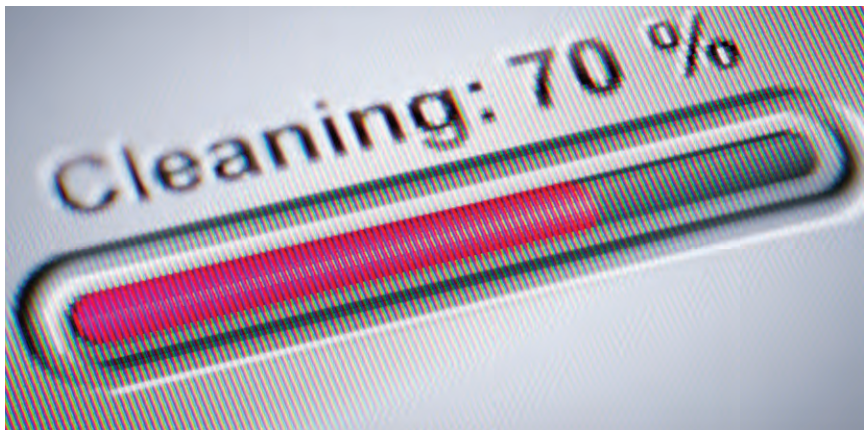
Information Management

RECORDS DESTRUCTION

Information Commissioner Says Town's Destruction of Records Was 'Careless' and 'Negligent'



The information commissioner of Newfoundland and Labrador has criticized the town council of Paradise for destroying records after someone sought them through freedom-of-information laws. In a report, Information Commissioner Donovan Molloy said the actions were "careless" and "grossly negligent."

One such request was for records from the 2017 municipal election. The council said it destroyed them in accordance with the Municipal Elections Act. Molloy said the council destroyed some records that weren't covered by that part of the law.

"While there is insufficient evidence to find that the town destroyed these records with the intent to evade the access request, the destruction was careless at best," Molloy asserted.

A second request was for video surveillance footage at an ice-skating rink. The town rejected the request based on "personal privacy reasons," even though no one checked the video to see if anyone was identifiable, according to a *CBCNews* article. In fact, the very footage had been erased weeks earlier because the system didn't have the capacity to store it for that long.

The commissioner urged the council to revise its policy on destroying election records, and to comply with its video surveillance policy by making sure there's proper storage capacity.

In response, the council said it is "in the process of reviewing its policies and procedures in light of the commissioner's recommendations and will take the steps necessary to ensure it continues to follow the Access to Information and Protection of Privacy Act."

AVAILABILITY

At HUD, Finding ESI Takes a Long Time

The U.S. Department of Housing and Urban Development (HUD) is required by law to respond to requests for documents within 20 business days. But an inspector general's evaluation found that HUD may struggle to meet the requirement because its e-discovery management system is just too slow.

According to a *FedScoop.com* article, HUD has a contract with Leidos Innovation Corporation for such e-discovery services. As set forth in the contract, the process works like this: A HUD customer submits a request for ESI. That request is approved by the general counsel e-discovery team and then passed on to the Leidos contractors for collection of the materials. But the system is struggling to meet demand.

"HUD customers are submitting more and larger requests for ESI than the contract was originally estimated to cover," the evaluation states.

Among its recommendations for relieving the slowdown, the report suggests moving ESI from its localized storage to the cloud, which would make it easier to find.

According to *FedScoop*, general counsel at HUD agreed with the report's recommendations.

PRIVACY

LegalWeek 2018: GDPR Makes the Proper Disposal of Data More Urgent

At the ARMA track at *Legalweek 2018*, a panel of IG professionals discussed how the General Data Protection Regulation (GDPR) is changing the game for data deletion, as reported on *Law.com*. "Making Disposition Defensible: The Tools You Need" included panelists Jason Stearns, director of the legal and compliance group at BlackRock (and an ARMA board member); John Isaza, partner at Rimon PC; and Richard Kessler, director of cybersecurity services and strategy at KPMG.

"I like to think that the whole game is changing," said Kessler, noting that the GDPR mandates that companies can only store the personally identifiable information (PII) of EU citizens for as long as it satisfies the primary business purposes for which it was collected. "For years we were focused [on data] at the end of its life cycle: What is preventing us from disposing of it? What is occurring now [with the GDPR] is changing the focus to the front of the life cycle . . . it really pushes the thoughts around disposition, in particular with the right to erasure, to the very beginning of the life cycle when data is first created or received."

