Information Management

E-DISCOVERY

Federal Judges Give E-Discovery Advice at inFusion 2017

LegalTechNews.com reports that a recent panel discussion among federal judges resulted in a wealth of advice for legal teams that need guidance on e-discovery. The judges – retired Magistrate Judge Frank Maas, Magistrate Judge Andrew Peck of the Southern District of New York, and District Judge Xavier Rodriguez of the Western District of Texas – conferred at inFusion 2017 in a session titled "State of E-Discovery: A Candid E-Discovery Conversation Between 3 Judges."

According to the article, the conversation generated four strains of advice. One is to "be mindful of new data types." According to Maas, there are always cutting-edge communication technologies that pose problems for e-discovery practitioners. "Back in the '90s it was email, now it's text messaging and other media like that. There is the problem that corporations by and large don't know where their data is,

who is keeping it, or where it is kept," he said. Judge Rodriguez noted that texting is particularly nettlesome because it's a method that tends to "bypass all of a company's [communication] systems."

The judges also encouraged more communication with outside counsel. Peck suggested that often the outside counsel provides arguments in court that are not entirely accurate, owing to a lack of sufficient communication with corporate counsel.

"Document everything" was also guidance the judges agreed upon. While the 2015 amendments to the U.S. Federal Rules of Civil Procedure give more leeway in deleting data in-house, organizations must still be able to demonstrate *why* they are not keeping the records. Rodriguez encouraged corporate counsel to "loop back in with outside counsel to get their opinion" when deleting data.

The fourth prevailing piece of advice was to obtain Federal Rules of Evidence 502(d) orders. The order essentially stresses there is no waiver of attorney-client privilege or work product privilege during the process of production. According to Peck, "It is akin to malpractice if you're the producing party and you have more than five documents to produce, to not consider or obtain a 502(d) order."

CYBERSECURITY

Survey Shows Info Security Chiefs Not Confident in Digital Defense

An IDG Connect survey, conducted on behalf of RiskIQ, finds that most information security executives have little or no faith in being able to manage digital threats, according to a summary on *Information-Management.com.*

A survey this year of 465 IT information security decision makers in the United States and United Kingdom shows that 68% of organizations have zero to modest confidence in managing digital threats, and 70% have zero to modest confidence in reducing their digital attack surface.

The survey also found that an average of 40% of organizations experienced five or more significant security incidents in the past 12 months. Among most cited external threats: malware, ransomware, phishing, domain and brand abuse, online scams, rogue mobile apps, and social impersonation.

E-DISCOVERY

"Do No Harm": Third Edition of *The Sedona Principles* Released

For the first time since 2007, The Sedona Conference® has completed a full update of its e-discovery principles, which are among the most referenced guidelines for e-discovery and for the meet-and-confer process.

The new third edition, according to an item on *LegalTechNews.com,* resulted from a four-year process and comment period.

"Our first guideline in the revision process was first, do no harm," said Kenneth Withers, deputy executive director of The Sedona Conference®. "The reason for that is because people have really built their practices, and judges have relied, on the Principles for years. So we can't willy-nilly pop into a Principle and say, 'Hey, all this precedent is out the window.'"

The Sedona Principles includes 14 statements the organization says are a "reasonable and balanced approach to the treatment of electronically stored information [ESI] in the legal process."

Notably, Principle 2, which focuses on the concept of proportionality, was updated to reflect the 2015 changes to the Federal Rules of Civil Procedure.

"We reformulated it to align with an updated view of proportionality," Eric Mandel, a member of the drafting team, told *LegalTechNews.com*. "The language of the principle changed, and every one of the comments was essentially rewritten. In 2006, proportionality was not as forefront as it became over time, which was particularly reflected in the 2015 amendments."

Additionally, Principle 3 was revised to reflect the inevitability of ESI in the e-discovery process, a point of contention during the drafting of the second edition some 10 years ago. Said Mandel: "We stopped the [phrase], 'if and when ESI show up,' because that's not the case anymore. I think [last time] we were trying to be diplomatic to the larger litigation community … but now we know that ESI is here to stay. It's not going anywhere, it is a fundamental part of discovery."

