INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

MARCH/APRIL 2014

Protecting Information Privacy Per U.S. Federal Law

Page 18

Procedures for Developing an Electronic File Plan

Page 28

An International Perspective on Protecting Personal Information

Page 34

Special in this issue:

hottopic

SECURING INFORMATION

Strategies for Cradle-to Grave Protection

INFORMATION MANAGEMENT

MARCH/APRIL 2014 **VOLUME 48 NUMBER 2**

DEPARTMENTS

4 **IN FOCUS** A Message from the Editor

6 **UP FRONT** News, Trends , and Analysis

FEATURES

18 **Protecting Information Privacy Per U.S. Federal Law**
Virginia A. Jones, CRM, FAI

24 **Procedures for Developing an Electronic File Plan**
Kathryn A. Scanlan, J.D., CRM

33 **An International Perspective on Protecting Personal Information**
Cherri-Ann Beckles

SPOTLIGHTS

38 **GENERALLY ACCEPTED RECORDKEEPING PRINCIPLES®SERIES**
The Principles in Practice in a New RIM Program
Julie Gable, CRM, CDIA, FAI

42 **RIM FUNDAMENTALS SERIES**
Elements to Be Assessed in a RIM Audit
ARMA International Standards Workgroup

CREDITS

47 **AUTHOR INFO**

48 **ADVERTISING INDEX**

INFORMATION MANAGEMENT

AN ARMA INTERNATIONAL PUBLICATION

Publisher: Marilyn Bier

Editor in Chief: Vicki Wiler

Contributing Editors: Cyndy Launchbaugh, Jeff Whited

Art Director: Brett Dietrich

Advertising Sales Manager: Elizabeth Zlitni

Information Management (ISSN 1535-2897) is published bimonthly by ARMA International. Executive, editorial, and advertising offices are located at 11880 College Blvd., Suite 450, Overland Park, KS 66210.

An annual subscription is included as a benefit of professional membership in ARMA International. Nonmember individual and institutional subscriptions are $140/year (plus $25 shipping to destinations outside the United States and Canada).

ARMA International (*www.arma.org*) is a not-for-profit professional association and the authority on managing records and information. Formed in 1955, ARMA International is the oldest and largest association for the records and information management profession, with a current international membership of more than 10,000. It provides education, publications, and information on the efficient maintenance, retrieval, and preservation of vital information created in public and private organizations in all sectors of the economy.

Information Management welcomes editorial submissions. We reserve the right to edit submissions for grammar, length, and clarity. For submission procedures, please see the "Author Guidelines" at *http://content.arma.org/IMM*.

Editorial Inquiries: Contact Vicki Wiler at 913.217.6014 or by e-mail at *editor@armaintl.org*.

Advertising Inquiries: Contact Karen Lind Russell or Krista Markley at +1 888.277.5838 (US/Canada), +1 913.217.6022 (International), +1 913.341.3742, or e-mail *Karen.Krista@ armaintl.org*.

Opinions and suggestions of the writers and authors of articles in *Information Management* do not necessarily reflect the opinion or policy of ARMA International. Acceptance of advertising is for the benefit and information of the membership and readers, but it does not constitute official endorsement by ARMA International of the product or service advertised.

Periodical postage paid at Shawnee Mission, KS 66202 and additional mailing office.

Canada Post Corp. Agreement No. 40035771

Postmaster: Send address changes to Information Management, 11880 College Blvd., Suite 450, Overland Park, KS 66210.

You will flip for it.

Get your hands on Zasio's latest version of Versatile Retention. With over 40,000 legal citations containing records retention requirements, this intuitive software will help you keep your retention schedule—whether domestic and/or international—up-to-date, easily accessible, and legally compliant.

ZASIO

800 513 8000
www.zasio.com

Principles for Protecting Your Organization's Information Assets

According to the Identity Theft Resource Center, nearly 58 million records were reported compromised in the United States last year – 40 million of them from Target customers during the Christmas shopping season.

At $188 per record, according to Ponemon Institute's "2013 Cost of Data Breach Study: Global Analysis," the direct cost of a data breach can have a huge impact on the bottom line. Other costs due to customers' loss of confidence could supply a knockout punch. Target reported that its 2013 fiscal fourth quarter profits were down $440 million due to its breach.

As a professional with responsibilities around safeguarding your organization's information assets, you'll find plenty of help in this issue of *Information Management (IM)* and the *Hot Topic* that is tipped inside.

In our cover article, Virginia Jones, CRM, FAI, provides an overview of U.S. federal privacy laws and their information governance implications. A comprehensive discussion of these laws is available in her ARMA International Educational Foundation report "Requirements for Personal Information Protection, Part 1: U.S. Federal Law," available at *www.arma.org/bookstore*.

Any organization that has international customers must also be concerned about other countries' legislation. Experian's "2014 Data Breach Industry Forecast" predicts that the rise of the cloud, which allows data to move seamlessly across borders, and the EU regulations that "will be enforced based on where the customer lives, rather than where the data is located," will lead to an increasing number of complex information-related violations. Google recently found out how expensive this can be, as France levied the maximum fine possible under French law – €150,000 ($205,000 U.S.) – against it for violating its privacy law.

Cherri-Ann Beckles covers this terrain in her feature article, "Managing Privacy in Recordkeeping Systems: An International Perspective." Among other advice Beckles gives, she writes, "Classification schemes that group record series containing personal data in logical, functional categories, could be used as the foundation on which sound data protection strategies are built."

For those developing or revising classification schemes, the case study written by Kathryn Scanlan, J.D., CRM, "Procedures for Developing an Electronic File Plan," will be a valuable resource. In addition to discussing the use of folders to control access, as Beckles suggests, the case study covers how to initiate the project, whom to involve, and how to design and implement the structure. It also provides a variety of sample file structures.

Auditing the RIM program is a critical aspect of ensuring that information is properly protected.

Our RIM Fundamental series article, which was excerpted from ARMA International's just-published *Auditing for Records and Information Management Program Compliance* (ARMA International TR 25-2014), identifies "The Elements to Be Assessed in a RIM Audit."

Of course, basing a RIM program on the Generally Accepted Recordkeeping Principles® (Principles) is the most comprehensive way to ensure information protection. Julie Gable, CRM, CDIA, FAI, developed two case studies that show the Principles in practice for new RIM programs.

We aim to provide practical help in every issue of *IM*. Please e-mail *editor@armaintl.org* to tell us what topics would be of the most value to you!

Vicki Wiler
Editor in Chief

Compliance monitoring is just a click away

Data protection regulations require organizations to monitor the qualifications and compliance of service providers that process sensitive information.

NAID just made this a lot easier!

Select the "**NAID AAA Notification**" link in NAID's member directory to receive emails announcing status changes to that member's certification and compliance qualifications.

