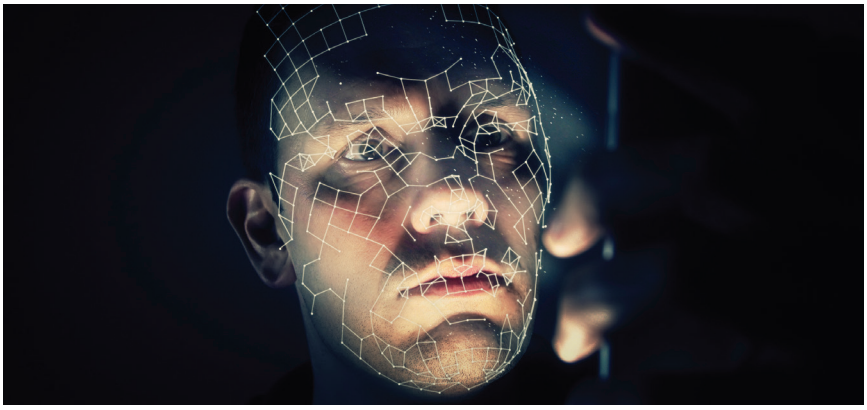
Information Management

BIOMETRICS

Facial Recognition Links 28 U.S. Reps With 28 Mug Shots



Yahoo.com writer Rob Pegoraro believes an ACLU study provided reason for everyone to think carefully about the evolution of facial recognition technology. In the study, the ACLU used Amazon's Rekognition service to compare portraits of members of Congress to 25,000 arrest mugshots. The result: 28 members were mistakenly matched with 28 suspects.

Recently, Microsoft's president, Brad Smith, used the company's blog to ask that the development of facial recognition systems not be left up to tech companies.

Smith wrote that the technology "raises issues that go to the heart of fundamental human rights protections like privacy and freedom of expression." According to the Yahoo article, he called for "a government initiative to regulate the proper use of facial recognition technology, informed first by a bipartisan and expert commission."

But author Pegoraro warns we may not get new laws anytime soon. He writes: "The nuances are complex, while Congress remains as reluctant as ever to regulate privacy. We may find ourselves stuck struggling to agree on norms well after the technology has redefined everything from policing to marketing."

The proliferation of connected cameras and databases for such images has made the technology nearly unavoidable and have put its powers beyond the control of consumers. The author cites a Georgetown Law Center study from 2016 that found that 26 states had opened such databases to police searches.

"The problem is you can't assume to know when a camera and its software identify you, that their recognition algorithms are accurate or that the underlying databases are always secure," Pegoraro writes.

He asserts that facial recognition is often done clandestinely. "Its accuracy is iffy, especially among non-white populations. Some 39% of the false matches in the ACLU test involved legislators of color, who only account for 20% of Congress. What's more, companies can't seem to stop data breaches from happening," Pegoraro writes.

In his blog post, Smith said such conditions often lead to government intervention. Pegoraro suggests the technology should not be used to put names to random faces "passing by."

E-MAIL SECURITY

Senator Asks DHS for Updates on E-mail Security Measure

Sen. Ron Wyden, D-Ore., has asked the Department of Homeland Security (DHS) how it is turning the implementation of an important e-mail security protocol at federal civilian agencies into "actionable cyber intelligence" to guard against hackers.

In an August letter, Wyden asked the department how it is analyzing reports that civilian agencies are required to notify DHS about attempts by hackers and spammers to spoof federal e-mail accounts. He also inquired whether there are agencies that aren't sending those reports.

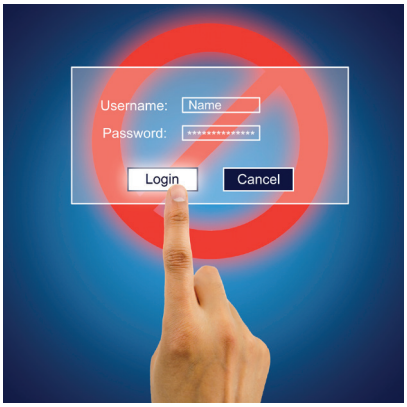
The protocol at issue, Domain-based Message, Authentication, Reporting and Conformance (DMARC), is an anti-phishing mechanism that requires a public record for checking if a sender is authorized to transmit on behalf of that domain. Industry experts consider DMARC to be effective in neutralizing the wave of phishing attempts that plague the federal government daily.

Agencies were given until mid-January to adopt the minimum level of DMARC, according to an article on *Cyberscoop.com,* and they have an October deadline to implement top-level DMARC, which blocks spoofed messages from being sent.