The new edition of The Sedona Principles, which contains many other revisions, can be found on the The Sedona Conference® website at *https://thesedonaconference.org/download-pub/5339*.

PRIVACY

Spain Fines Facebook for Using Personal Data Without Informed Consent

The Spanish data protection authority, AEPD, recently said it would fine Facebook, Inc. 1.2 million for allegedly collecting personal data for advertising purposes without clearly informing the individuals of the methods and getting their consent, according to a report on *DataGuidance.com.*

More specifically, the complaint suggests the social media giant had mined personal data for advertising purposes by monitoring users' interactions with certain services and with third-party pages using the "like" buttons.

The AEPD said Facebook's privacy policy used generic and unclear terms in describing its collecting, processing, and storing of customer data. It also claimed Facebook misled users by saying it did not process sensitive personal data for advertising purposes, and that the company retained sensitive data for much longer than was useful for the purposes it was collected.

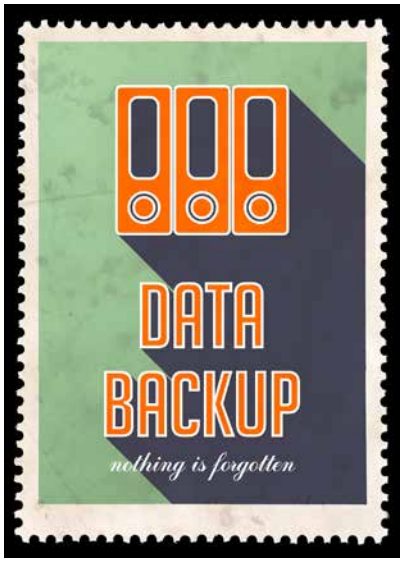
The sanction follows a joint investigation into Facebook's privacy and cookie policies, carried out by the AEPD, the Dutch data protection authority, the Hamburg State Commissioner for Data Protection and Freedom of Information, and the Belgian Commission for the Protection of Privacy.

An attorney in Spain, Joaquin Muñoz Rodríguez, noted that such violations could exact heavier fines after the General Data Protection Regulation (GDPR) is in effect next May. "It is true that the infringements committed by Facebook are among those listed in the GDPR as serious, and in this case they may have reached a fine of up to 4% of the total worldwide annual turnover of the preceding financial year, but alleviating and aggravating circumstances must also be taken into account."

Rodriguez encouraged all companies to review their data processing practices in anticipation of the GDPR launch.

CYBERSECURITY

Evidence Lost in Rapid Recovery from Data Breach



Because it has a solid back-up policy, a healthcare center in Salina, Kansas, was able to bounce back quickly from a ransomware attack this summer. Unfortunately, the response was so rapid that evidence of the attack itself was forever lost, making it difficult to assess the damage and discern what information was compromised.

According to an article on *Information-Management.com*, Salina Family Healthcare backs up data nightly, its servers weekly, and its entire system monthly. All content is encrypted and stored offsite. But the back-up policy had a flaw that wasn't known until the attack.

"We were so intent on getting back online, we didn't think about preserving evidence," Rob Freelove, the center's CEO, told *Information-Management.com*. Evidence had been lost because all the servers were scrubbed of data and rebuilt from the back-up tapes.

"Leaving one server uncleaned would have helped in getting more forensics evidence," Freelove said. "We had 33 end-user terminals deleted and rebuilt and should have saved one or two hard drives for the forensic investigators."

Because the center could not dismiss the possibility that data had been compromised, it had to send notification letters to some 70,000 patients and offer a year of credit monitoring and identity protection services.

"To date, we are not aware of the misuse of anyone's information as a result of this incident," the organization said in the patient notification letter

COMPLIANCE

Too Many Fail to Meet Payment Card Industry Standards

Take Our Latest One-Question *IM* Poll

In her article, Vicki Lemieux, Ph.D., CISSP, explains blockchain technology and describes its promises, perils, and future in a way that will help readers provide sound advice about its potential for their business. Please take a moment to tell us whether your organization uses, does not use, or plans to use blockchain technology at ***http://imm.explorearma.org/Blockchain.***

Read the article on page 20 that prompted this survey.