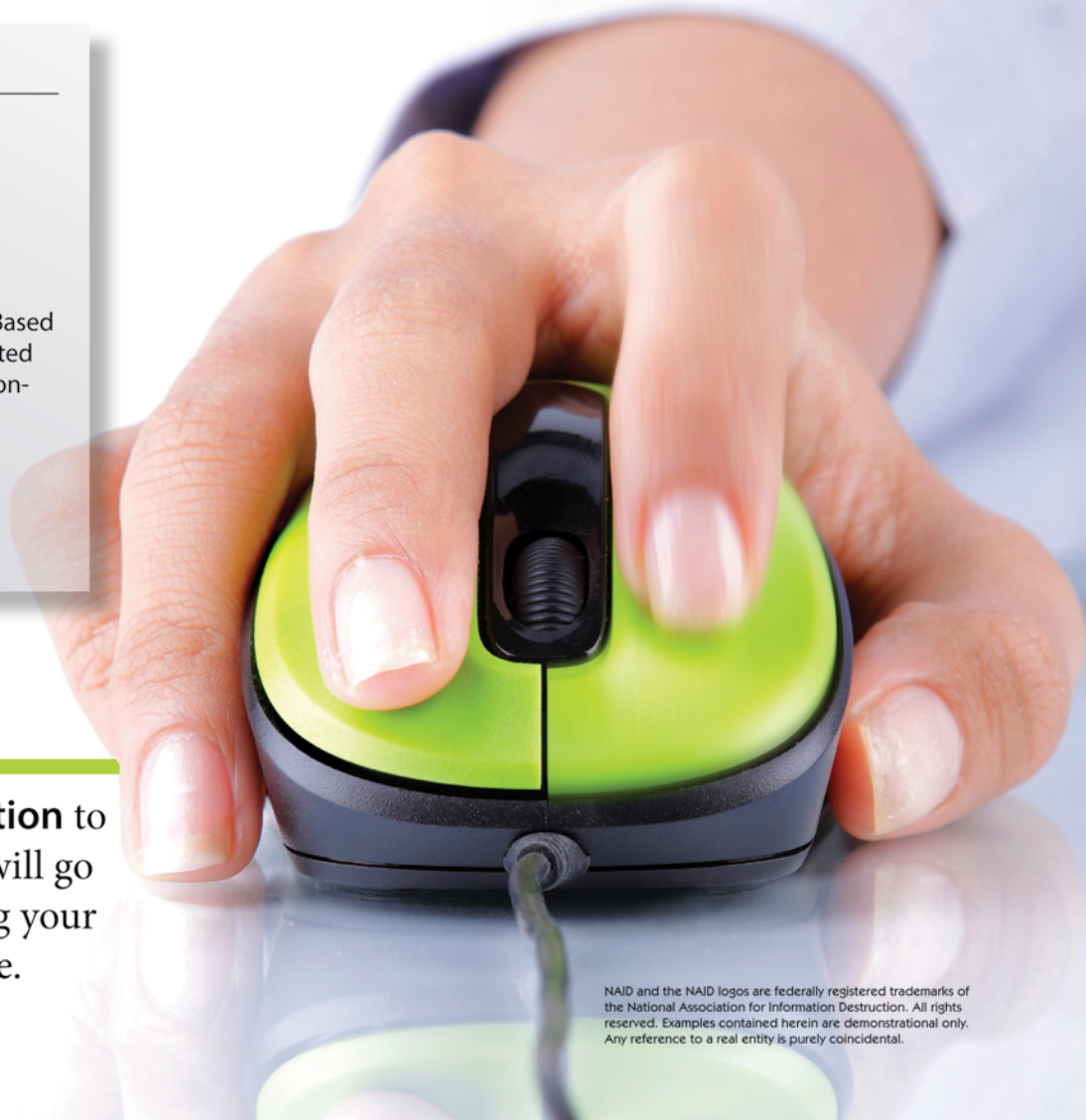
Data Destruction Co.

John Smith
123 S. 1st Ave.
Smalltown, AZ 85011
234-567-8901
www.123destruction.com

NAID CERTIFIED: Mobile and Plant-Based Operations Endorsed for Paper/Printed Media, Computer Hard Drive and Non-Paper Media Destruction

Original Date: January 16, 2008
Expiration Date: August 31, 2014

NAID AAA Notification



Visit **bit.ly/AAAnotification** to sign up. This simple act will go a long way in establishing your organization's compliance.

INFO SECURITY

Data Security Bills Await Action in U.S. Senate – Again

The recent Target and Neiman Marcus breaches have drawn a good deal of attention and provided extra fuel for the introduction of two bills in the U.S. Senate in early January.

Sen. Patrick Leahy (D-Vt.) cited the breaches when reintroducing S. 1897 – Personal Data Privacy and Security Act of 2014. The legislation would update the Computer Fraud and Abuse Act (CFAA) to allow the U.S. Justice Department to prosecute "significant" attempts of computer hacking and conspiracy to commit computer hacking. Key provisions in the bill include:

- Tough criminal penalties for individuals who intentionally or willfully conceal a security breach involving personal data when the breach causes economic damage to consumers
- A requirement for companies that maintain personal data to establish and implement internal policies to protect data privacy and security

The U.S. attorney general would also be required to report annually to Congress the number of criminal cases filed under the CFAA that were based solely on the defendant either accessing a nongovernmental computer without authorization or exceeding authorized access.

Leahy first introduced the bill in 2005 and has reintroduced it in the last four congressional sessions.

Less than two weeks later, Senators Roy Blunt (R-Mo.) and Tom Carper (D-Del.) introduced S. 1927 – Data Security Act (DSA) of 2014. This bill would replace a patchwork of state laws with a single set of requirements for public and private institutions to follow to prevent and respond to data breaches such as the one experienced by Target. The current bill builds on existing law such as the Gramm-Leach-Bliley Act of 1999.

If the financial establishment, retailer, federal agency, or other entity determines that sensitive information was compromised or may have been compromised, the DSA requires the organization to investigate the scope of the breach, the type of information compromised or potentially compromised, and whether the information could be used to cause an individual harm or to perpetrate bank fraud. If indeed the information was compromised and will cause harm, the organization must notify the appropriate federal government regulatory agency, law enforcement agency, and national consumer reporting agencies (if more than 5,000 individuals are affected), as well as the actual individuals whose information was breached.

Both bills are now in committee: Leahy's is in the Senate Judicial Committee (which Leahy chairs) and the Blunt-Carper bill is in the Committee on Banking, Housing and Urban Affairs.

CLOUD

Deadline Draws Near for Cloud Vendor Accreditation

Cloud service providers have until June to be accredited by the Federal Risk and Authorization Management Program (FedRAMP) if they want to continue to service U.S. federal agencies. FedRAMP is a government-wide, standardized approach to cloud security assessments and the continuous monitoring of the assessments and authorization. Federal agencies are allowed to use only cloud products and services that have been accredited by FedRAMP.

Maria Roat, the program's director within the General Services Administration, advised providers and federal agencies in December to work directly with the FedRAMP office and to get the review process underway soon because the process is a lengthy one. Providers working directly with FedRAMP should expect the process to take four to five months to complete, while those going it alone can expect it to take six months, according to an article on *TalkinCloud.com*.

The new accreditation program is a "do once, use many times" framework that will eliminate previous redundancies. Each agency currently manages its own security risks and provides ongoing security assessments and authorizations for each IT system it uses, even if that system is being used by other agencies.

FedRAMP is mandatory for all low- to medium-risk federal agency cloud deployments and service models; private deployments intended for single organizations and implemented fully within federal facilities are excluded.

E-DISCOVERY

Cloud Can Complicate Discovery

As the cloud grows, so does the number of places where individuals and corporations can store information that may be discoverable. Dropbox and Google Drive, both of which provide cloud storage, are reportedly two of the most popular free applications downloaded on Apple and Android devices.

A subpoena sent directly to one of these application providers will likely meet a motion to quash based on Title II of the Electronic Communications Privacy Act (also known as the Stored Communications Act or SCA). In "Discovery Difficulties Presented by Cloud Computing" in *The National Law Review*, J. Michael Nolan III, of Jackson Lewis PC, cited *Crispin v. Christian Augigier Inc.*, in which "the court found … that the SCA was passed by Congress to prohibit electronic communication service providers, such as Facebook and Myspace, from revealing the contents of communications electronically stored to anyone other than the addressee or other intended recipient." The better option may be to subpoena the plaintiff or defendant app user to obtain electronically stored information in the cloud

Nolan also wrote that in the ongoing case of *Integral Development Corp. v. Tolat,* the court ordered the defendant to return any proprietary information he possessed on any storage medium, including Dropbox. Dropbox opposed the subpoena based on the SCA, so the court ordered that the Dropbox data be produced directly to the defendant's attorney, who in turn was ordered to turn it over directly to the plaintiff's forensic expert to determine whether any relevant information had been uploaded, transferred, or deleted from the Dropbox account.

Because viewing the file on an end-user's computer would have changed the metadata, there were two options for providing this information: 1) Dropbox could generate a complete forensic report that included information about who accessed the cloud account or 2) the information could be reconstructed by accessing each computer that had synchronized with the account – a very labor-intensive (and therefore costly) alternative. The court chose the latter.

INFO SECURITY

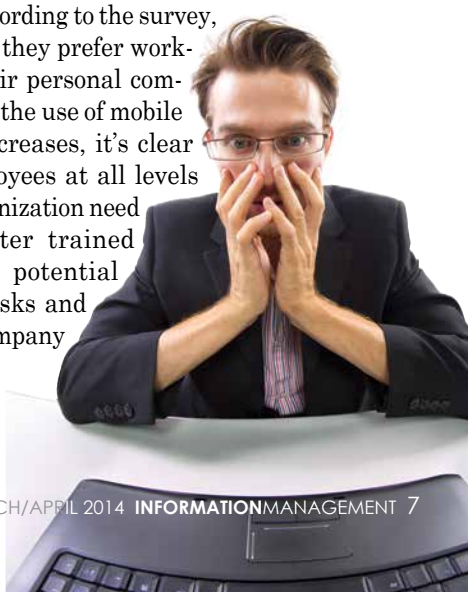
Senior Managers Behaving Badly

Oftentimes the biggest risk to your data's security comes from inside the company … from senior management.