Isaza said that among his clients, "personal data is, by far, their number one concern" because of the GDPR.

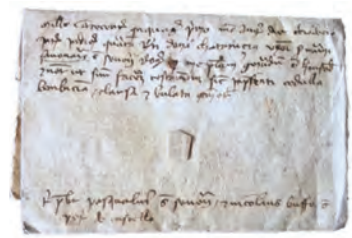
The panelists suggested the new regulation is already inspiring some IG consultants to encourage a more proactive approach to deleting data. Stearns, for example, said he instructs business groups to dispose of data that has PII unless they can justify its retention. "I can speak to deleting tens of thousands of backup tapes with that approach alone," he said.

According to Kessler, some companies will need to perform "micro-surgery" to find the PII throughout the enterprise. "Those doing the data analytics may say, 'Hey we want to keep this data around, we want to see trends over years' or something like that," Kessler said.

Under the GDPR, companies will likely need to get consent from EU citizens whose PII they want to keep. Stearns believes some companies will cite data analytics as a reason to retain such data. "Big data, artificial intelligence, analytics – these keep being reasons used to do nothing," he said.

INFO TECHNOLOGY

New Technology Reads Age-Old Documents Without Opening Them



Scientists in Switzerland say they have enhanced a method to read ancient documents without even touching them.

As reported by *LearningEnglish.voanews.com*, researchers at the Swiss Federal Institute of Technology are using radiation in the form of X-rays to create images of the documents. The method is called *X-ray computed tomography or X-ray tomography.*

Italian officials are planning to use X-ray tomography to build an open digital system in the State Archives of Venice, which will be beneficial because so many of the documents show signs of weathering and are easily broken.

Researcher Giorgio Margaritondo says, "What you find inside the Archives are not only small documents. But most of the items are huge volumes the size of a table, and so we must be able in the future to look inside them."

Fauzia Albertin, a member of the Institute, says, "We need a non-invasive technique to read inside them. Thanks to the use for thousands of years of iron-based inks we can read them using X-rays."

The State Archives of Venice has records that were produced over a period of about 1,000 years.

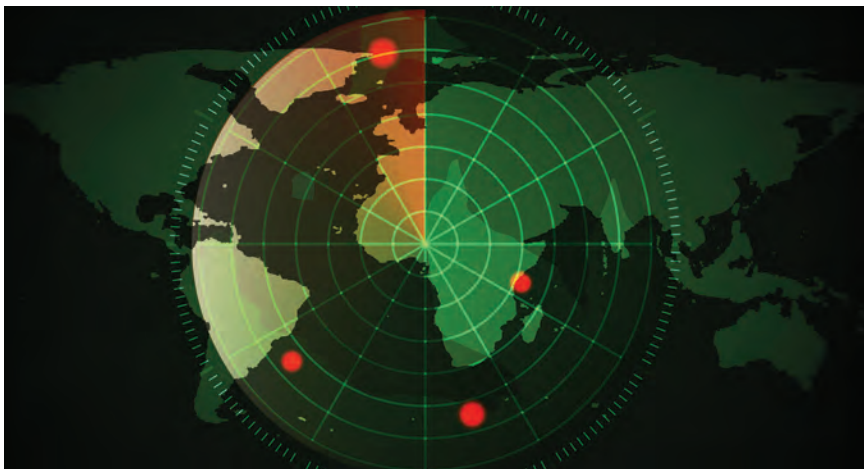
TRACKING

Fitness Tracking App Reveals Locations of Secret U.S. Army Bases

TheGuardian.com reports that sensitive information about the location and staffing of military bases and spy outposts around the world has been revealed by Strava, a fitness tracking company.

The company released the details in a data visualization map that shows all the activity tracked by users of its app, which lets people record their exercise and share it.

The map shows every activity ever uploaded to Strava – more than 3 trillion individual GPS data points. The app can be used on smartphones and fitness trackers like Fitbit to see popular running routes in major cities, or to spot individuals in more remote areas who have unusual exercise patterns.



Military analysts soon noticed that the map is also detailed enough to potentially give away extremely sensitive information about a subset of Strava users: military personnel on active service.

According to *The Guardian*, an analyst with the Institute for United Conflict Analysts first noted the lapse. The heatmap "looks very pretty" wrote Nathan Ruser, but is "not amazing for Op-Sec" – short for operational security. He said the U.S. bases were clearly identifiable.