The Sept./Oct. *IM* poll revealed that respondents' (128) greatest challenge is:

- Devising effective retention/disposition strategies (**29%**)
- Ensuring legal/regulatory compliance (**13%**)
- Protecting personal information privacy (**10%**)

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

A Verizon report, summarized on *ZDNet.com*, suggests that while a growing number of enterprises are in compliance with the Payment Card Industry Data Security Standards (PCI DSS), too many still are struggling to get or remain in compliance with its controls.

The Verizon 2017 Payment Security Report says that 55% of organizations complied with PCI DSS when validated last year, a 6% boost from 2015. But, that means roughly 45% continue to fall short of PCI expectations, opening the door to breaches. PCI DSS requirements are focused on such measures as firewalls, data-in-transit controls, encryption, and authentication. The report says that of the companies that pass validation, about half of them fail to maintain that compliance for a full year.

The IT services industry scored the highest, with 61.3% of that field's respondents deemed fully compliant.

ZL TECH

Information Governance Solutions

where insight meets action

RIM

eDiscovery

File Analysis

Compliance

Archive

www.zlti.com

@zltechnologies

(+1) 408 240-8989

ZL Technologies

GOVERNMENT RECORDS

Victoria Australia Appoints First Info Commissioner

Sven Bluemmel

ZDNet.com reports that the Australian state of Victoria appointed Sven Bluemmel as its first information commissioner this summer. Bluemmel now oversees the state's data protection laws, freedom of information regime, and the privacy of its departments and agencies. In a public statement, Special Minister of State Gavin Jennings said the information commissioner would provide advice and improve how Victoria manages its data.

Said Bluemmel: "The creation of the new commissioner is an excellent opportunity to bring together freedom of information, privacy, and data protection under a single regulator and I am looking forward to leading the new office."

The appointment coincides with Victoria's release of a five-year cybersecurity strategy, which intends to take a "whole-of-government" approach. The strategy document says "the time for an agency-by-agency (only) approach has passed." This holistic approach differs from that of the Commonwealth government, which leaves departments responsible for their own cybersecurity.

PRIVACY

EU Commission Reports on First Review of Privacy Shield Framework

In October, the EU Commission published a report and a working document on its first review of the EU-U.S. Privacy Shield framework.

According to a summary on the *Hunton Privacy Blog*, the report says the Privacy Shield framework "continues to ensure an adequate level of protection for personal data that is transferred from the EU to the U.S." Additionally, it suggests the U.S. authorities have enacted the necessary procedures to assure the proper functioning of the Privacy Shield – in part by adding redress options for EU citizens and instituting safeguards to protect personal data from government access.

Titled "Report from the Commission to the European Parliament and the Council," the document also says that adequate procedures have been established for complaints and enforcement measures.

The report offers recommendations to help assure continued proper functioning of the Privacy Shield. It states the U.S. Department of Commerce should more robustly monitor framework compliance and conduct regular audits of organizations that claim to be participating. Further, the report says there needs to be more awareness among EU individuals on how to exercise their privacy rights and how to submit complaints within the framework. It calls for more collaboration among the framework's enforcers: Commerce, the U.S. Federal Trade Commission, and the EU data protection authorities. The report also finds the need for a permanent Privacy Shield ombudsperson to be appointed as soon as practicable.

Regarding the review, one Commission member, Vera Jourová of Czechoslovakia, voiced a "so far so good (mostly)" comment: "Transatlantic data transfers are essential for our economy, but the fundamental right to data protection must be ensured also when personal data leaves the EU. Our first review shows that the Privacy Shield works well, but there is some room for improving its implementation. The Privacy Shield is not a document lying in a drawer. It's a living arrangement that both the EU and U.S. must actively monitor to ensure we keep guard over our high data protection standards."

According to the summary, the Commission will work with U.S. authorities to implement the report's recommendations.