"On the Pulse: Information Security Risk in American Business," a recent survey by digital risk managers at Stroz Friedberg, revealed that more than half of the respondents don't think U.S. companies are adequately securing their information (61%). Nearly three-quarters (73%) said a hacker could break into their employers' computer networks and steal their personal information.

Many respondents admitted to engaging in high-risk behaviors, such as uploading work files to their personal e-mail and cloud accounts (87%) and accidentally sending sensitive information to the wrong person (58%). Senior managers – who typically have high levels of access to valuable company information – were among the worst offenders. Indeed, 87% of senior managers said they upload work files to their personal accounts. More than half (51%) confessed that they have also taken files with them when leaving a previous job. These behaviors mean proprietary information could easily fall into the wrong hands.

The main reason senior managers upload work files to personal accounts, according to the survey, is because they prefer working on their personal computers. As the use of mobile devices increases, it's clear that employees at all levels in the organization need to be better trained about the potential security risks and current company policies.



INFO SECURITY

Data Backup and Migration Continue to Vex Enterprises

A new data management survey of 3,500 IT professionals revealed that even though the volume of data companies are managing is growing up to 40% annually, IT professionals lack confidence in their companies' data backup and migration processes. Almost 40% of the respondents said they've experienced data loss, and 83% either have no disaster recovery plan or are not entirely confident about their plan.

"We found that … companies are not protecting or backing up their data as often, for fears of security, manpower costs, or downtime," said Marty Gilbert, vice president of marketing for Vision Solutions, which conducted the survey. "Data recovery strategies are not evolving or being tested at nearly the rate they should be; with so many data breaches and disasters in the news, it's puzzling why corporations aren't moving at light speed to protect this data – the backbone of their business."

The survey also found that:

- Use of tape is the most predominant method of data backup (81% of companies) and is at a four-year high; meanwhile, software-based backup strategies are only inching up, barely above 50%.
- More than 60% of companies delayed a data migration, largely because of downtime (47%) and lack of resources (36%).
- Four out of five companies have never taken a complete business approach to migration or calculated the true cost of migration downtime.
- Only 39% of organizations test disaster recovery plans annually; 8% had no disaster recovery plan at all.

INTERNET

FCC Loses Battle for Net Neutrality

The U.S. Federal Communications Commission (FCC) may have lost the battle over "net neutrality" because of a recent court ruling, but it hasn't necessarily lost the war.

For some time, the FCC has been trying to ensure free and equal access to the Internet to all content providers, the same as it does for common carriers such as telephone companies. A U.S. appeals court, however, has ruled the FCC has been overstepping its authority because Internet providers are classified as broadband carriers, which are regulated differently.

The reaction to the court's decision has been varied: some have shrugged it off while others worry it could be the end of the Internet as we know it. Still others point out that even though the FCC lost this particular battle, it won an even bigger one because the court reinforced the commission's contention that Congress has given it the authority to regulate the Internet.

"While the court deemed that the FCC's Open Internet rules were based on faulty logic, it gave the agency a blueprint to revise its argument so that the rules would stick," summarized Maggie Reardon in a recent *CNet* article.

Judge Laurence Silberman of the U.S. Court of Appeals for the District of Columbia Circuit dissented in part to the court's ruling. While he agreed the FCC could not regulate broadband services under common carrier rules, he disagreed with the other justices' interpretation of the FCC's authority for regulation. He added that the court's decision grants the "FCC virtually unlimited power to regulate the Internet," which was not the intent of Congress when it passed the Communications Act.

FCC Chairman Tom Wheeler

responded that the FCC's authority to regulate broadband networks had always been the intent of Congress, and he would make sure the agency does not use its powers gratuitously.

"No one got what they wanted out of this decision," said Harold Feld, senior vice president with Public Knowledge, a nonprofit whose mission is to preserve the openness of the Internet. "Confusion over the proper role of the FCC is greater than ever."

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 shows that you have the experience and expertise that others may lack, and skills to show that you are a leader in the RIM profession.

For more information about becoming a Certified Records Manager, contact (518) 463-8644 or visit www.icrm.org

ICRM®
Institute of Certified Records Managers

E-DISCOVERY

Some U.S. Courts Seeking Discovery Details

Several recent federal cases indicate that U.S. courts are becoming increasingly engaged in assessing the details of e-discovery, such as whether the correct search terms or custodians have been identified, according to Daniel J. Weiss, a partner at Jenner & Block, in a recent *Lexology* article. He cited the following three cases as evidence:

American Home Assurance Co. v. Greater Omaha Packing Co.: The court ordered a party that had produced very few e-mails to "disclose the sources it has searched or intends to search and, for each source, the search terms used."

Swanson v. ALZA Corp.: The court ordered a party to apply several search terms (including Boolean operators) to a database of collected electronic information and produce the results to the requesting party. The court also reviewed the requested search terms in detail and determined that about half of the terms should be applied even though more than 600,000 pages of electronic documents had already been produced.

Banas v. Volcano Corp.: The court reviewed a party's e-discovery effort and faulted the party for not searching the e-mail of several custodians.

INTERNET

Global Commission Tackles Internet Governance

International concern over the reports of mass online surveillance by the United States and some of its allies was a hot topic of discussion in January at the World Economic Forum in Switzerland. In response, The Centre for International Governance Innovation and the Royal Institute of International Affairs (Chatham House), two independent global think-tanks, announced the launch of the Global Commission on Internet Governance.

The 25-member group, chaired by Sweden's foreign minister, Carl Bildt, is undertaking a two-year investigation into the various ways governments use Internet data. Its goal is to produce "a comprehensive stand on the future of multistakeholder Internet governance."

"In most countries, increased attention is being given to all the issues of net freedom, net security, and net governance," said Bildt. "The rapid evolution of the net has been made possible by the open and flexible model by which it has evolved and been governed. But increasingly this is happening as issues of net freedom, net security, and net surveillance are increasingly debated. Net freedom is as fundamental as freedom of information and freedom of speech in our societies."

The commission will investigate a wide range of topics within four key themes:

1. *Enhancing governance legitimacy* – including regulatory approaches and standards
2. *Preserving innovation* – including critical Internet resources, infrastructure, and competition policy
3. *Ensuring rights online* – including establishing the principle of technological neutrality for human rights, privacy, cybercrime, and free expression
4. *Avoiding systemic risk* – including establishing norms regarding state conduct, cybercrime cooperation, and proliferation and disarmament issues

"Internet governance is too important to be left just to governments," said Patricia Lewis, research director of Chatham House's International Security Department. "The Internet is a fundamental part of the global economy and how we manage its future will be decisive in facilitating development for all."

The commission comprises technology experts from various sectors, as well as academics and policy and government specialists. Its members include Sir David Omand, the first security and intelligence coordinator for the United Kingdom and a former director of the UK's Government Communications Headquarters (a British intelligence agency), and Michael Chertoff, a former secretary of the U.S. Department of Homeland Security.

Introducing the official

Information Governance Assessment

Based on a large body of generally accepted practices, international- and national-level standards, and legal and regulatory requirements, the **Information Governance Assessment** provides an authoritative and objective means of measuring your organization's information governance (IG) program's maturity.

The **IG Assessment** can be used to:

- Identify your organization's IG maturity
- Track deficiencies by principle and overall score
- Monitor the progress of risk mitigation efforts
- Assess the sufficiency of IG training and documentation

Find out how the
IG Assessment
can work for you!

Visit ***www.arma.org/assessment***
Contact: **Elizabeth Zlitni**
+1 888.279.7378 (U.S., Canada)
+1 913.217.6015 (international)

CLOUD

Copyright Violations Shut Down Cloud Storage Site

One of the most used file-sharing sites on the Internet, Hotfile, went dark in early December as a result of copyright infringement charges filed against it by the Motion Picture Association of America (MPAA). Hotfile was facing a possible $500 million fine had the case proceeded to court; instead the two parties settled for $80 million. The deal, approved by the U.S. District Court for the Southern District of Florida, required Hotfile to start using "digital fingerprinting" technology to filter copyright-infringing content or shut down its operations.

Implementing filtering techniques is a drastic step, but not an unusual one in the file-hosting business, reported *TorrentFreak*, an online publication focused on copyright and other issues related to digital file sharing. *TorrentFreak* noted that cyberlocker MediaFire uses digital fingerprinting technology and remains the most-used storage site on the Internet.