"If soldiers use the app like normal people do, by turning it on tracking when they go to do exercise, it could be especially dangerous," Ruser added.

In locations like Afghanistan, Djibouti, and Syria, Strava users seem to be almost exclusively foreign military personnel, which means that those bases stand out brightly. In Helmand province, Afghanistan, for instance, the locations of forward operating bases can be seen glowing white against the black map.

The article illustrates how zooming in on a base clearly reveals its internal layout, as mapped by the tracked jogging routes of numerous soldiers. The base itself is not visible on the satellite views of commercial providers such as Google Maps or Apple's Maps, yet it can be clearly seen through Strava.

When Strava released the heatmap, it said "this update includes six times more data than before – in total 1 billion activities from all Strava data through September 2017. Our global heatmap is the largest, richest, and most beautiful dataset of its kind. It is a direct visualization of Strava's global network of athletes."

Take Our Latest One-Minute *IM* Poll

In her Fellows Forum article, Susan Goodman, IGP, CRM, CIP, CIPP, CIPM, FAI, makes the case for "Aligning Privacy with IM within the IG Framework." An effective information governance program (IG) requires collaboration not only between IM and privacy, but also among all IG stakeholder functions. Please visit our latest poll at ***http://imm.explorearma.org/IG_Collaborations*** to tell us with what IG functional areas your IM program collaborates.

Read the article on page 30 that prompted this survey.

The Jan./Feb. IM poll revealed that the top three limitations organizations (20) put around data are:

- The purpose for which data is collected (45%)
- Who may use the data (40%)
- The length of time the data will be retained (35%)

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

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

GOVERNMENT RECORDS

Former National Archivist Reflects on His Dynamic Tenure

The Hutchinson News recently reported on former Kansas Governor John Carlin's presentation to a Kiwanis Club in Lindsborg, Kan., during which he reminisced about his years as archivist of the United States.

In 1995, President Bill Clinton appointed Carlin to the position, even though the former Kansas governor lacked the traditional credentials.

Carlin told the Kiwanis members that as a dairy farmer he learned early in life how important it was to preserve records.

"Record-keeping holds the government accountable on a number of matters, including issues involving America's veterans," he said. "As an example, within the archives are records to prove that veterans, applying for benefits, were honorably discharged from the military."

Carlin presided in an era that featured many changes and challenges – including how to manage e-mail records. Right away he foresaw the significance of this communications method: "It was not easy to convince the powers-to-be that email was the coming trend," he said.

Carlin

Carlin also resisted a suggestion that the original copies of the Declaration of Independence and Constitution be moved down the street to the Smithsonian Institution.

Carlin told the audience he had also helped effect the release of presidential tape recordings from the Oval Office.

"President Lyndon Johnson installed a system where he could selectively record conversations by activating an on-and-off switch," Carlin said. "On the other hand, [President Richard] Nixon's tape-recording system remained on at all times, so noises from the evening housecleaning crew were tape recorded too."

The former archivist also spoke fondly of a time when the political parties managed to work together despite their differences.

"In the 1950s, Dwight Eisenhower was president, Sam Rayburn was speaker of the House of Representatives, and Lyndon Johnson was majority leader of the United States Senate, creating an environment where many great things were accomplished, including passage of the interstate highway system," Carlin said.

CYBERSECURITY

U.S. Economy Could Lose $15B if a Major Cloud Provider Is Inoperable for a Few Days

If a cyberattack stops a cloud giant from operating for just three days, it would have a massive impact on U.S. businesses, according to a report from insurance provider Lloyd's and risk modeler AIR Worldwide.

Projections for the full economic impact of such an attack are in the report *Cloud Down - The impacts on the US economy,* released by Lloyd's in January.

The projections point to the increasingly important role that cloud computing is playing in the U.S. economy. Reportedly, 37% of companies will use public infrastructure as a service (IaaS) for at least one workload by the end of the year, and the numbers are expected to keep growing, says McKinsey & Company research that is referenced in the report. Conner Forrest, author of the *TechRepublic.com* article that summarizes the report, writes, "As such, it is critical that businesses have a clear disaster recovery plan, as well as a plan for protecting their cloud assets."

The report suggests that *Fortune* 1000 companies would carry 37% of economic losses and 43% of insured losses, while other companies would suffer a 63% share of economic losses and 57% of insured losses. If the projections are accurate, then smaller companies are clearly at a much higher risk.