CYBERSECURITY

Equifax Incident Prompts Reintroduction of Data Breach Bill

On Sept. 18, Rep. Jim Langevin (D-R.I.) reintroduced legislation to establish national standards for informing consumers when their data has been hacked or breached. According to *FCW.com*, The Personal Data Notification and Protection Act of 2017 would require companies that use, store, or access sensitive or personally identifying information for more than 10,000 people per year to notify their customers within 30 days of discovering a breach. The legislation would also designate the Federal Trade Commission as the government's coordinating agency to ensure a company's customers are properly notified.

"There is much still to learn about the Equifax breach and its ramifications. What is abundantly clear, however, is that consumers are still not sure whether they were affected and what information was stolen," said Langevin in a statement announcing the bill's reintroduction. "Equifax has done a terrible job communicating about the breach to date, and this legislation will ensure that any future such breach has a single standard and one federal regulator to help get actionable information to consumers quickly."

"What is abundantly clear is that consumers are not sure whether they were affected and what information was stolen."

PRESERVATION

NARA Reminds White House of Duty to Preserve

According to a report on *Politico.com*, National Archives and Records Administration (NARA) officials have at times warned White House lawyers that the administration must follow document preservation laws, according to individuals familiar with the conversations and based on e-mails seen by *Politico*.

To comply with legal requirements, the White House must preserve all presidential records, which are given to NARA after the president leaves office. The documents that require preservation include written memos, e-mails, speeches, record logs, and more.

White House officials have assured NARA staff that its personnel are being reminded of the rules. In a September 26 e-mail that was later forwarded to *Politico*, a senior White House lawyer did remind the team to comply: "Pursuant to our conversation this morning ... the email chain below recirculates written guidance issued in February consistent with verbal instruction our team has been providing since Transition." The e-mail came one day after disclosures that senior adviser Jared Kushner and others had been using private e-mail accounts for official business.

In the message, staff were reminded of the proper use of communications and record-keeping under the law: "Use of personal email, text messages, instant messages, social networks, messaging apps (such as Snapchat, Confide, Slack or others) or other internet-based means of communication to conduct official business is not permitted . . . ." Employees were advised that all work-related communications must take place on official government e-mail accounts as well, and that any official communication that comes in on a private account must be forwarded to the official account.

"Failure to abide by these requirements may lead to administrative penalties," White House officials were reminded. "The willful destruction or concealment of federal records is a federal crime."

The article suggests there have been general concerns among NARA staff that the White House has been haphazard with handling government materials. *Politico* earlier reported on several White House officials using personal devices and personal e-mail accounts for official business, which raises concerns about security and preservation.

The White House lawyer also informed NARA that every new White House employee was required to attend a training session on ethics, which includes guidance on the use of personal and professional e-mail.

The White House declined to comment on these reports.

GOVERNMENT RECORDS

ICE Seeks to Destroy Detainee Death Records and Other Files

As U.S. Immigration and Customs Enforcement (ICE) steps up enforcement operations, the agency is asking to destroy some detainee records. Some of these records, however, will be maintained by National Archives and Records Administration (NARA) in perpetuity, as recently reported on *TheNation.com.*

In an e-mail to a reporter for *The Nation*, Laurence Brewer, chief records officer for the U.S. government, said that federal records are kept permanently to document: 1) the rights of citizens, 2) the actions of federal officials that are essential to understanding and evaluating federal actions, or 3) "the national experience."

In July, NARA published a request made by ICE to begin destroying detainee records, including those related to in-custody deaths, sexual assault, and the use of solitary confinement. The request has been given preliminary approval. ICE petitioned to begin destroying some types of records as quickly as three years after they are created, and after 20 years for others.

Examples of documents that NARA will permanently keep are ICE's Internal Affairs Significant Misconduct Investigative Case Files and the Department of Homeland Security's Civil Rights and Civil Liberties annual report.

INFO SECURITY

Security, Cost, Reliability Advantages Revive Appeal of Tape Storage

To stay current in the battle against cyber crooks, some companies are resorting to a 1950s technology – storing data on tape, according to an article on *WSJ.com.* The big security advantage of this vintage technology is that hackers have no way to get at the information. The federal government, financial services firms, health insurers, and other regulated industries still use tape as a backup to digital records. Now other companies are returning to it as the crooks are getting smarter about penetrating defenses and doing more damage when they get in.