Hotfile, however, chose to shut down its operations rather than implement the filtering technology. It did so within hours of the settlement announcement and without first notifying its millions of individual and business users. Those users who hadn't backed up their virtual site to an alternate site were left adrift.

E-DISCOVERY

No Major E-Discovery Issues in 2013

Looking back, it was all quiet on the e-discovery front last year. "No earth-shattering opinions, no imprisoned spoliators, and barely a whimper from reported decisions related to parties' chosen form of production," observed Cecil Lynn, director of e-discovery and technology at eBay, and Lauren Schwartzreich, e-discovery counsel at Littler Mendelson, in a recent *Law Technology News* article.

"Perhaps the bench and bar are getting more sophisticated and technology savvy," they hypothesized. "Or perhaps the courts implicitly recognized the current state of flux, what with the proposed amendments to the Federal Rules of Civil Procedure (FRCP) that specifically address [electronic data discovery]. Or possibly, the industry is evolving from what was once considered cutting-edge and novel to what is emerging as best practices."

As in previous years, judges reinforced their expectation of cooperation with the electronic data discovery (EDD) competency. The Eastern District of Michigan went so far as to develop a "Meet and Confer Checklist and Model Order Related to the Discovery of Electronically Stored Information."

The courts also continued to focus on the parties' efforts to streamline discovery and consider the cost and burdens associated with their discovery requests, as well as on cost shifting, not only between parties but also for expenses incurred by non-parties. Even when the non-party and a party share an interest in the subject matter of litigation – a factor that weighs against cost shifting – one court held that the sheer volume of discovery tipped the balance in favor of shifting EDD-related expenses.

In 2012 many in the industry predicted there would be more movement in the use of predictive coding in 2013, but there was relatively little discussion of the use of technology-assisted document review. The authors noted that case law underscored that traditional keywords and document review may appropriately be used in conjunction with technology-assisted review.

"While 2013 did not produce any 'bombshell' e-discovery opinions," they concluded, "it did underscore that EDD standards are far from settled, including because of variances among circuits (and oftentimes individual judges). Whether the proposed amendments to the FRCP that address EDD will bring more uniformity to the field remains an open issue for 2014."

CYBERSECURITY

Financial Exchanges Unite Against Hackers

The World Federation of Exchanges (WFE) has decided it's time for the global financial exchanges to work together to thwart cyber attacks. The federation recently announced the formation of the Cyber Security Working Group, the exchange industry's first cybersecurity committee. Its mission is to help protect global capital markets by collaborating on best practices for protecting their infrastructures.

More than half the world's exchanges were victims of cyber crime in 2013, according to a paper published last summer by the WFE and the International Organization of Securities Commissions. Fortunately cyber attacks on stock markets have thus far focused on non-trading-related online services and websites and haven't come close to knocking out critical systems or trading platforms. Furthermore, most of the exchanges are confident in their protocols and preparedness.

That being said, 83% of the exchanges agree that cyber crime in securities markets should be considered a systemic risk because of its potential effect on confidence and reputation, market integrity and efficiency, and financial stability. The exchanges are united in their belief that a broader, system-wide response is needed.

Mark Graff, NASDAQ's chief information security officer, will chair the committee, which will include representation from more than a dozen exchanges and clearinghouses around the world.

CLOUD

China Is New Cloud Frontier

Many in the cloud industry are banking on China. In December, Amazon made headlines by announcing that it will extend its cloud-computing services – Amazon Web Services (AWS) – to China in 2014. *Xinhuanet.com* reports that AWS signed a memorandum of understanding with Beijing and Ningxia for jointly constructing and developing cloud services for Chinese clients. The business office will be located in Beijing and the data center in Ningxia. The AWS China deal is part of Ningxia's plan to build a cloud base that eventually will be able to house 1 million servers.

Amazon's entry into the China market sparked an impressive flurry of activity. Only hours before Amazon publicized its plans, Allyun – the cloud-computing arm of China's e-commerce giant Alibaba Group Holding – announced it was cutting its cloud service prices by as much as 35%. Shortly after Amazon's declaration, IBM said it would be teaming up with a local partner to provide cloud services to Chinese enterprises. The country's two largest mobile operators – China Mobile and China Unicom – announced earlier in December that they had begun construction of cloud computing facilities in Guizhou Province.

Although many Chinese companies currently offer cloud services, only Allyun comes close to AWS in size and is expected to feel the pressure of its entry in the Chinese market. Qian Lili, an analyst with Analysys International, told Xinhuanet that AWS China's arrival may not completely change the market landscape, but it will likely push out some of the small players. Other analysts contend the National Security Agency spying scandal could adversely affect AWS China's influence.

CYBERSECURITY

Kroll: Organizations Get Serious About Security in 2014

Kroll's recently released 2014 Cyber Security Forecast highlights seven trends that indicate changing tides in cyber standards and the need for organizations to take stronger actions to protect themselves from financial, legal, and reputational risks.

1. **Security frameworks such as the National Institute of Standards and Technology (NIST) Cyber Security Framework will become *de facto* standards.** "This trend will move the United States in the direction of the EU, where there is a greater recognition of privacy as a right," said Alan Brill, senior managing director at Kroll. Whether compulsory or unstated, these standards will drive decision-making in organizations that want to protect themselves from shareholder lawsuits, actions by regulators, and other legal implications.
2. **The data supply chain will continue to challenge even the most sophisticated organizations.** Contracting with third parties to store or process data will continue to be commonplace, making it imperative that companies closely vet their subcontractors as to their technical and legal roles and responsibilities in the event of a breach. This requires technical, procedural, and legal reviews.
3. **The malicious insider will remain a serious threat but will become more visible.** Kroll predicts that in 2014 a significant number – if not almost half – of data breaches will come at the hands of people on the inside. However, as the federal government and individual states add muscle to privacy breach notification laws and enforcement regimes, the hidden nature of insider attacks will become more widely known.
4. **Corporate board audit committees will take a greater interest in cybersecurity risks and how the organization plans to address them.** Data breaches pose significant threats to the organization's reputation, compliance efforts, and financial well-being, putting it squarely in the lap of corporate audit committees. "As corporate boards carry out their fiduciary responsibilities, they must also protect the company from possible shareholder lawsuits that allege the company's cyber security wasn't at a level that could be reasonably viewed to be 'commercially reasonable' and that incident response plans weren't in place to mitigate the risk," said Brill.
5. **Sophisticated tools will enable smart companies to quickly uncover data breach details and react faster.**
6. **New standards related to breach remediation are gaining traction and will have a greater impact on corporate data breach response.** Credit monitoring will no longer be the gold standard in breach remediation in 2014, as lawmakers, consumer advocates, and the public at large continue to question the relevancy and thoroughness of this as a stand-alone solution. The Federal Trade Commission and states like California and Illinois are already suggesting a risk-based approach to consumer remediation – one that matches remedy to individual risk based on the unique circumstances of a breach.
7. **As more organizations adopt the cloud and BYOD, they will be held accountable for implementing policies and managing technologies.**

E-DISCOVERY

Copyright Infringement on the Internet

400%
the increase in copyright infringement cases from 2012 to 2013.

235M
Number of takedown requests Google received from copyright holders in 2013.

50M
Number of takedown requests Google received in 2012.

10M
Number of takedown requests Google received in 2011.

A significant number of the requests came from the music industry's anti-piracy groups BPI and RIAA (41.7 million and 30.8 million, respectively).

CYBERSECURITY

Prediction for 2014: Expect More Cybersecurity Challenges

Coalfire, an independent IT security business, welcomed the new year with its predictions for the top cybersecurity trends expected in 2014. Organizations should be prepared to identify or respond to the following emerging risks:

1. **There will be a significant security breach at a cloud service provider that causes a major outage.** Businesses must evaluate the risk within their third-party cloud service provider systems to protect sensitive information, including trade secrets and intellectual property.
2. **The migration from compliance to IT risk management will accelerate.** Risk and compliance management firms need to be more in tune with their clients' business needs – more proactive than reactive.
3. **Emerging threats will shift security programs from static boundary protection to more proactive monitoring and response programs.** Expect more virulent types of attacks that will be significant enough to require more proactive monitoring and response.
4. **There will be a significant increase in malware for Android phones, and malware will begin to affect iPhones, too.** Smartphones are woefully unprotected from malware as users harbor a false sense of security.
5. **The number of data breaches in health care caused by business associates (BAs) will increase dramatically because of the Omnibus Rule.** The Omnibus Rule required that all BAs be HIPAA compliant by September 23, 2013. Unfortunately, many organizations don't know they are BAs and are ignoring the requirements, increasing their vulnerability.