The policy also requires agencies to send the DHS reports on any fraudulent e-mails. Such reporting, according to Wyden, gives the DHS "an unparalleled, government-wide perspective on efforts by malicious actors to impersonate federal agencies."

EMPLOYEE RIGHTS

Law Would Block Feds' Personal E-mail and Social Media Access



According to *NextGov.com*, the House Oversight Committee recently advanced a bill that would give federal agency leaders broad authority to block employee access to personal e-mail accounts and social media without consulting their unions.

The goal of H.R. 5300 is to permit agency leaders to act quickly to counter cyber threats that come from web-based e-mail and social media, both of which are common vectors for phishing attacks, said the bill's sponsor, Rep. Gary Palmer, R-Ala.

Committee Democrats argued that Palmer and other committee Republicans were using cybersecurity as an excuse to restrict employee rights and dim the power of federal unions. The American Federation of Government Employees released a statement saying the bill "does not increase federal IT security," and asserted it would strip from employees their right to collective bargaining when it comes to IT matters.

Similar legislation passed the House in 2016 but did not reach the Senate floor.

According to Palmer, "Federal agencies have a responsibility to protect IT systems and they should be able to carry out that responsibility without unnecessary hindrance."

In response, Democrats said the bill would grant agency leaders too much power to decide which websites employees can visit. Further, the erosion in collective bargaining rights would make federal jobs less attractive.

H.R. 5300 would also make it tougher for federal employees' families to contact them in emergencies or for other family matters, according to Rep. Gerry Connolly, D-Va., the ranking Democrat on the committee's government operations panel.

PRESERVATION

E-Mail Preservation Bill Clears House

Four years after it was introduced, a bill to require agencies and the White House to modernize their systems for preserving e-mail records cleared the House recently by voice vote.

Managed on the floor by Rep. Mark Walker, R-N.C., the Electronic Message Preservation Act (H.R. 1376) was long championed by Rep. Elijah Cummings, D-Md., ranking member of the Oversight and Government Reform Committee. "This legislation would provide accountability to encourage every president to have the controls in place that are necessary to preserve emails and other electronic records," he said on the floor.

As summarized on *GovExec.com*, the bill would not only require tightened procedures for preserving electronic messages, it would also require new systems to make them easily retrievable through search engines.

Cummings, citing an October 2017 report from the National Archives and Records Administration (NARA), said 46% of federal agencies continue to print and file paper copies of e-mail messages.

According to the article, Cummings further noted that NARA has hailed the greater use of electronic storage for "long-term cost savings, information security, and more efficient and effective implementation of the Freedom of Information Act."

The bill would codify existing NARA guidance and require the U.S. archivist to establish standards for the preservation and management of e-mail records that are presidential records and to certify annually that the White House has parallel records management controls in place.

Similar legislation passed the House in 2014 but stalled in the Senate. Cummings has expressed optimism because the bill is considered noncontroversial.

CONSUMER PRIVACY

New California Privacy Act Could Be a 'De Facto' National Law

California's new Consumer Privacy Act of 2018 is likely to be treated as a *de facto* nationwide requirement, says information privacy expert Susan Goodman, a member of ARMA's Board of Directors. That is largely because the law, passed on June 28, will apply to more than a half-million U.S. organizations that do business with California residents, most of them small or medium-sized ones, according to analysis done by the International Association of Privacy Professionals.

Goodman, the CEO of Infoflo Consulting LLC, says the new act, among other things:

- Requires organizations to disclose the type of data they collect and – upon request – with whom that data is shared
- Requires organizations to disclose to consumers their right to delete their personal data and to delete that data (with certain exceptions)
- Allows consumers to opt out of having their data sold or distributed
- Prohibits companies from treating consumers who opt out differently than those who don't

"This law goes a long way toward operationalizing the Fair Information Practice Principles, which have been broadly adopted worldwide – especially the principles of transparency, individual participation, purpose specification, use limitation, security, and accountability," Goodman says; and she notes that it also is in keeping with several of ARMA International's Generally Accepted Recordkeeping Principles®.

"Many businesses have professed concern for their customers' privacy while placing obstacles in the way of privacy protection," she says. "This law addresses and prohibits many of these obstacles."

Goodman says the framers of the California law clearly understood that many privacy principles and restrictions have been circumvented. For example, many organizations found ways to not technically "sell" consumers' personal information without their consent by instead "distributing" that information for free along with another product or service for which they received payment. Given the specificity of requirements in this law, she predicts it will be much harder to continue these practices.

"Compliance with this law is going to require a significant expenditure of resources by most U.S. organizations for which the law applies," she states. "They will need to upgrade their privacy and information security programs, systems, policies, and procedures." After all, Goodman says, even if California residents constitute only a small percentage of their customers, it's typically more resource-intensive to upgrade practices for just a segment of a customer base than to apply overarching practices to all customers.