Rob Pritchard, founder of the Cyber Security Expert consulting firm, says, "Companies of all sizes must be able to restore data quickly if needed, but also have a robust, slower-time, recovery mechanism should the worst happen. A good backup strategy will have multiple layers. Cloud and online services have their place, but can be compromised."

Marc Langer, founder and president of Recovery Point Systems, a business continuity and disaster recovery firm, says tape isn't meant to be the primary way for companies to restore data lost to hackers, but it can be a safe choice.

"Most people are looking for convenience and the cloud is convenient," he says. "Tape isn't inefficient or ineffective, but it can be inconvenient. Good security is almost always inconvenient."

Tape has other storage advantages, such as a higher reliability rate than hard drives and longer lifespans – more than 30 years, according to security experts. Additionally, the cost of ownership per terabyte is the lowest of any storage medium, according to the article. The best tapes can hold up to 15 terabytes and be archived in third-party locations at a fraction of the cost of the cheapest cloud storage.

"Tape is our main form of backup and recovery" says Computer Operations and Network Manager Rick Heisey of PDP Group, an insurance company. "We remain confident that tape will continue to be the most reliable and cost-effective means of protecting our company data."

ONLINE CENSORSHIP

EU Issues Guidance for Curbing Illegal Web Content

Reuters.com reports that in September the European Commission (EC) published guidelines to step up the prevention, detection, and removal of hate speech and terrorist-related content from the Internet, and it warned that legislation may be next.

"The rule of law applies online just as much as offline," Commissioner Vera Jourová said in a statement. "We cannot accept a digital Wild West, and we must act."

The proliferation of illegal content on the Internet has ignited debate in Europe between those who fear that restrictions will impinge on free speech and those who seek more restraint.

The EC-issued guidelines suggest that Internet companies establish trusted flaggers or invest more in automatic detection technologies as two tactics for more quickly and efficiently removing the illegal content.

The companies have already agreed to an EU code of conduct to remove hate speech within 24 hours and to assemble a global working group to combine their efforts in removing illegal content from their platforms. But, the EC said the companies were still too slow.

"The situation is not sustainable: in more than 28 percent of cases, it takes more than one week for online platforms to take down illegal content," said Mariya Gabriel, EU digital commissioner.

PRIVACY

India Supreme Court Rules Against Mandated Biometric Info Enrollment

India's Supreme Court has declared the right to individual privacy "intrinsic" and fundamental to dignified human existence under the country's constitution. The ruling is a rebuke to the government's plans to force all Indians to enroll in a massive identification system, according to a story in the W*ashington Post*.

For a few years, the Indian government has strong-armed its citizens to join a database called Aadhaar, which takes iris scans and fingerprints. To ensure complete enrollment, the government restricted access to essential services for anyone who did not join the database.

One activist says the court's message is clear: "This judgment says that the people of this country have rights, in case you've forgotten," said Usha Ramanathan, an independent law researcher.

With a guaranteed right to privacy, opponents of the database expect favorable rulings on petitions against the efforts to make enrollment mandatory.

The Indian government says Aadhaar is vital for better governance and that it can save Indian taxpayers billions of rupees by reducing welfare and tax fraud.

FOIA

Agencies Launch Lawsuits Against Those Seeking FOIA Records

An Oregon parent sought information on school employees who were paid to stay home. A retired educator requested data about student performance in Louisiana. And college journalists in Kentucky asked for documents about the investigations of employees accused of sexual misconduct. Instead of getting data, they got sued by the agencies they'd asked for public records, says a report by *APNews.com.*

Governments are increasingly suing citizens who seek public records that may be embarrassing or legally sensitive. A growing number of school districts, municipalities, and state agencies have filed suit against those making the requests.

The lawsuits generally ask judges to rule that the records being sought do not have to be divulged. They name the requesters as defendants but do not seek damages. Still, the recent trend has alarmed freedom-of-information advocates, who say it's a new way for governments to hide information, delay disclosure, and intimidate critics.

"This practice essentially says to a records requester, 'File a request at your peril,'" said University of Kansas journalism professor Jonathan Peters, who wrote about the issue for the *Columbia Journalism Review* in 2015, before several more cases were filed. "These lawsuits are an absurd practice and noxious to open government."