E-DISCOVERY

Court: 'Saved Everything' Defense Not Good Enough

If you think you don't need to issue a formal legal hold because your policy is to save everything, think again.

A California magistrate judge recently reminded a party of that. It seems the party neglected to issue a legal hold when it became apparent that litigation was likely. As it turns out, e-mails from key players were destroyed in the absence of a legal hold. The defendant later argued that it had a company-wide "no documents are to be deleted" policy that was equivalent to a legal hold. The judge disagreed.

"Although defendants argue that there was no need for a litigation hold because of their document retention policy, it is obvious that defendants' document retention policy did not prevent documents from being destroyed," the court said. "Further, defendants did not have a back-up system to prevent the destruction of documents…."

The court approved the adverse inference instructions and ordered monetary sanctions in the form of attorney fees and costs.

BYOD

Forrester: Act Now to Stamp Out BYOD Risks

If you can't beat them, join them." That adage fairly summarizes the results of a recent Forrester study of the legal implications related to a bring your own device (BYOD) policy, "Navigating the Legal and Compliance Applications of BYOD." According to a January 13 Forrester blog by David Johnson, a co-author of the study, technology attorneys participating in the study agreed that "once you learn that BYOD is happening in your organization, you have a legal obligation to do something about it, whether you have established industry guidance to draw on or not." In other words, you must take action to minimize the risk.

If only it were as easy as it sounds. As pointed out by Johnson:

- The more restrictions you put in place, the more incentive people will have to work around them and the more sophisticated and clandestine their efforts will be.
- There is no data leak prevention tool for the human brain, so arguably the most valuable and sensitive information walks around on two legs and leaves the building every night. Accepting this is important for keeping a healthy perspective about information risk on employee-owned devices.

Despite the challenges, organizations need to address the issue. Intellectual property misuse and accidental data loss are the top BYOD risks cited by Forrester. Patent, trademark, and copyright infringement may be very common, wrote Johnson, but they also are next to impossible to police with technical controls.

For example, Johnson wrote, if attorneys can prove that employees are using software that is not properly licensed for the organization's business purposes, it can be considered "willful and illegal misuse of someone else's property," and the organization can be held liable for past licensing fees and damages.

According to Charles F. Luce, Jr., partner at Moye White in Denver, it doesn't matter whether the employee or the organization owns the device on which the software is installed. Charles Gray, practice manager for Accuvant's risk and compliance business, added that any device used in a regulated business needs to adhere to the same regulations and industry standards as company-owned equipment.

Unfortunately, there is little specific guidance for BYOD policies and technical controls. Johnson noted that auditors tend to look to the U.S. National Institute of Standards and Technology's (NIST) technical control specifications for guidance, but "it's often subjective because devices and platforms evolve so quickly that it renders the guidance obsolete almost immediately."

Effective BYOD governance starts with a clear policy and education. Johnson stated that a signed BYOD agreement with each employee, along with adequate education on the risks and employees' responsibilities, are the absolute minimum controls that should be in place. He also recommends electronically enforcing policies for employees incapable or unwilling to do their part.

"A viable BYOD strategy addresses culture, responsibilities, education, policy, and technical controls. It recognizes the value that BYOD brings to employee engagement and performance and features a clear agreement between the organization and each BYOD employee that outlines what each is responsible for. Technology's role is to help foster safe behaviors, control information access, and verify ongoing compliance – all without getting in the way of creativity, productivity, collaboration, or other daily activities," Johnson wrote.

Forrester suggests creating a technology approach that promotes engagement while enforcing the policy. This means keeping employee-owned devices off of the corporate trust network while allowing access to information through secure proxies and interfaces. In regulated environments, it also means sensitive data is never stored on employee-owned devices, but in less stringent environments it can mean simply controlling access to systems of record such as customer databases to prevent anyone from walking away with a data dump.

CYBERSECURITY

NIST Presents Cybersecurity Standard

In February the U.S. Commerce Department's National Institute of Standards and Technology (NIST) released the first version of the "Framework for Improving Critical Infrastructure Cybersecurity." It was presented exactly one year after President Obama issued an executive order directing the agency to collaborate with industry to create a voluntary framework for managing cybersecurity-related risk.

According to NIST, the framework uses a common language to manage cybersecurity risk in a cost-effective way based on business needs without placing regulations on businesses. It focuses on using business drivers to guide cybersecurity activities and on considering cybersecurity risks as part of the risk-management process.

Per the executive order, the framework also provides guidance on how organizations can incorporate the protection of individual privacy and civil liberties into the program.

NIST has stressed that the framework is not a one-size-fits-all approach to managing cybersecurity risk. "Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the framework will vary."

The framework is generally regarded as a good first step, but some don't think it goes far enough. Ann M. Beauchesne, vice president of national security and emergency preparedness for the U.S. Chamber of Commerce, stated: "[T]he Chamber believes that the framework will be fundamentally incomplete without the enactment of information-sharing legislation. Businesses need policies that foster public-private partnerships – unencumbered by legal and regulatory penalties – so that individuals can experiment freely and quickly to counter evolving threats to U.S. companies."

Greg Nojeim, director of the Center for Democracy and Technology's Project on Freedom, Security and Technology said: "The framework will be useful to companies and their privacy officers, because it will remind them that processes should be put in place to deal with the privacy issues that arise in the cybersecurity context. However, we are concerned that the privacy provisions in the framework were watered down from the original draft. We would have preferred a framework that requires more measurable privacy protections as opposed to the privacy processes that were recommended."

NIST noted that the framework "is a living document and will continue to be updated and improved as industry provides feedback on implementation." **END**

Protecting Information Privacy Per U.S. Federal Law

Virginia A. Jones, CRM, FAI

Protecting the privacy of internal and external customers is a critical responsibility for those with records and information management responsibilities. This article provides a high-level overview of privacy issues and broadly applicable U.S. federal laws governing them.

Business and government entities must understand and apply increasingly complex laws and regulations to protect the data and records of their customers and citizens. Compliance with U.S. personal information protection laws is often difficult due to the number and interrelationship of federal and state laws and regulations that affect or relate to these issues.

In 2013, nearly 58 million records were reported compromised in the United States according to the Identity Theft Resource Center. With increased collection of data and easier methods of collection, protecting personal information has become a big issue in today's business and government environment.

Contributing Factors to Data Breaches

There is now prolific and far-reaching collection and distribution of personally identifiable information (PII) due to increased use of the Internet for a number of activities such as conducting business meetings, interacting with government, personal and business banking and other financial transactions, data vaulting, shopping, socializing, and even attending classes.

Online Transactions

There is a generational trust of and reliance on computerized data with a desire for easier and quicker methods to conduct these actions. The need to more quickly access information or activities leads many to submit personal information online and, in doing so, leave themselves open to unauthorized access to their personal information.

Often online submittal of PII either explicitly or implicitly authorizes data sharing between entities. While several U.S. federal laws require an "opt-out" opportunity to be provided by online businesses to allow consumers to choose not to have their data shared (or even marketed), it is not always obvious to the user that a choice exists or, in many cases, the user does not pay attention to the choice.

Data Sharing

To increase efficiency, data is frequently shared by those who collect it. In the private sector, acquired data is often shared or sold. Acquisitions and mergers of business entities also might provide useable data to disparate sectors of business. For example, an entertainment company might buy a mortgage company, giving it access to personal information it would not otherwise collect. In the government sector, collected data is often shared between agencies to expedite processes and to determine eligibility for a variety of programs and benefits. In fact, the EGovernment Act of 2002 encourages the sharing of various data between certain federal agencies when appropriate.

Ease of Access

Exposure to privacy information breaches is compounded by the ease of access to personal information. The use of Google, Yahoo, AnyWho, or other search engines and locators makes it easier to obtain the personal information of others through increased hacking into computer systems, Internet phishing, and just plain stealing hard media or information from hard media, such as credit cards, credit card statements, checks, and other documents containing PII thrown in the trash or recycling. This proliferation of accessible personal information has resulted in misuse of personal information by the unscrupulous through identity theft, spamming, stalking, or preying.