Recognizing the probability of this new law being considered a *de facto* U.S. federal requirement for many organizations, the fact that there is great concern by the public, legislators, and courts about privacy and information security, and the reality that having solid privacy and information security programs is good business practice, even those organizations for whom the law may not be applicable would be smart to work toward compliance.

Take Our Latest One-Minute *IM* Poll

In this issue's cover article, "Out of the Box: Why Organizations Are Jumping to Office 365/SharePoint Online," Mark Grysiuk, CRM, CIP, provides an overview of out-of-the-box Office 365/SharePoint Online functionality and what organizations can and should do with it. We'd like to know whether your organization has moved to Office 365 or similar products/services. Please visit our latest poll at ***http://imm.explorearma.org/O365*** to let us know and see what others are using.

Read the article that prompted this survey on page 20.

Respondents to the July/August IM poll shared where they are in their efforts to clean up the redundant, outdated, and trivial information (ROT) from their shared drives:

- We are planning the process of cleaning up ROT on our shared drives. (41%)
- We are in the process of cleaning up ROT on our shared drives. (32%)
- We have no plans to clean up ROT on our shared drives. (16%)

Take or see results for previous polls at ***http://imm.explorearma.org/RIM_Polls.***

Don't Find Yourself Guilty of Costly Scanning Practices in Your Law Firm

In today's legal environment, the advantages of having paper documents in electronic format are tremendous. Once the paper documents are converted into digital data, case files are readily available. Employees no longer have to waste time searching for them. For law firms that specialize in collections, digitizing documents upon receipt allows for faster and safer processing.

The number of paper documents produced and gathered during discovery can be overwhelming and the resulting case files even more so. These important records can include anything from statements, spreadsheets, technical drawings, images and even hand written notes. They can span every facet of the legal process from client interviews to final case appeals.

You may have thought about ways to make your law office paperless with the intention to keep your practice as efficient as possible. The truth is, digitizing your case files can set your law firm free. That is, free from excessive labor costs during discovery and freeing up space currently housing bulky filing cabinets and stacks of boxes crammed with documents.

Does digitizing documents in your office look a crime scene?

We recently encountered this crime scene in a law firm scanning operation. You may relate:

Exhibit A:

- The 8-hour shift began with eight well-paid paraprofessionals sitting on the floor amidst a pile of nearly 3500 envelopes. Each morning, they pre-sorted this incoming mail into two piles: those opened pieces containing payments and those sealed envelopes whose contents are unknown.
- Unopened mail was opened with a high-speed envelope opener.
- And then the labor began. Documents were sorted into 15 categories – each assigned a sort bin along the wallsuch as garnishments, claims, judgments, affidavits and payments.
- These grouped documents were then scanned in order of priority. Employees transported the documents to their workstations to commence the task of imaging on desktop scanners.
- Once all the payments were collected, four people were tasked with a separate job of processing these payments on check scanners, manually verifying and validating each check along the way.

The Smoking Gun

The facts above clearly show:

- The security and integrity of each transaction were placed in jeopardy. The labor-intensive sort processes required employees to handle documents and payments as many as five times before they were finally digitized
- Excessive costs, long turn-around times and wasted resources abounded. Due to the mount of time spent preparing documents and payments for scanning; lower priority documents weren't being scanned the same day. This created carry over and backlogs for the rest of the week.

How do you plead?

Is your legal scanning operation fraught with excessive cost, wasted resources, and potential breaches in security and integrity of your incoming mail? Do you identify with the above-described Exhibit A? Have you been looking for a solution to streamline your document scanning and electronic content management?

There is a better way to rest your case.

Fortunately for you and the law firm referenced above, there is a better way to manage your incoming documents and mail. The solution will save you time, money, resources and allow you and your team to focus on what you do best. If you would like to learn more about how an OPEX digital mailroom solution can help you rest your case(s) more quickly, easily and with substantial labor savings, give us a call or stop by opex.com and request more information. We are here to help.

For more information visit www.opex.com

OPEX® CORPORATION

DATA TRACKING

The Way You Swipe Your Phone Can Be Used To Track You

CNET.com reminds us that we've been warned about apps that track our behavior or store our private information, but writer Claire Reilly asks, "What if your smartphone screen is betraying you?"

Research suggests that the way you swipe, pinch, and tap your smartphone screen could be used to track your identity and perhaps breach your privacy.

The research, from an Australian team, was presented this summer at the Privacy Enhancing Technologies Symposium in Barcelona. Among the discoveries was that touch gestures contain sufficient information to

uniquely identify and track users.

The team had built an Android app called Touch-Track, which gathered gestures from 89 users, and soon determined that if users are writing on a touchpad, their handwriting would reveal 73.7% of the information needed to identify them.

The team warns that this "touch-based tracking" can be used to continuously track users, both on a single smartphone and across multiple devices.

"While regular tracking tracks virtual identities such as online profiles, touch-based tracking has the potential to track and identify the actual (physical) person operating the device," the researchers wrote. "It can distinguish and track multiple users accessing the same device."

RETENTION

Pittsburgh Is Pennsylvania's Only City Without Retention Policy

According to *PublicSource.com,* in Pennsylvania the Right-to-Know Law gives citizens and journalists the power to request information from every level of government. But if you do file a request, there's no guarantee you'll get what you're after.

Article writer J. Dale Shoemaker poses this question: "Suppose your favorite parking spot was replaced by a bike lane—and now you must park around the block to make room for the cyclists' right-of-way. As a resident, you may wonder how much the city of Pittsburgh paid to have that bike lane installed and how it came about. Is that information available to you?"

His answer? "Generally . . . yes." That's because the Right-to-Know Law is based on the assumption that all government business is public information. But if you file a Right-to-Know request for that bike lane spending data, there's no guarantee you'll get what you're after.

Shoemakes writes that Pittsburgh hired a city archivist, Nicholas Hartley, who is combing through old records in an effort to make them more accessible. Hartley says Pittsburgh doesn't keep track of its records because it was no one's job to do so.

"Frankly ... there's never been anyone in place to think about it," he says. "The city is busy putting out fires, protecting the community and there's been no one in place who's specifically charged with records management."

Further, the Right-to-Know Law doesn't specify the documents that government agencies must keep track of. Shoemaker asserts that a record retention policy could solve many of Pittsburgh's related problems. It would outline how long the city must keep records, the format in which those records are stored, and possibly whether those records are confidential.

Howard Pollman, an official with the Pennsylvania Historical and Museum Commission (PHMC), which sets uniform retention policies for smaller cities in the state, draws a distinction between having a records management policy and managing records.

> "Frankly ... there's never been anyone in place to think about it…"

"Managing records and [having] a retention schedule are not the same thing, but having a schedule makes managing records easier," he wrote in an e-mail. He added that from the PHMC's point of view, it is good that Pittsburgh is working on creating a record retention policy.

DATA LEGISLATION

Ohio Law Encourages Cybersecurity in the Private Sector

As reported on *DataGuidance.com,* Ohio passed a Senate bill in August that provides a legal safe harbor to entities that voluntarily implement a specified cybersecurity program to protect customer information. The new legislation gives covered organizations a legal defense to any claims that it failed to implement reasonable information security controls in case of a data breach.

Gregory J. Krabacher, a partner at Bricker & Eckler LLP, told *Data Guidance* the act "takes a thoughtful, narrow approach to encouraging the private sector to maintain reasonable cybersecurity."

According to Krabacher, the law is flexible because organizations have many security frameworks to choose from; and it is narrow because it doesn't try to solve the "entirety of the cybersecurity problem" and neither does it impact existing breach notification laws in Ohio.

Covered organizations that seek an affirmative defense must create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information and that reasonably conforms to an industry-recognized cybersecurity framework. The law identifies 10 such frameworks, including the ISO 27000 standards and those published by the National Institute of Standards and Technology.

The law defines data in two ways. One way refers to the state's existing definition of personal data; the second way refers to "restricted information," which means any data about an individual that alone or in combination with other data can be used to distinguish that person's identity or which is directly or indirectly linked to an individual. According to the language of the law, if an organization reasonably protects personal information, then it can assert the affirmative defense to claims involving personal information. If the organization reasonably protects personal information and restricted information, it can raise the affirmative defense to claims involving both forms of data.

PIPEDA

OPC Says Re-use of Social Media Data Violates PIPEDA

Recently, Canada's Office of the Privacy Commissioner (OPC) found that a New Zealand company had violated a Canadian law by re-purposing and making public some personal information concerning 4.5 million Canadians it had gleaned from Facebook.

The company, Profile Technology Ltd, is accused of violating Canada's Personal Information Protection and Electronic Documents Act 2000 (PIPEDA) for having repurposed private information without the consumers' knowledge or consent. The data in question apparently surfaced on The Profile Engine, a site operated by the company in question. Additionally, the company is accused of having failed to confirm whether any of the individuals' Facebook privacy settings had changed or if any of the data had been removed by them. Such neglect can result in unlawful indefinite retention of personal data.

During the investigation, Profile Technology claimed the data was publicly available and therefore didn't require consumers' consent. The OPC found differently, saying "PIPEDA recognises that not all information in the public domain will be considered 'publicly available' [and] that information that may be in the public domain is still worthy of privacy protection."

The OPC forwarded its findings to the Office of the Privacy Commissioner of New Zealand, which had expressed interest in the issue.

CLOUD COMPUTING

Is the Cloud Going Away? The Term Itself May Be in Jeopardy

Andrew Ross writes on *Information-Age.com* that the concept of the cloud is now so deeply embedded in the business world that the word itself may soon go away.

He cites a Citrix study of 750 IT decision makers across the UK, in which roughly one-quarter of respondents believe they "won't be talking about 'cloud' by the end of 2025." More than half (56%) think that cloud technology will be so embedded that it will no longer be viewed as a separate term.

In a separate Citrix survey, this one polling 1,000 adolescents, 30% of the young teens did not know what the term "cloud" even meant, and 42% said they used it to share things like photos and music.

Research conducted by Citrix suggests that roughly 6 in 10 UK businesses continue to manage their data on premises, while nearly 4 in 10 large businesses store more than half of their data in the cloud. About 9 in

10 UK businesses have implemented a cloud strategy or plan to put one in place. The study further shows that 31% of participants are not confident that a public cloud can handle their organization's data security.

A director at Citrix, Darren Fields, says that like BYOD, the cloud as a term may soon be relegated to the buzzword graveyard. "This has nothing to do with its relevance in the IT industry but everything to do with the evolution of technology and the ubiquity of cloud services to underpin future ways of working."

"DATA DUMPING"

E-Discovery, Data Dumps, and the Absence of Ethics

On *NationalLawReview.com,* Jaliz Maldonado writes that many otherwise ethical attorneys are increasingly tempted to smother opposing counsel with "an enormous amount of electronic data during e-discovery."

She defines data dumping as "when a party decides to over-provide information, whether it was requested or not, in an attempt to hide the needle of relevant information in a haystack of electronic documents." It becomes difficult, time-consuming, and costly to sift through the avalanche of information in search of what's relevant.

She cites *SEC v. Collins & Aikman Corp.* (S.D.N.Y. 2009), in which the U.S. Securities and Exchange Commission (SEC) dumped more than 10 million pages on the opponent's attorneys. In response, a disgruntled Judge Scheindlin wrote that Rule 34 of the Federal Rules of Civil Procedure prohibits "simply dumping large quantities of unrequested materials onto the discovering party along with the items actually sought."

In response to an SEC claim that opposing counsel could merely review the e-documents, Scheindlin wrote the following: "A page-by-page manual review of ten million pages of records is strikingly expensive in both monetary and human terms and constitutes 'undue hardship' by any definition."

Nonetheless, according to the article, many believe data dumping continues – and at an alarming rate. "Rules and expectations regarding this frontier seem not to be quite set at this time," writes Maldonado.

Ben Sexton, a writer for *Legal Tech News*, suggests using referees to help parties stick to their ethical values in these instances. To decrease such unethical temptations, Sexton suggests the attorneys learn how to ask for what they want; find an e-discovery technology expert you can trust, and seek his or her guidance often; use technology to create transparency; and be mindful of the opportunities for opposing counsel to skirt the rules.

Take Your Career to the Next Level

Master of Archives and Records Administration

Convenient, flexible, 100% online graduate program

Built on the competencies required to become a certified archivist and a certified records manager, the Master of Archives and Records Administration online degree program at San José State University uniquely combines archival science, records management and information governance into one comprehensive master's degree.

In this flexible 100% online program, you'll study the entire information lifecycle and prepare for a wide range of professional positions. And through a partnership with the Institute of Certified Records Managers, you can apply MARA courses for credit toward the ICRM examinations.

> *"The SJSU MARA program assisted me in advancing my career. It was an extremely flexible program that allowed me to complete a degree while I was working. I would recommend it to anyone in the records management field."*
>
> *Robert McLauchlin, '11 MARA*
> *Director of Records Management · Burnett, Duckworth & Palmer LLP Law Firm*

10TH MARA ANNIVERSARY

Master of Archives and Records Administration

Celebrating 10 Years!

Want to learn more?

Visit us at ARMA Live! in Booth #412
and join us for breakfast at nFuse Restaurant
in the Anaheim Convention Center Marriott
on Monday, October 22 (7:30 – 9 a.m.)

100% Online · Scholarships Available · Self-Paced Program

Now accepting applications for admission!

ischool.sjsu.edu/mara

SJSU SAN JOSÉ STATE UNIVERSITY

PRIVACY

New Privacy Rules in PIPEDA Could Surprise Unprepared Organizations

ITWorldCanada.com reports that new regulations in Canada's Personal Information Protection and Electronics Documents Act (PIPEDA) could cause problems for organizations that are not prepared for their November 1 effective date.

Cindy Baker writes that the new regulations define the requirements for mandatory breach reporting for Canada's private sector, and she implies that these requirements are not "on the radar for most Canadian organizations."

Research conducted by Canada's privacy commissioner suggests that only 40% of Canadian organizations have procedures to comply with the new rules. Violations could result in fines of up to $100,000.

The new language requires organizations to report a security breach if it might pose a "real risk of significant harm," such as identity theft or damage to relationships or reputations. The reports, according to the article, must be sent to the individuals, the privacy commissioner, and any third-parties that could help reduce the potential for harm.

PIPEDA also requires organizations to keep records for two years on all security breaches involving personal information. This stipulation, according to the article, will prove troublesome for many organizations.

Baker writes that the best way to prepare is to "work with a solutions provider to bring all of the organization's content into one place for tracking, search and retrieval."

A compliance expert, Sylvia Kingsmill, says organizations should look into automation to track everything. "It is an evergreen exercise to continuously update the information, which would be very arduous to do manually," she tells *Forbes*.

CYBERSECURITY

Director of Non-Profit Alliance Suggests 'Shared Responsibility' for Internet Security

Byron V. Acohido, of *The Last Watchdog*, recently spoke with Russ Schrader, new executive director of the National Cyber Security Alliance (NCSA), about the evolving state of online security. The NCSA is a non-profit entity underwritten by the top tech companies and biggest banks. It operates *StaySafeOnline*, a website providing educational resources on cybersecurity.

In light of the recent headlines and the election year in America, Director Schrader said a current focus of the agency is to "work with people on the Hill, and try to help them during this election time, or when there may be unfriendly actors trying to hack into their e-mails or hijack their social media accounts."

Regarding the private sector, Schrader is concerned that too many smaller companies might not be investing adequately in cybersecurity, which presents a risk up and down the chain. "A large retailer may spend millions on cybersecurity. But their contractors may not be spending that kind of money, and simply do not have that expertise," he said. "So we've boiled the NIST framework down into a very focused workshop exercise."

He further stressed that everyone has a shared responsibility in preserving online security: "Everyone who works at a company is also a consumer. We are all always using our connected devices, no matter where you are, no matter what you're doing. We bring our devices home and use them in our personal lives. We're all continually exposed to cyber threats. So security has become a shared responsibility."

Schrader advocates a "digital spring cleaning" to help ensure security. "Chances are your phone and your laptop have apps that you haven't touched in a year," he said. "Well, get rid of them; clean up that space. Find out what information they've been collecting from you, quietly in the background. And get rid of them. . . . Simple steps will make your device cleaner, faster and open up storage space. And it will also help prevent possible malware infections."

DISPOSITION

The Sedona Conference® Publishes on Defensible Disposition

In August, as reported by *JDSupra.com*, The Sedona Conference® and its Working Group 1 on Electronic Document Retention & Production (WG1) published its public comment version of *The Sedona Conference Principles and Commentary on Defensible Disposition*.

The update is in response to the group's perception of a need to provide more guidance to organizations and counsel on "the adequate and proper disposition of information that is no longer subject to a legal hold and has exceeded the applicable legal, regulatory, and business retention requirements," according to the site.

The article suggests that many organizations struggle with executing effective disposition because, among other reasons, they fear they'll be forced to defend their actions if litigation later occurs.

The commentary offers these three principles to aid organizations and their counsel in making proper disposition decisions:

1. Absent a legal retention or preservation obligation, organizations may dispose of their information.
2. When designing and implementing an information disposition program, organizations should identify and manage the risks of over-retention.
3. Disposition should be based on Information Governance policies that reflect and harmonize with an organization's information, technological capabilities, and objectives.

Each principle includes "comments" that provide additional guidance.

The new content is open for public comment through October 10. Questions and comments may be sent to *comments@sedonaconference.org*. You can download a free copy by visiting this site: *https://tinyurl.com/yahgzt7a*.

INTEGRITY

'Data Veracity' Is Seen as Challenge Organizations Must Confront

The value of data can scarcely be understated. According to an opinion piece on *Information-Management.com*, 82% of business leaders say their organizations are increasingly using data to drive critical and automated decision-making at scale.

In his article, Pat Sullivan suggests the data explosion will continue apace because businesses will "continue to adopt data-reliant technologies such as artificial intelligence, blockchain, augmented/virtual reality and robotics, to name just a few."

Accompanying all of this, Sullivan says, will be increases in the damage that comes from inaccurate or manipulated data: "Incorrect or falsified data threatens to compromise the insights that companies rely on to plan, operate, and grow."

A study sponsored by the tech firm Oracle suggests that 79% of the executives in its survey agreed that many organizations are not giving enough attention to data integrity.

Writes Sullivan: "If we're to fully harness data for the full benefit to businesses and society, then this challenge needs to be addressed head on."

He introduces his idea of the three tenets of data veracity: 1) provenance, or verifying its history; 2) context, or considering the circumstances around its use; and 3) integrity, or securing and maintaining the data.

Sullivan urges organizations to address these three tenets by way of a combined data intelligence group that would ensure the right data is used to support systems and processes, embed data integrity and security, analyze data to recognize when its findings don't synch with existing knowledge, and more.

"Without these efforts," he concludes, "securing the trust of consumers will become increasingly difficult and the huge benefits that data analytics at scale promises our communities may not be fully realized. All organizations should therefore act now and implement specialized technologies, processes and teams for robust data governance."

PRESERVATION

Library Council Report Examines Complexity of Preservation

A report from the Council on Library and Information Resources (CLIR) discusses what makes e-mail archiving so complex and describes emerging strategies to address the archiving challenge, as reported on the CLIR site, by Kathlin Smith.

"The Future of Email Archives" presents the findings of a yearlong investigation of a task force funded by the Andrew W. Mellon Foundation and the Digital Preservation Coalition.

According to the report, 215 billion messages are sent and received for personal and business communication on an average day. These messages are documentation of personal and public stories, but few archives have policies for systematically capturing, preserving, and providing access to them.

Complexity is part of the problem, the report suggests: "Email is not one thing, but a complicated interaction of the technical subsystems for composition, transport, viewing and storage."

Task-group Co-Chair Christopher Prom believes that the complexity should not dissuade efforts to properly manage e-mail. "Archives can and should do everything they can to capture and preserve email, if we want to assemble a historical record that future generations can interrogate and use," he says.

The report summarizes five institutions that have created preservation workflows, but they are the rare exceptions.

"Just as the protocols that define the email environment are heavily standardized to facilitate interoperability across the diverse landscape of email, so too must the tools to preserve email be able to interact with one another across the lifecycle," the report says. Smith notes that addressing the challenges "will require commitment and engagement from a wide variety of stakeholders."

Print and online versions of the CLIR report are available at *https://www.clir.org/pubs/reports/pub175.*

VITAL RECORDS

CISS Offers Guidance for Conquering 'Data Sprawl'

Gene Fredriksen, chief information security strategist for PSCU, a credit union service organization, writes on *Forbes.com* that reducing data sprawl and identifying your organization's vital information are tough but feasible objectives.

The process, he says, "will take considerable time, energy and coordination across the business. It requires knowledge and a good understanding of data locations, data ownership and data flows both inside and outside of the company, regardless of whether it involves regulated or compliance-related information."

Fredriksen spells out the steps for creating a process to identify your vital cyber assets.

First, he says to formulate ground rules. "Being systematic minimizes the chance that data will be left undiscovered and thus unprotected. Being continuous reduces the likelihood of gaps occurring that could

devolve into an unmanaged state," he writes.

The risk of not establishing these ground rules early, he posits, is that groups in your company will improperly determine what is valuable. The legal department or information managers can provide retention and protection guidance. According to Fredriksen, "Establishing strict data retention requirements with automatic document deletion early on will greatly reduce classification efforts and the amount of exposure for the company."

Second, organizations should assign "point people" who will own data so that it doesn't get lost when it enters a file share or repository. These owners will create the business policies around the data and determine who can access it.

Third, the author recommends mapping how the data flows in your organization. Such a step will help track any data transformations, changes in classification or status, and more.

"Mapping data flow also aids in identifying where data may be stored temporarily or permanently or where copies may be stored along the way, resulting in an increased risk of duplicate data and increased risk exposure," he writes.

Risk profiles can then be created after these other determinations have been made.

According to Fredriksen, information "has a limited useful life" and "once its useful life is over, it must be retired in a secure manner to prevent leakage to unauthorized sources."

Applying Emerging Technologies to Microfilm Solutions

James Westoby

Microfilm is an ancient document storage medium that is still relevant today. Microfilm has long been trusted as a low cost, reliable, and secure method of document storage across all sectors of the world's societies. And, now, with the proliferation of computer technology speeding our use of data, microfilm scanners have become a true partner in the advancing capabilities of the records management enterprise.

For several decades microfilm scanners have been an essential tool for retrieving and digitizing stored documents. Technological strides have enabled replacing yesterday's large, slow, and weighty machines with today's small, light, speedy, and efficient multi-purpose scanners. Today's microfilm scanners are also recognized as being environmentally friendly, both cutting back on paper waste and providing energy efficiency. Most leading scanners today are Energy Star certified.

Until recently, however, customers needed to purchase two pieces of equipment to accomplish the full range of scanner capability. One scanner was needed for **on-demand** reading, printing, and scanning and an additional scanner was needed for **conversion scanning** when converting microfilm to digital formats.

Conversion scanners are, generally, large, expensive, high-speed microfilm-to-digital conversion machines. Years of documents can be safely converted in just a few days, leading to greater business efficiency and eliminating the chance of lost or misplaced information.

Most **on-demand scanners** are smaller, lighter, less expensive microform (film, fiche, roll film, cartridge film, micro opaques, aperture cards, micro cards) devices. They allow the user to view-on-screen, print, and scan to other devices documents made efficiently available by a variety of on-board tools. The user can easily choose the desired image, alter it to obtain the best image quality for viewing, and print it or scan it for later use. On-demand scanning offers quick retrieval and sharing of documents.

With new and innovative technology emerging in the micrographics industry, the single device combination of a desktop on-demand scanner and a conversion scanner is now being introduced. This type of scanner is the only microfilm solution that combines the features and benefits of both an on-demand reader/printer/scanner with the capability to do high-speed conversion right at your desktop. The conversion of confidential and highly sensitive information now can be handled on-site by your own staff, at your convenience.

The opportunity to enjoy two scanners in one device is revolutionary and will not only greatly aid the users but will save on the budget and offer an excellent return on investment. Yes, Virginia, there is a Santa Claus!

For more information about on-demand, conversion scanners or the latest microfilm innovations, please visit *www.e-ImageData.com*.

SOCIAL MEDIA

Law.com Sheds Light on Suit Against Google for 'Location Snooping'

In a recent *Law.com* article, Ian Lopez writes that users should be aware of three things that relate to the lawsuit that alleges Google performs "location snooping."

"The bastion in big tech is being accused of big-brother like behavior, and the accusers are using the law to get the message across loud and clear," he writes.

The class-action complaint, filed in August in the U.S. District Court for the Northern District of California, says that Google's collection of location data "against the express wishes and expectations of its users" violates state privacy laws.

Lopez makes three points about the lawsuit that could inform the litigation.

First, the suit will make good use of the California privacy laws. "Consumer privacy is no laughing matter in California, widely regarded as leading the way in state privacy law," he states. The complaint says the tech titan is "acquiring and using the geolocation of mobile users, without their consent" and "in direct contravention of instructions clearly expressed through the turning off the location history function," and therefore is in direct violation of California's Invasion of Privacy Act (CIPA).

Second, Lopez cites the U.S. Supreme Court's recent decision in *Carpenter v. United States*, which holds that a search warrant is needed before obtaining an individual's historical cellphone location data. Though the ruling pertains to law enforcement, Lopez and others believe it opens the way for a wider array of protections.

Third, Lopez posits that the law firms (Lieff Cabraser Heimann & Bernstein and Carney Bates & Pulliam) that are filing suit have taken on big tech companies before, including Google. In 2015, the firms teamed to successfully stop Google from gleaning content within e-mail messages to profile its users. E

HIPAA

HHS Reminds Healthcare Entities to Follow Rules for Device Disposal

The *HIPAA Journal* summarizes a recent cybersecurity newsletter published by the Office for Civil Rights of the Department of Health and Human Services (HHS) that reminds HIPAA-covered organizations of the rules for disposing electronic devices and media.

The HIPAA rules are applicable to such electronic devices as desktop computers, laptops, servers, tablets, mobile phones, portable hard drives, zip drives, CDs, DVDs, and more. Additionally, organizations must also carefully dispose of their fax machines, photocopiers, and printers because they often store personal health data on internal hard drives.

Among the newsletter's guidelines for ensuring safe disposal are the following:

- Make sure the data disposal plan is up to date.
- Remove asset tags and corporate identifying marks.
- Identify and isolate all asset recovery-controlled equipment and devices, such as backup tapes and memory media.
- Ensure that all employees and vendors that handle the data destruction are certified.
- Understand your chain of custody for the devices.
- Consider performing initial hard-drive destruction onsite.
- Ensure safe handling and logistics of any equipment that will be disposed of and destroyed offsite.

The newsletter, together with information on secure disposal of physical health information, can be found at *https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-july-2018-Disposal.pdf*.