INFO SECURITY

University Report Describes role of 'Cyberpro'

IAPP.org cites an Ohio State University report that breaks down what a cyberpro is and describes the significance of the role across tech-driven fields.

The report defines a cyberpro as a professional who has hybridized skills and fluency across technology, law, regulations, and business processes. Being conversant with multiple fields and skillsets increases the efficacy greatly of those working toward securing the enterprise and ensuring data is used with the least risk for the most benefit.

"The siloed data governance professions of today will not be able to meet organizations' data risk management needs of tomorrow," says the report, titled "The Age of the Cyberpro," co-written by Professor Dennis Hirsch and Program Manager Keir Lamont, both of the university's Michael E. Moritz College of Law Program on Data and Governance.

PRIVACY

Australia: Former Agency Head Questions Breach Disclosure Exemptions

David Irvine, former head of the Australian Security Intelligence Organisation (ASIO), wonders why political parties are exempt from Australia's looming data breach notification laws, says a report on *ZDNet.com.* The new laws mandated under the Privacy Amendment (Notifiable Data Breaches) Act apply only to companies covered by the act, and therefore see intelligence agencies, small businesses with turnover of less than AU$3 million annually, and political parties exempt from disclosing breaches.

"I think that should be treated as a rhetorical question; my response would be why indeed," Irvine said when asked why political parties are exempt. "I think the parties probably do need a good cyber disaster to focus on this issue as is now happening in the United States. The fake news debacle in the US is probably doing a better job of raising the cybersecurity awareness within the political parties, not necessarily privacy, but if you think about the ultimate game is about raising security, that's going a long way. The parties are standing up and listening."

INFO VALIDATION

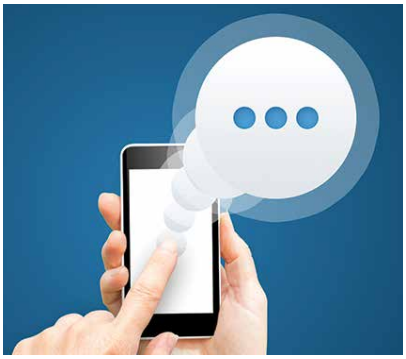
Australian Court Accepts Unsent Text Message as a Valid Will

An unsent text message has been accepted as an official will by a court in Queensland, Australia, according to an article originating on *EndGadget.com*. The message, found in the drafts folder of a deceased man's phone, said his possessions should go to his brother and nephew instead of his wife and son. The man composed the text message before taking his own life in October 2016.

The widow took the case to the Brisbane Supreme Court to manage her deceased husband's estate. She argued the text was not valid because it was never sent. But judge Susan Brown said the phrasing of the message (which included the words "my will") indicated the man was of sound mind. In the text, he'd also directed for his ashes to be put "in the back garden," and wrote he had a "bit of cash behind TV and bit in the bank."

According to the news item, the judge's action also considered evidence of the man's fraught relationship with his wife.

The Queensland government advises that a valid will must typically be in writing and signed in front of two witnesses, but a change in the law in 2006 allowed for less formal types of documents to be considered as well.



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

INFO CAREERS

Industry Study Suggests High Turnover Rate Among CDOs

More organizations are seeing the need for a chief data officer (CDO), but they're having a hard time retaining these professionals for very long.

An Experian Data Quality study suggests the average length of time on the job for a CDO is just 24 months, which is much lower than other C-level executives, as reported on *Information-Management.com*.

The study, titled "The Chief Data Officer: Powering Business Opportunities With Data," finds the CDO role is still very new in many organizations and those in the role have yet to be fully accepted as peers by their fellow executives.

The report found that fewer than half of CDOs said they were given clear objectives when they signed on to the position, and 90% said they were not able to devote their time to the areas they wanted.

FINRA

SEC Settles with Broker -Dealer on FINRA Charges

BOK Financial Securities, Inc., a registered broker-dealer, has reached a settlement with the U.S. Securities and Exchange Commission (SEC) over charges brought by the Financial Industry Regulatory Authority (FINRA), as widely reported in late October. The FINRA charges allege that for years BOK failed to keep nearly a quarter of a million electronic records in the "WORM" format (write once, read many), as required. FINRA also claimed that BOK lacked an audit system for the entry of digital records and failed to have adequate written supervisory procedures for retaining records.