Increase in Social Security Numbers Issued

The most overused personal information is the Social Security Number (SSN). Originally established in 1935 by the federal government as part of the Social Security program requiring employees to contribute a portion of their earnings toward a national retirement fund, the issuance of SSN was expanded in the 1970s to include newborns and non-employed residents in the United States.

With the majority of the population having a centrally recorded identification number, the SSN became an accurate method of uniquely identifying individuals. Businesses and government required the SSN for a number of services and benefits, even for accepting personal checks. One of the earliest abuses of personal privacy was the stealing and misuse of SSN.

As breaches and misuse of personally identifiable information became more prevalent, laws became necessary to prevent misuse, to prevent unauthorized sharing, and to ensure protection of individual personal information. A variety of federal laws have been enacted that require organizations to be responsible for the privacy of certain records and data.

Right to Privacy Established

In Public Law 93-579, enacted in 1974 as the Privacy Act, Congress found that the right to privacy is a personal and fundamental right protected by the Constitution of the United States. The need for information privacy encom-

passes all segments of the population.

Citizens are affected by government data collection and dissemination, and a number of privacy laws apply directly to this sector. Employees are affected by employer data collection and dissemination and the use made of the data by employers. Customers/consumers are affected by business data collection and dissemination and how well the data may be protected. Medical care recipients are affected by data collection and dissemination by medical care, medicine, and medical supplies providers and how the data is protected, shared, and accessed.

There is no one definition of "personally identifiable information" in U.S. federal law. Where a definition is listed, there is some variance from law to law. For the most part, definitions of the term are based, in part or in whole, on the definition set by the Federal Trade Commission (FTC) in "Online Profiling: A Report to Congress":

> Data that can be linked to specific individuals, and includes but is not limited to such information as name, postal address, phone number, e-mail address, social security number and driver's license number.

Depending on the act, PII can also include medical information, financial information, political affiliation, educational records, social organization affiliation, video viewing preferences, and religious affiliation.

There is agreement in privacy laws in the need to protect the SSN. At least five federal laws restrict the use or disclosure of SSN, including the Fair Credit Reporting Act, the Fair and Accurate Credit Transactions Act, the Graham-Leach-Bliley Act, the Drivers Privacy Protection Act, and the Health Insurance Portability and Accountability Act.

A 2007 memorandum from the Office of Management and Budget, required federal agencies to review their use of SSN in their systems and programs to identify superfluous collection or use of SSN and to eliminate unnecessary collection and use by mid-2010. Agencies were also asked to participate in government-wide efforts to explore alternatives to the SSN as a personal identifier for both federal employees and in federal programs.

Classes of Privacy

According to *Information Privacy, Official Reference for the Certified Information Privacy Professional (CIPP)* by Peter P. Swire, CIPP, and Sol Bermann, CIPP, privacy can be categorized into four classes.

- *Information privacy* is concerned with establishing rules that govern the collection and handling of personal information, including credit information, medical data, and government records.
- *Bodily privacy* is focused exclusively on a person's physical being and any invasion thereof, such as genetic testing, drug testing, or body cavity searches.
- *Territorial privacy* is concerned with placing limitations on the ability of one to intrude into another individual's environment. This may be the home, workplace, or public space and can extend to an international level. Invasion typically comes in the form of video surveillance, ID checks, and use of similar technology and procedures.
- *Communication privacy* encompasses protection of the means of correspondence, including postal mail, telephone conversations, electronic mail, and other forms of communicative behavior and apparatus.

Citizens are affected by government data collection and dissemination.

Impacts on RIM

Information privacy is the class that directly relates to records and information management (RIM). Communication privacy also impacts RIM through correspondence issues. The records management impacts of the laws and regulations discussed in this paper are based on the records management life cycle concept – from creation/receipt of the records and data to final disposition. Although not all laws have all elements, privacy law can impact records creation, file management for both active and inactive records, records protection, records access, and records retention and disposition.

Recordkeeping Requirements

The impact on records creation can be either specific or implied. Wording such as "a record shall be kept of," "a report shall be generated," "a written policy shall be created," or "data about [something] shall be collected," is frequently included in the laws.

For example, the Family Educational Rights and Privacy Act requires a record to be kept of all access to or dissemination of a student's records, and the Privacy Act of 1974 requires agencies to keep an accounting of certain disclosures of personal data.

Many of the laws require the generation of reports regarding PII disclosures or breaches. Some laws include wording that directs or implies how the record file should be managed. The Americans with Disabilities Act, for example, states specifically that medical records must be filed separately from other records in an employee file. The Privacy Act of 1974 requires agencies to allow a data subject to review a record about themselves and to "have a copy made of all or any portion thereof in a form comprehensible to him."

The requirement to protect records and data containing PII is implied, and often explicit, in every privacy law. For example, the Cable Communications Policy Act requires cable operators to take such actions as are necessary to

THERE'S NO SUCH THING AS TOO MUCH INFORMATION

Study Information Governance at San José State University
Convenient, flexible, 100% online graduate program

The volume of digital data is increasing exponentially, and many organizations are in need of updated and simplified content management infrastructures. That's why the exclusively online Master of Archives and Records Administration (MARA) program at San José State University focuses on preparing information governance professionals to solve these complex management challenges. As a MARA graduate student, you'll learn to use sophisticated technologies to organize, preserve, and provide access to a growing volume of records and digital assets. And, with degree in hand, you'll be ready to take on leadership roles in the rapidly expanding field of electronic records and digital asset management. **Join us today!**

Applications due April 1. Apply Today!

"The greatest strengths of the MARA program are the small class sizes, online learning tools, and fantastic instructors."

– Spring 2013 graduate

SAN JOSÉ STATE UNIVERSITY | SCHOOL OF LIBRARY AND INFORMATION SCIENCE

Let the learning begin:
slisweb.sjsu.edu/mara

Broadly Applicable U.S. Federal Privacy Laws and Regulations

Name — Year Enacted	Scope	Applies to
Children's Online Privacy Protection Act (1998)	Governs personal information collected online that can serve to identify an individual child	Entities that collect personal information online (including websites or online services and persons who have an interest in the online collection of children's personal information)
Computer Fraud and Abuse Act (1986, amended 1990)	Governs unauthorized access to a protected computer to obtain information	Anyone accessing a computer to obtain information
Electronic Communications Privacy Act, Title 1 Wire And Electronic Communications Interception And Interception Of Oral Communications (1968)	Regulates the interception of wire, oral, and electronic communications to protect the privacy of innocent persons	Any employee or agent of the United States or any state or political subdivision thereof and any individual, partnership, association, joint stock company, trust, or corporation
Electronic Communications Privacy Act – Title II Stored Electronic Communications Privacy Act (1986)	Regulates the accessing of stored electronic communications	Any employee, or agent of the United States or any state or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation
Fair Credit Reporting Act (2003)	Addresses the use and disclosure of an individual's credit report information, including the use of credit report information by employers in making employment decisions	Consumer reporting agencies and persons who use consumer reports from such agencies, persons who furnish information to such agencies, and users of information that are subject to section 1681m
Fair and Accurate Credit Transactions Act (Amends the Fair Credit Reporting Act) (2003)	Governs opt-out notices, use of credit report information by employers in making employment decisions, and disposal of consumer credit information	Consumer reporting agencies and persons who use consumer reports from such agencies, persons who furnish information to such agencies, and users of information that are subject to section 1681m
Family Educational Rights & Privacy Act & Privacy Act	Governs privacy of student's education records	Applies to educational agencies or institutions
Financial Services Modernization Act (aka Gramm-Leach-Bliley Act) (1999)	Governs the privacy and security of personal financial information	Financial institutions
Health Insurance Portability & Accountability Act (1996)	Governs the disclosure of protected health information	Health plans, healthcare clearinghouses, and healthcare providers
Privacy Act of 1974	Governs third party access to personal information maintained by the federal government	U.S. federal executive branch
Computer Matching & Privacy Protection Act (Amends the Privacy Act of 1974) (1988, amended 1990)	Governs requirements federal agencies must follow when matching information on individuals with information held by other federal, state, or local agencies	U.S. federal executive branch
Privacy Protection Act (1980)	Governs the search for or seizure of work product or documentary materials in connections with dissemination to the public a newspaper, book, broadcast, or other similar form of public communication	Government officer or employee
Right to Financial Privacy Act (1978)	Governs access to financial records of any customer of a financial institution	Any U.S. government agency or department
Safe Harbor Data Privacy Framework (2000)	Governs transfer of personal information between the E.U. and third countries	Any organization subject to FTC jurisdiction wanting to do business with the EU, U.S. air carriers and ticket agents subject to Dept. of Transportation
Uniting & Strengthening America by Providing Appropriate Tools Required to Intercept & Obstruct Terrorism Act (aka USA Patriot Act) (Amends a number of statutes) (2001, amended 2006)	Governs the deterrent and punishment of terrorist acts in the United States and around the world and enhances law enforcement investigatory tools	Law enforcement, businesses that provide financial and communications services

prevent unauthorized access to PII by a person other than the subscriber or cable operator. Most privacy laws set penalties for failure to protect PII or for misuse or unlawful disclosure of PII.

Rights to Access Personal Info

Almost every privacy law sets some requirement for access to personal information and data. This includes requirements for who may or may not access the data, who may or may not receive the data, and the right of a *data subject* – the person the collected data is about – to inspect records and to correct records about themselves.

The Privacy Act of 1974, for example, requires an agency to allow data subjects to:

- Access their record or any information pertaining to them that is contained in the system
- Review their record
- Request amendment of their record
- Request a review of a refusal to amend their record and to clearly note any portion of the record that is disputed and, in any disclosure, provide copies of the dispute and the reason(s) for not making the requested amendments

The Fair Credit Transaction Act requires consumer reporting agencies to disclose to data subjects all information in their file (with some exceptions) at the time of request and the right of data subjects to dispute incorrect information and require it be corrected.

Some privacy laws address permitted selling or disclosure of personal data. The Driver's Privacy Protection Act, for example, allows an authorized recipient of personal information in a motor vehicle record to resell or re-disclose the information only for a use permitted under the act, generally for motor vehicle-related reasons such as safety and theft, emissions, product alterations or recalls, and performance monitoring of vehicles. Highly restricted personal information cannot be disclosed without the permission of the data subject.

Data Retention

Some of the privacy laws set requirements for records or data retention and/or records or data disposition, although most retention requirements are usually covered in rules and regulations that are part of the Code of Federal Regulations.

Those laws that do cover retention or disposition include provisions on how long to retain records or data, how to dispose of records or data containing PII, or when to dispose of the records or data.

For instance, the Stored Electronic Communications Privacy Act (Title II of the Electronics Communications Privacy Act) requires records authorizing disclosure of a subscriber or consumer record be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

The Driver's Privacy Protection Act requires any authorized recipient that resells or re-discloses motor vehicle information to keep, for a period of five years, records identifying recipients of the information and the permitted purpose for which the information will be used.

Examples of disposal requirements include the Fair and Accurate Credit Transaction Act which requires federal banking agencies, the National Credit Union Administration, and the FTC to issue final regulations requiring the "proper disposal" of consumer information or any compilation of consumer information derived from consumer reports for a business purpose.

The Cable Communications Policy Act requires a cable operator to destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information as allowed by law or pursuant to a court order.

Some of the privacy laws set requirements for records or data retention.

Responsibility for Privacy Protection

Because information privacy is integral to RIM, it should be the responsibility of the records manager (or the person whose function includes records management) to assist or advise in the establishment of processes, procedures, and monitoring for compliance with applicable laws and regulations.

Records managers should be aware of laws pertinent to their organizations, the requirements of those laws, and any pertinent rules or regulations generated under the authority of the laws. All RIM procedures and policies should include provisions for protecting personally identifiable information.

Learn More

For an extensive discussion of more than 30 U.S. federal privacy laws, as well an expanded version of the sidebar with this article, read the ARMA International Educational Foundation (AIEF) research report by this author, "Requirements for Personal Information Protection, Part 1: U.S. Federal Law," which is available for free download from the ARMA International online bookstore at *www.arma.org/bookstore*.

To learn about U.S. state privacy laws, you can also download the free AIEF research report by this author, "Requirements for Personal Information Protection, Part 2: U.S. State Laws," also available at *www.arma.org/bookstore*. **END**

Virginia A Jones, CRM, FAI, can be contacted at vjones@nngov.com. *Her bio is on page 47.*

Procedures for Developing an Electronic File Plan

Consistency in folder structures and file naming conventions is fundamental to managing electronic information throughout its lifecycle. This case study will be useful to anyone tasked with developing, revising, or implementing an electronic file structure.

Kathryn A. Scanlan, J.D., CRM

As information management has become increasingly complex, the need for well-designed electronic file plans, as a component of good information governance, has been heightened. As defined in ARMA TR 22-2012, *Glossary of Records and Information Management Terms, 4th edition*, a file plan is "a classification scheme that defines and identifies all files, including indexing and storage of the files, and referencing the disposition schedule for each file."

The following case study provides an example of how an electronic file structure can be developed and implemented according to the procedures described in *Developing Electronic File Structures* (ARMA International 23-2013). A hypothetical, industry-neutral work environment is used to illustrate the application of these procedures in a plausible business context.

Background

An organization's recent involvement in litigation brought executive-level attention to the lack of uniform recordkeeping practices across the company. The records and information governance office (RIG) was recruited by the Chief Executive Officer (CEO) to investigate the company's recordkeeping practices and provide recommendations for improvement. RIG conducted an extensive analysis of institutional policies and procedures, the current level of compliance, and external standards and best practices pertaining to the management of records and information.

In the course of its evaluation, RIG identified several recordkeeping problems, including unnecessary duplication of information, inability to quickly locate needed information, inadequate controls over information access, lack of compliance with the organization's records retention schedule, and inappropriate storage of company information in non-approved locations.

RIG reported several direct and indirect costs and risks associated with these problems, including substantial storage and maintenance expenses, unreasonable amounts of staff time devoted to information search and retrieval, increased likelihood of information security breaches, and legal sanctions and reputational damage that could result from negligent recordkeeping practices.

RIG recognized that office directors were concerned that stronger controls on records and information management would overburden employees and decrease productivity. RIG also noticed tensions related to the distribution of authority and budgetary resources. Despite clear gaps in the company's recordkeeping practices, the corporate culture, as a whole, was one of resistance to change.

RIG used ARMA International's Generally Accepted Recordkeeping Principles® as a foundation for its recommendations and was granted authority by the CEO to implement them. The development of a consistent and adaptable electronic file plan structure was identified as a critical piece of RIG's ongoing efforts to correct the organization's recordkeeping problems and to improve its overall information governance. This initiative would focus primarily on unstructured information, i.e., records and non-records, but would operate in conjunction with other information governance systems, such as structured databases.

RIG gathered reliable estimates of costs and return on investment, which helped ease directors' concerns about productivity and efficiency. While requiring substantial staffing resources up front, RIG's cost-benefit analyses rendered the investment worthwhile.

In discussions with end users, it was clear that the organization and retrieval of information could be improved, but that changes from the status quo would be met with skepticism unless they were deemed facile and advantageous to end users. With a combination of executive management support, staff training, and the use of change management principles to keep the organization informed, RIG was confident in its ability to create an improved structure.

Specific to the organization's unique reporting structure, the Compliance, Audit, Information Technology, Records and Information Management, Information Security, and Legal departments may be represented on the project committee. Organizations are encouraged to also identify subject matter experts and interested stakeholders.

A well-designed, scalable, and widely adopted electronic file plan structure would substantially decrease duplication and improper storage of company information; it would also improve access controls and adherence to records retention procedures. And the successful implementation of an electronic file plan structure might spur the adoption of an enterprise-wide electronic document management system in the next five to ten years.

To encourage widespread acceptance of the company's long-term information governance initiatives, RIG strategically identified highly visible and cooperative departments to participate in an electronic file structure pilot project: the CEO's office, Human Resources (HR), and RIG itself. As the department with "project leader" designation, RIG worked with executive leadership to assign representatives from HR, RIG, and the CEO's office to serve on a project committee. RIG also recruited committee members from the Legal, Compliance, and Archives

Regulatory requirements and best practices vary based on industry and location. Organizations are advised to consult with legal counsel to ensure ongoing compliance with a changing legal landscape.

offices to ensure that project decisions would reflect the interests of all information governance stakeholders.

Plan Design

The project committee reviewed the current records retention schedule, as well as paper and electronic recordkeeping practices of pilot offices, identifying necessary updates and process improvements. The committee then developed an electronic file plan structure that would meet the information needs of the pilot offices and provide a framework for the rest of the organization to adapt based on varying business practices.

It is critical to develop reliable and sustainable processes for the assignment of access permission levels. Regular analysis of audit trails can help ensure that company information is being used only by authorized persons and only for authorized purposes.

While focusing primarily on the three pilot offices in its creation of controlled vocabularies, naming conventions, and metadata protocols, the committee maintained a broad perspective to ensure that the end product could be applied to other office units with minimal adjustments. The committee developed a controlled vocabulary to provide a list of preferred terms for department names, position titles, proper names of committees and work groups, acceptable abbreviations, and other commonly used words and phrases. The committee also established certain rules and naming conventions that would apply to the entire enterprise, as described below.

Access, Retention, and Legal Holds

Read and write access permissions are applied at the most restrictive folder level appropriate for the office or individual. Access is limited to those offices or individuals with a legitimate business need to view, print, edit, and/or add to records. Access permissions are granted by the department head, implemented and monitored by the RIG office, and reviewed at least once per year. Access permissions are removed immediately upon an employee's departure.

All records must be reflected in the company's records retention schedule. Retention and disposition of all records must adhere to the records retention schedule. Department leaders work with RIG to maintain an up-to-date records retention schedule. The schedule accounts for the administrative, legal, fiscal, and historical value of all company records, identifies vital records, indicates detailed retention and disposition plans—including trigger points in the records lifecycle—and provides reference to current legal citations.

In the event of litigation or anticipated litigation, all scheduled destruction will be suspended until further notice from the Legal department.

File and Naming Conventions

File names will not include blank spaces. Spaces will be replaced with underscores (_). Folder titles may include blank spaces.

When a file name includes a date, the format "yyyymmdd" with padded zeroes shall be used. The date is recorded at the beginning of the file name.

Examples:

20100607_Minutes (for minutes of a meeting that occurred on June 7, 2010)

20150800_Report (for a report prepared in August 2015)

When multiple drafts or versions of a file are created, the notations "v.#" and "final" will be added to the end of the file name.

Examples:

20100607_Minutes_v.1

20100607_Minutes_v.2

20100607_Minutes_final

When a file name includes an individual's name, the format "Last_First" shall be used.

Examples:

Doe_John_Employment_Offer

Doe_John_Resume

Any paper documents to be filed in the electronic file plan will be scanned into PDFs according to company imaging specifications. Paper documents are to be destroyed immediately after they are filed electronically and reviewed for quality assurance.

Working files and work-in-progress documents are to be filed within the electronic file plan in native file format. Such materials should be routinely destroyed when superseded by final documents. Per the organization's RIM policy, working files and work-in-progress documents will be purged and destroyed by the RIG records manager after three years.

Final documents are to be classified as official records, converted to PDF with appropriate metadata based on a standardized template, and filed according to the electronic file plan.

Metadata capture is automated to the fullest extent possible. Employees with access privileges are advised to set default metadata templates to meet metadata requirements, but are expected to add core metadata elements, as necessary. All documents filed in the electronic file plan will include core metadata elements that adhere to the controlled vocabulary and file naming conventions. For a PDF, core metadata is assigned to the title, author, and subject properties

HP Enterprise Content Management

Improve collaboration, enhance processes and governance

- Document & email management
- Cloud-based file sharing & collaboration
- Policy-driven information /records management
- Business process management
- Pan-enterprise search & knowledge management

as follows:

Title: Unique File Name
Author: Name of Organization, Name of Office, Name of Individual Capturing the Record
Subject: Record Series as Listed in Record Retention Schedule, Date of Capture

The company will monitor and potentially modify or expand metadata requirements to meet user search and retrieval needs, as use of the file plan increases.

Requested changes or additions to the existing file plan structure must be forwarded to the RIG records manager for approval and implementation.

Records with date-based retention periods (e.g., current year + 3) must be maintained in folders labeled by date.

For records with activity-based retention periods (e.g., three years after closed), the activity date must be added to the folder name at the point of occurrence (e.g., a folder titled "Doe_John_Contract" will be changed to "Closed_20140601_Doe_John_Contract" when the contract expires).

Once per year, the RIG records manager, in consultation with department heads, will review each department's file structure, facilitate transfer or destruction of records that have passed their retention period, and destroy non-record working files that are more than three years old.

The management of working files and non-record materials, including duplicate copies of records in paper or electronic format, can be a complex aspect of developing electronic file plans. Depending on the scope and goals of an organization's electronic file plan initiative, it may be necessary to investigate the existence of unauthorized copies or shadow systems; this may be especially appropriate when attempting to decrease litigation risks and storage costs.

Pilot Project Report (Excerpts)

Office of the CEO

Background

The CEO's office holds records of board and committee meetings. Paper committee files are stored in the archives with the organization's articles of incorporation and other historical records. In recent years, electronic committee records have been printed out to add to the archives' files. With multiple copies and drafts stored electronically as born-digital files, however, it is difficult to identify which electronic file corresponds to the official print-out.

Henceforth, the office will cease to print out the official records and will utilize an electronic file structure to track drafts and versions, ensuring the preservation of the official committee files. After finalizing the documentation of a particular committee meeting, those records will be placed in the electronic file plan according to established procedures. All copies or drafts will be deleted. In the future, the office may consider imaging the official paper committee files and incorporating them into the electronic file plan.

The CEO's office manages the public relations function of the organization, including handling company correspondence. Incoming correspondence arrives via mail, fax, and e-mail. Outgoing correspondence is prepared electronically but may be distributed via mail, fax, or e-mail. The office will capture all correspondence in PDF format, either by saving an electronic file as PDF or by scanning a paper file into PDF. Correspondence will be filed by date, segregated into incoming and outgoing, and further segregated by primary topic. Paper and electronic copies will be destroyed when PDFs are properly captured and filed.

Stewardship of all final CEO records will be transferred to the custody of the archives after 10 years but will remain accessible to the CEO's office with read-only permissions for an additional 10 years. (See "Office of the CEO File Structure" on page 29.)

Human Resources

Background

Human Resources (HR) has a well-established system of filing hiring records by date and position number using the naming conventions yyyymm.# where yyyymm indicates the year and month and the .# is used to insert a unique identification number in sequential order. (See page 29.)

While converting to electronic records, the office maintained its existing paper file structure and applied it to the electronic files. Hiring records are destroyed after three years in accordance with the records retention schedule. Upon completion of the hiring process, records of hired employees are copied into HR's personnel files. Those are retained for 20 years after an employee's departure, then transferred to the custody of the archives for historical appraisal.

HR will develop its personnel file structure to accommodate retrieval by employee name, but will incorporate supplemental metadata (start date, end date, department) to permit retrieval by other data elements.

End users are unlikely to comply with overly detailed or cumbersome metadata requirements. Organizations are encouraged to utilize technology to automate the capture and maintenance of metadata, as much as possible. Metadata are particularly useful when reviewing permission levels, audit trails, and adherence to policies surrounding the use of the electronic file plan. Pertinent metadata may be stored within documents' properties, in a separate but connected database, or in both locations.

Office of the CEO File Structure

File Structure

- Committee Records
  - Board of Directors
    - 20130105 Meeting
      - Announcement
      - Agenda
      - Handout1
      - Handout2
      - Minutes
  - Finance Committee
  - Marketing Committee
- Public Relations
  - Correspondence
    - 2010 Incoming
      - Acquisition
        - Doe_Jane_Pro-Acquisition
        - Doe_John_Anti-Acquisition
      - Profit Margin
    - 2010 Outgoing
      - Acquisition
        - Doe_John_Response
    - 2011 Incoming
    - 2011 Outgoing
  - Marketing and Communications
    - 2010 Press Releases
      - 20100130_Press_Release_Acquisition
      - 20100601_Press_Release_Leadership_Changes
- Reports
  - Annual Reports
    - 2005
      - Company_Annual_Report
      - HR_Annual_Report
      - RIG_Annual_Report
    - 2006
    - 2007
  - Audit Reports

Human Resources File Structure

File Structure

- Case Files
  - 2012 Doe John Disciplinary Action
  - 2014 Doe Jane Lawsuit
- Hiring
  - 2011.1
    - Job_Posting
    - Position_Description
    - Employment Applications
    - Interviews and Selection
  - 2011.2
    - Job_Posting
    - Position_Description
    - Employment Applications
    - Interviews and Selection
  - 2012.1
    - Job_Posting
    - Position_Description
    - Employment Applications
    - Interviews and Selection
  - 2012.2
    - Job_Posting
    - Position_Description
    - Employment Applications
    - Interviews and Selection
  - 2012.3
    - Job_Posting
    - Position_Description
    - Employment Applications
    - Interviews and Selection
- Personnel Files
  - Doe Jane
    - