

E-Notarization Gaining Popularity, Whitepaper Finds

As e-notarization processes have become more secure, two types are gaining traction. In-person e-notarizations call for a signer and notary to sign electronically on a computer or mobile device. Remote notarization allows the notary to verify signers' identities through a video conference, meaning the two parties don't need to be together in the same place.

Currently, remote notarizations are legal only in Montana and Virginia. Montana e-notarizations require both notaries and signers to be based in Montana, but Virginia's policy allows Virginia notaries to issue remote e-notarizations for signers in other states, according to Legaltech News.

By removing the need to meet in person, notarization becomes a less expensive, simpler process, proponents say. But critics question the security of webcam notarizations.



Pem Guerry, executive vice president of e-signature company SIGNiX, told Legaltech News that while there are some risks, there are big advantages to remote notarizations, especially concerning form security.

"You've captured the video of the notarization, so if there was fraud, it's caught on camera. It's a tremendous deterrent to fraud because you're captured on camera if you're attempting to commit fraud," he said.

Guerry said the digital record enhances security of any notarization process. E-notarizations produce tamper-evident records – any document signed and notarized cannot be altered without a digital record of the alteration.

While most states have adopted the Uniform Electronic Transactions Act allowing for electronic transactions, signatures, and notarizations, Illinois, New York, and Washington are holding out, meaning that e-notarizations aren't allowed in those states. Other states have put regulations in place for e-notarizations.

According to Legaltech News, courts and law enforcement are beginning to adopt e-notarization. But the biggest beneficiary is expected to be the mortgage banking industry.