BOK agreed to pay a $175,000 fine to settle the charges.

PRIVACY

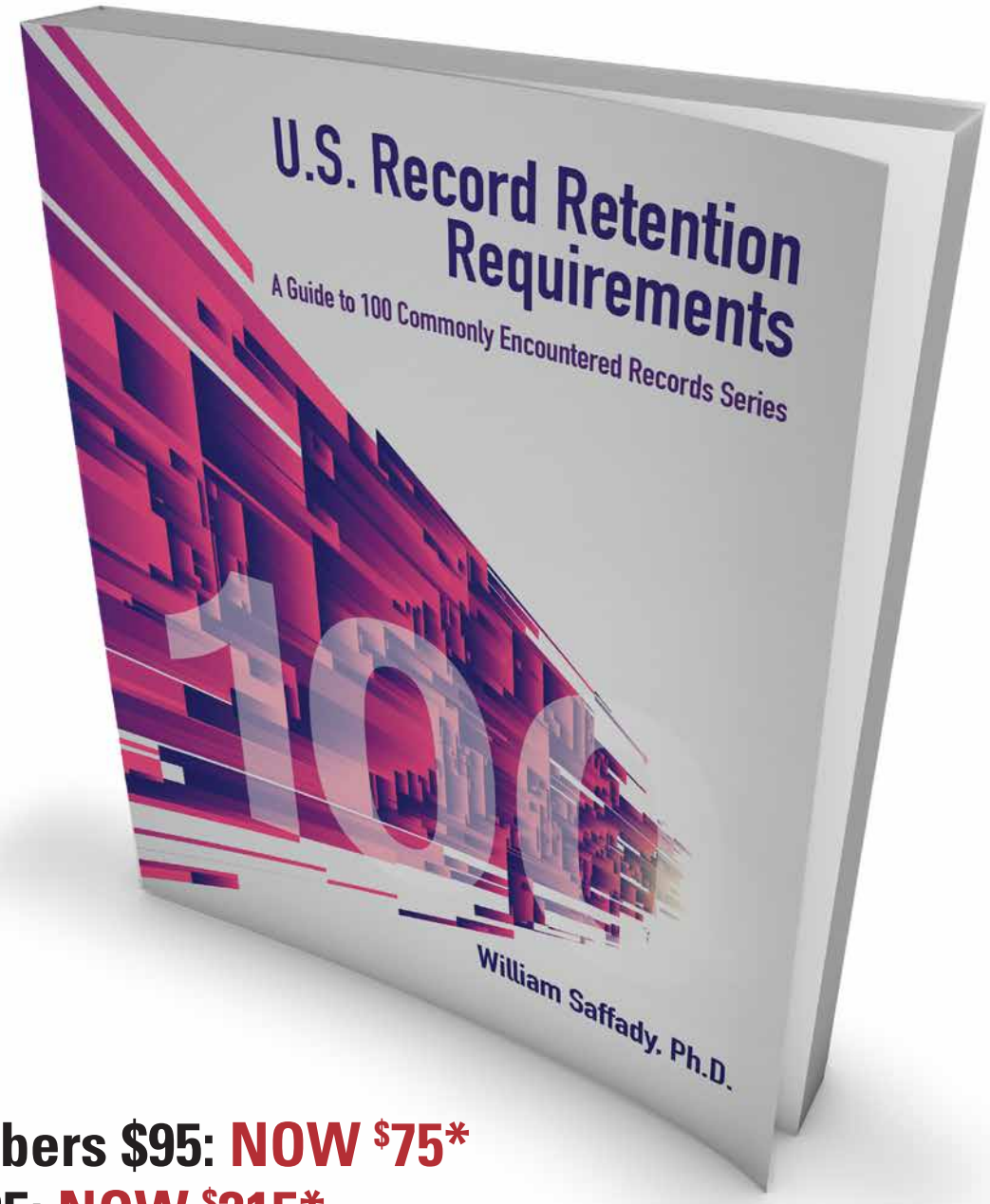
British Library Exempted from 'Right to Be Forgotten' Rule

Bloomberg.com reports that for decades and decades, if you wanted to learn more about a person, you had to pore through archives and public records. Of course, the Internet and search engines changed all of that. But now a proposed U.K. law may compel researchers back to the bookshelves, or at least to the British Library's website.

While the British government plans to make it easier for people to delete embarrassing or erroneous information about themselves online, new privacy rules will exempt Internet archives maintained by the British Library.

In August, U.K. Digital Minister Matt Hancock said new privacy legislation would expand "the right to be forgotten" beyond search engine results to any personal data held by a third party. The law would bring the United Kingdom in line with the European Union's existing General Data Protection Regulation, which takes effect in May 2018.

Coming Soon!
Pre-order now and save!



ARMA Members $95: NOW $75*
Regular: $235: NOW $215*

***Order by December 31, 2017 to save $20!**

www.arma.org/go/prod/A5308

Order online today! ARMA INTERNATIONAL BOOKSTORE

TRANSPARENCY

Newspaper Joins with FSU to Make Records Public from FBI Probe

The *Tallahassee Democrat* reports that it and the DeVoe L. Moore Center at Florida State University are combining to buy 90,000 pages of e-mail and other records that the City of Tallahassee gave to the FBI as part of a public corruption investigation.

Tallahassee officials had given the records in response to subpoenas on a project involving the Community Redevelopment Agency (CRA) and several business owners, some with ties to city officials.

The city came up with a fee of $9,375 for the records to be made public, based on staff time for reviewing and redacting confidential information; the fee also reflects $25 per hour to defray the "blended labor cost" of staff and supervisory time for processing such public records requests.

Publisher Skip Foster of *The Democrat* criticized the government for setting up such a steep financial obstacle: "Our view remains the same and is consistent with what I've preached in my 28 years in the business. The government ought to make it as easy as possible for the public to have access to records."

Foster said the documents would be put online in their entirety in the coming weeks.

"It's not a 'media records law,' it's a 'public records law,'" he said. "Charging thousands of dollars for public records when the very foundation of our city government is being called into question by this FBI investigation is misguided and short-sighted."

City officials said the nature of the emails – about 50,000 – called for "extensive" review to redact any data that can be exempted under state law and to exclude any "non-public records," which Tallahassee defines as e-mails "relating to personal matters; non-city business, including campaign events."

"We are interested in trying to provide substance to the debate and long-term solutions," said Sam Staley, director of the DeVoe Moore Center, which takes an evidence-based approach to transparency, accountability, and government performance.

The FBI subpoenas had sought records dating to 2012, related to the CRA and eight developers and their associated corporations. *The Democrat* and lawyer Steve Andrews had argued that the records are of vital public interest and the fees should be waived for anyone who asks for the records.

Generally, according to the article, agencies can only bill 15 cents per copy for documents or $1 a page for certified records. In some cases, an agency can charge more when the volume of a request requires "extensive use of the agency's information technology resources or of the clerical or supervisory personnel assigned to make copies or safeguard records," according to the Florida attorney general. In such cases, state law permits the agency to bill a services fee "for the inspection and copying of public records." Service charges are instructed to be reasonable, and based on actual labor costs of those people completing the request.

GOVERNMENT RECORDS

National Archives to Accept Only E-Records After 2022

The U.S. National Archives and Records Administration (NARA) has said it will stop accepting non-electronic records submissions from agencies by the end of 2022, according to a story on *FCW.com.* In a step to ensure a fully electronic archive, NARA released for public comment a draft of a strategic plan that said it will "no longer accept transfers of permanent or temporary records in analog formats and will accept records only in electronic format and with appropriate metadata."

A longtime federal records management expert, now with IBM, said the goals are "aggressive." According to Don Lueders, "the government must understand that agencies will not be able to meet that deadline using the same records management methodologies they've deployed for the last few decades ... agencies will have to begin to fully invest in more innovative technologies, such as cognitive systems, content analytics and big data solutions, if they hope to meet that deadline." E