"Clouds can fail or be brought down in many ways – ranging from malicious attacks by terrorists to lighting strikes, flooding or simply a mundane error by an employee," Trevor Maynard of Lloyd's said in the report. "Whatever the cause, it is important for businesses to quantify the risks they are exposed to as failure to do so will not only lead to financial losses but also potential loss of customers and reputation."

PRIVACY

European Court's Decision on Video Surveillance Favors Employees

Early this year, the European Court of Human Rights (ECtHR) issued its judgement in *López Ribalda v. Spain* regarding the covert video surveillance of a Spanish supermarket chain's employees after suspicions of theft had arisen. The judgment centered on the fact that the employer had installed both visible and hidden cameras but only told its workers of those that were visible.

According to *DataGuidance.com*, the ECtHR held that under Spanish law, individuals should be clearly informed about the storage and processing of personal data, and the applicants had been given no such warning. Moreover, the ECtHR held that the employer's rights could have been safeguarded by other means and that it could have at least provided the applicants with general information about the surveillance. As a result, the ECtHR ruled that the domestic courts had failed to strike a fair balance between the applicants' right to privacy and the employer's property rights.

Attorney Joaquin Muñoz Rodríguez, of Ontier LLP, believes the judgement is critical of the balance the national courts had held between the rights that were at stake. Rodriguez told *DataGuidance.com* that these types of cases are tough to resolve because there are strong arguments for both sides.

"As a result, it is not easy for me to understand a judgement that is so categorical, where the judges have given such little importance to the great losses suffered by the employer, when it was demonstrated that suspicions regarding theft from employees were justified," he said. "On the other hand, the fact that not only suspected employees, but all the employees were investigated and that the hidden cameras were installed with the apparent intention of remaining, meant that the principle of proportionality was not complied with. Therefore, it is interesting to remark upon the opinion expressed by Judge Dedov that the right to data protection should never be used as an alibi to commit criminal acts."

INFO TECHNOLOGY

Virginia Delegate Introduces Blockchain To State Recordkeeping

The *Republican Standard* reports that Delegate Glenn Davis (R-Virginia Beach) has proposed a House Joint Resolution to study blockchain technology in state recordkeeping.

The article describes blockchain as a technology in which "each block in the chain is marked with a link to a previous block in the sequence, a timestamp, and the subsequent transaction data." These markings help make the blockchain records resistant to modification and therefore permanently reliable. Additionally, the decentralized nature of the technology allows anyone to access records.

According to the report, H.J. 153 is stated to establish a "one-year joint subcommittee consisting of seven legislative members and five nonlegislative members to study the potential implementation of blockchain technology in state record keeping, information storage, and service delivery."

The resolution addresses three problems in electronic recordkeeping: maintenance, transparency, and cyber attacks. Reportedly, paperless transactions and the permanent, unalterable recordkeeping system will be immune to cyber attacks and data destruction.

The House of Delegates is expected to create a cryptocurrency wallet for private donations to fund the work.

E-DISCOVERY

Judge, Considered an E-Discovery Visionary, Retires from Bench

U.S. Magistrate Judge Andrew J. Peck of the Southern District of New York (SDNY), author of some of the most significant opinions on e-discovery, has retired from the bench after 23 years of service, according to a March 5 article on the New York Law Journal page of *Law.com.*

In the article, Ian Lopez writes that Peck is "recognized internationally for bringing e-discovery competency to the attention of both the judiciary and bar."

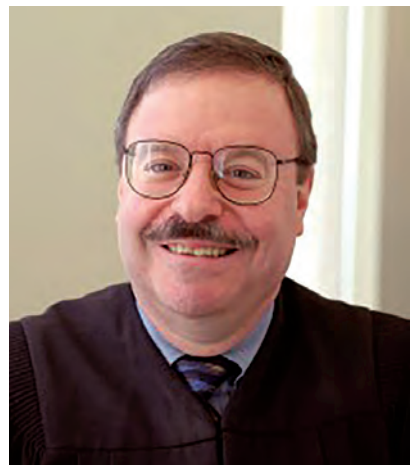
Retired SDNY District Judge Shira Scheindlin, who in her own right is noted for the influential Zubulake ruling, considers Peck to be perhaps the first judge to tackle the subject of e-discovery head on: "He's been a giant in the field of e-discovery. He was in the field first and last . . . [he issued] one of his earliest opinions before any of us were in [the field]."

According to the *Law.com* article, the opinion Scheindlin referenced was 1995's *Anti-Monopoly v Hasbro,* in which Peck said "computerized data is discoverable if relevant."

Kenneth Withers, deputy executive director at The Sedona Conference®, refers to Peck as "the first judge to actually identify e-discovery as a unique phenomenon."

Peck was especially influential in the area of predictive coding, and in *Monique Da Silva Moore, et. al. v. Publicis Groupe & MSL Group*, an employee class-action lawsuit, he provided the first judicial decision that approved the use of technology-assisted review (TAR), a process that relies on keyword searching and uses automation to strike potentially irrelevant documents from an e-discovery review set.

"Prior to Da Silva Moore, I don't think predictive coding and TAR really were all that well-known," said U.S. District Judge Xavier Rodriguez of the Western District of Texas, also a luminary on the topic of e-discovery. "Outside that little world, I don't think anybody really knew much about TAR or predictive coding."



Hon. Andrew J. Peck

Scheindlin calls *Da Silva Moore* Peck's "big blockbuster case."

In April, Peck plans to return to legal practice with the firm DLA Piper as a senior counsel. He is also a nominee to The Sedona Conference® Working Group 1 Steering Committee, which establishes guidance on e-discovery issues.

E-DISCOVERY

The Sedona Conference® Issues New Principles for E-Discovery

Earlier this year, The Sedona Conference® released the public comment version of its *Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations.* As reported on *JDSupra.com*, the draft contains five principles that apply to the issue of bring-your-own-device (BYOD):

1. Organizations should consider their business needs and objectives, their legal rights and obligations, and the rights and expectations of their employees when deciding whether to allow, or even require, BYOD.
2. An organization's BYOD program should help achieve its business objectives while also protecting both business and personal information from unauthorized access, disclosure, and use.
3. Employee-owned devices that contain unique, relevant electronically stored information (ESI) should be considered sources for discovery.
4. An organization's BYOD policy and practices should minimize the storage of – and facilitate the preservation and collection of – unique, relevant ESI from BYOD devices.
5. Employee-owned devices that do not contain unique, relevant ESI need not be considered sources for discovery.

The Sedona Conference® encourages the public to comment on the principles.

New! Job Descriptions

for Information Management and Information Governance

This publication is a guide for creating effective information management job descriptions at four levels – from entry to executive – as well as inforamtion governance job descriptions for professionals with the requisite knowledge and skills.

NOW AVAILABLE

Members Download **$45**

(non-member price: $65)

Available today at ***http://bit.ly/2tlsWur*** ARMA INTERNATIONAL BOOKSTORE

CYBERSECURITY

Opinion: Preparation, Fast Response Mitigate Data Breach Damages

Nearly 5 million data records are lost or stolen worldwide every single day, according to the Breach Level Index – a staggering 58 records every second.

In an opinion piece on *CSOOnline.com,* Michelle Drolet, a data security executive, focuses on the real costs of a data breach, asserting that the true picture is often understated – especially early in the process.

What's the cost of a data breach? Ponemon Institute's 2017 Cost of Data Breach Study puts the global average at $3.6 million, or $141 per data record. According to the study, the average cost of a data breach in the United States is $7.3 million.

Drolet suggests the expense of non-compliance could skyrocket when the General Data Protection Regulation becomes effective in May.

Using the Ponemon study as a frame of reference, Drolet emphasizes the importance of reacting properly to an incident. She writes: "While the initial breach is certain to cost money to fix, things get a great deal more expensive when they're mishandled. For example, Equifax made a bad situation a lot worse by delaying disclosure, misdirecting potential victims, and failing to patch known vulnerabilities."

A solid security program is more than a preventative measure, she argues, because it also trains employees how to respond when a suspected breach occurs. She writes: "Ponemon found that an incident response team can reduce the cost of a breach by up to $19 per record. If you want to keep costs down, having a solid response plan in place and taking the right action quickly is vital."

Drolet encourages organizations to reduce their response time to breaches by keeping current with the National Institute of Standards and Technology (NIST) cybersecurity framework, maintaining tighter management of data, and perhaps even scanning the "dark web" for intelligence on threats that may be looming.

DISPOSITION

Canadian Official: Mitigate Effects of Breaches by Following a Deletion Policy

As reported on *ITWorldCanada.com,* an official from the Auditor General of Canada recently told a forum that the greatest risk from retaining information for too long was a data breach.

"You don't want to be in the position where four years down the road [from the creation of an e-mail or document] where for whatever reason you're breached — someone has their briefcase stolen or loses a USB that isn't encrypted or you're hacked — and you're asked, 'Why did you have this information? It's useless,'" warned Cameron Fraser, in a presentation to the Canadian Institute's annual Privacy and Data Security Compliance Forum.

Instead, suggested Fraser, the proper approach is to create a data retention and destruction policy and appoint a retention office to monitor its compliance.

Fraser emphasized that data must have a life cycle. Generally, he posited, most information can be destroyed after two years unless it must be retained for legal or regulatory reasons.

He said a data retention team should establish such a policy, with representation from all business units. Further, the policy should have rules to make things easier for the users, such as limiting the size of inboxes and the retention of early drafts of documents.

Fraser did, however, caution against permitting staff to become too enthusiastic about reducing data. "Going too far and destroying things that may have business value," is the biggest mistake organizations make, he said.

CYBERSECURITY

GSA to Enhance its Cybersecurity Requirements

The U.S. General Services Administration (GSA) has proposed new rules to upgrade its cybersecurity requirements as it builds upon the Department of Defense's new requirements that recently became effective.

As reported on *HuntonPrivacyBlog.com*, the first proposed rule will require federal contractors to "protect the confidentiality, integrity and availability of unclassified GSA information and information systems from cybersecurity vulnerabilities and threats in accordance with the Federal Information Security Modernization Act of 2014 and associated Federal cybersecurity requirements."

The rule will mandate compliance with applicable standards and controls, such as those of the National Institute of Standards and Technology, and will update agency clauses that currently address data security. Additionally, contracting officers must include these cybersecurity requirements in their statements of work.

The proposed rule is scheduled to be released in April. The public will then have 60 days to comment.

The second proposed rule, scheduled for an August release, is designed to "update requirements for GSA contractors to report cyber incidents that could potentially affect GSA or its customer agencies."

More specifically, contractors must report any cyber incident "where the confidentiality, integrity or availability of GSA information or information systems are potentially compromised."

It will establish a timeframe for reporting cyber incidents, detail what the report must contain, provide points of contact for filing the report, establish requirements for contractors to preserve images of affected systems, and impose training requirements for contractor employees.

PRIVACY

UK Court Says Mass Surveillance Powers Are Not Legal

TheVerge.com reports that the UK might be compelled to scale back its digital mass surveillance plans after a recent court ruling.

The UK's Court of Appeal held that the Data Retention and Investigatory Powers Act (DRIPA) did not adequately restrict police access to such personal data as phone records and web-browsing history. Three appeal court judges said that because DRIPA lacked safeguards it was "inconsistent with EU law."

In 2014, DRIPA was passed as "emergency" legislation, having merited only a single day of debate. The law paved the way for the Investigatory Powers Act of 2016, which permitted additional intrusive powers.

The rejection of DRIPA means the government will likely need to scale back the Investigatory Powers Act, which essentially replaced DRIPA and which allows targeted hacking by UK security services and requires Internet service providers to retain a record of all users' web-browsing habits for at least a year.

MP Tom Watson, a driving player behind the case against DRIPA, praised the ruling in a statement:

"This legislation was flawed from the start. It was rushed through Parliament just before recess without proper parliamentary scrutiny. The government must now bring forward changes to the Investigatory Powers Act to ensure that hundreds of thousands of people, many of whom are innocent victims or witnesses to crime, are protected by a system of independent approval for access to communications data."

"This legislation was flawed from the start. It was rushed through Parliament just before recess without proper parliamentary scrutiny."

FRCP

Judges Say Laws for FRCP, Digital Evidence Can be Improved

At a *Legalweek 2018* session, three former federal judges spoke about the biggest challenges facing the judiciary.

A summary on *Law.com* suggests there were three main takeaways from the session "Back to the Future: Predictions from the Bench."

One prediction: "Sanctions are far from dead." U.S. District Judge Xavier Rodriguez said the Federal Rules of Civil Procedure (FRCP) Rule 37(e) has not efficiently helped rein in the sanctions from the mishandling of electronic evidence. "I don't think 37(e) has had the impact that the framers intended," he said. "We took a poll of judges a few months ago and determined they haven't seen a significant downturn in the number of sanction motions. [The rule] may have ameliorated the fear of counsel for facing the most-severe sanctions, but it hasn't reduced the number of sanctions."

Two, the system has been "papered to death." Former Magistrate Judge David Waxse suggested the

FRCP amendments shifted the responsibility to make civil proceedings "just, speedy and inexpensive" from the judges to the lawyers. "I think, and I've been saying this for years and years now, that lawyers have to come to grips with the fact that the litigation system is not set up to give them a place to play or make lots of money. The purpose of the litigation system is to get disputes resolved," he said.

Despite the FRCP's intention, civil litigation can still be as inefficient and laborious as ever. "Everybody files a motion to dismiss, everybody files a motion to summary judgment, and somehow if you get past this, the expert will be challenged by a Daubert challenge," said Rodriguez. "That's just what we see; we are papered to death here."

He added that such inefficiencies cut to the core of the civil litigation system: "We are competing against arbitration, and if we don't make the civil justice system speedier or economic—you know there's a reason why everybody goes to arbitration now."

Three, there's a "digital evidence divide." Judges are noting how the rise of digital evidence is outpacing the laws that are meant to regulate it.

Said Waxse: "The law is very unclear on how you apply the Fourth Amendment to situations with electronic information. I kept seeing government requests for search warrants that were exceedingly broad; they were unconstitutionally broad."

CYBERSECURITY

Cyber Attacks Have Doubled, But More Incidents Are Being Thwarted

ThreatMetrix, a company that provides user-identity intelligence services, says there's been a 100% spike in the volume of cyber attacks over the past two years, as reported by *Information-management.com*. Meanwhile, on the positive side, "record numbers of these attacks were thwarted by organizations that have deployed strategies to protect against large-scale data breaches," the article asserts.

The report took into account the analysis of cybersecurity attacks as seen across the global network monitored by ThreatMetrix, which analyzes 100 million transactions per day.

Such analysis suggests that cyber crooks are focusing on attacks that can generate long-term profits by leveraging sets of stolen identity data. In particular, account creations are seen as vulnerable activities: Greater than one in nine of all new accounts opened in 2017 were fraudulent, says ThreatMetrix.

The report also found that account takeover attacks increased 170%, that 83 million fraudulent new accounts were attempted between 2015 and 2017, and that fraudulent payments increased 100% over the last two years.

Congratulations

to the **IGP** Fall Class of 2017

Joshua Aldrich
Clifford Anglim
Jessica Arts
Christopher Austin
Christopher Barden
Jennifer Barsetti
Baird Brueseke
Sharon Burnett
Laural Byrd
Jacqueline Carmona
Patrick Chavez
Adrian Clayton
Stephen Cole
Liane Cooper
Dustin Dowdy
Katalin Fur
Ralph Furino
Ann Gorr
William Henson
Allan Hollingsworth
Ulrich Houzanme
Michele Hovermale
Lynne Hunks
Mark Lagodinski
Traci Larsen
Caroline Lawrence Depue
Seth Magaw
Robert McKee
Daniel McKnight
Vineet Mehta
Katy Andrew Mjelde
Samantha Moss
James Mullen
Natalie Noonan
Barbara Nye
Babette Orenstein
Nathan Owens
Treesa Parker
Lisa Ricciuti-Borenstein
Michael Rogers
Donald Rosen
Tyler Selle
Erik Sokolovsky
Marry-Ellyn Strauser
Megan Sughroue
Kedar Thakkar
Kathi Vosicky
Larry Weir

Spring 2018 Testing Dates: March 19 - May 18. Apply by May 11. *http://bit.ly/2AyyAYe*

INFO SECURITY

DPO Role is Hottest Tech Ticket in Town, Says Reuters

To illustrate the importance of the data protection officer (DPO), a February *Reuters.com* article pointed to the career arc of Jen Brown, who attained her first certification for information privacy in 2006 and had a difficult time finding a job.

But now Brown's inbox is "besieged by recruiters."

That's because organizations around the world are scrambling to conform with the General Data Protection Regulation (GDPR), which takes effect in May.

"I got into security before anyone cared about it, and I had a hard time finding a job," she told *Reuters*. "Suddenly, people are sitting up and taking notice."

Brown is DPO of analytics for Sumo Logic in Redwood City, Calif.

The GDPR gives European citizens more control over their online information and applies to all organizations that do business with EU citizens. Organizations whose core activities include substantial monitoring or processing of personal data must hire a DPO.

And finding DPOs is not easy. According to the International Association of Privacy Professionals, more than 28,000 will be needed in Europe and the United States alone, with an estimated 75,000 needed worldwide. According to *Reuters*, DPO listings in Britain on the Indeed job search site have spiked by more than 700% over the past 18 months.

The need for DPOs is expected to be particularly high in any data-rich industry, such as tech, digital marketing, finance, health care, and retail.

"I would say that I get between eight and 10 calls a week about a role (from recruiters)," said Marc French, DPO of a Massachusetts company called Mimecast. "Come Jan. 1 the phone calls increased exponentially because everybody realized, 'Oh my god, GDPR is only five months away.'"

GDPR requires that DPOs help their organizations on data audits for compliance with privacy laws, train employees on data privacy, and serve as the point of contact for European regulators.

GDPR

EU Commission Issues Further Guidance on GDPR

As noted on the International Association of Privacy Professionals site, the European Commission (EC) has released a new website with extensive guidance on General Data Protection Regulation (GDPR) implementation for data protection authorities (DPAs), member states, businesses, and data subjects. The site has infographics, explainer documents, a guide to GDPR enforcement, and general FAQ-style information.

The Commission has earmarked €1.7 million to help fund DPAs and train data protection professionals, as well as another €2 million for member state-level information campaigns, particularly targeted at small businesses.

"There will be targeted outreach to SMEs in member states where we hear there is large-scale lack of awareness thus far," said Renate Nikolay, an EC official, in a conference presentation in Brussels. "We have to carry everyone with us. It's not that homogenous in the EU yet. In some member states, the awareness for data protection is much more developed than in other member states."

In an effort to spread the word to newer EC nations, officials will travel to Croatia, the Czech Republic, and Bulgaria.

Nikolay said the EC is planning a one-year-anniversary meeting with subject matter experts, politicians, DPAs, and other stakeholders to evaluate the guidance initiative's progress.

RETENTION

Rethink Your Outdated Retention Procedures, Says IM Consultant

In a *BusinessLawToday.org* opinion piece, Randolph A. Kahn, Esq., a Chicago-based authority on e-records and information management, recently urged organizations to rethink their records retention programs. In particular, Kahn asserts that using retention rules that were constructed decades ago is no longer viable; he compares it to "a dude in a leisure suit ready for disco dancing is jettisoned into a mosh pit in 2018."

In his Feb. 12 article, Kahn says it's nearly impossible today to get a handle on all of the information in a large organization, and there are competing interests that have their own agendas for how to retain and use data. "Big Data professionals want to keep as much information for long periods of time because they don't know what information will prove useful when using analytics tools to answer business questions," he writes.

Further, the looming General Data Privacy Regulation (GDPR) "requires ensuring that the period for which the personal data are stored is limited to a strict minimum."

He also cites the dynamic changes in the way business is now conducted, which complicates the management of information. "We regularly enter contracts using e-mail, modify them with a text message, and breach them in social media. Business is now casual and immediate," he writes.

Kahn provides and fully describes what he calls "12 Rules to Help Fix Records Retention and Wrangle the Information Piles."

Among his rules are "simpler retention built for technology," "different storage locations for records and nonrecords," "seek reasonableness, not perfection," and "resist permanent retention where possible."

He concludes that organizations must not be deceived by the claim that "storage is cheap." The costs of having too much information can be significant in the contexts of security, risk, availability, and business efficiencies.

PRIVACY

NY AG Office Fines Aetna for Leaking Members' HIV Status

Aetna, Inc. must pay a $1.15 million civil fine and boost its privacy practices to settle charges that it leaked the HIV-positive status of 2,460 New York members by using envelopes with large transparent windows.

According to *Reuters*, New York Attorney General Eric Schneiderman said names, addresses, claim numbers, and HIV medication instructions in a July mailing were "clearly visible" to anyone because of how the insurance company folded letters and inserted them into the envelopes.

Ironically, the mailing was intended to help ensure privacy: it notified members of a class action settlement permitting them to buy HIV medication at actual pharmacies rather than by mail, where their privacy could be compromised if family or neighbors saw the drug packages.

The settlement papers cited the stigma associated with HIV, which can result in denial of proper health care and other discriminatory practices.

"Through its own carelessness, Aetna blatantly violated its promise to safeguard members' private health information," the attorney general said in a statement.

While Aetna did not admit or deny wrongdoing, it agreed to retain an independent consultant for two years to monitor its efforts to improve member privacy.

"We have worked to address the potential impact to members following this unfortunate incident," Aetna said in a statement. "We are implementing measures designed to ensure something like this does not happen again as part of our commitment to best practices in protecting sensitive health information." E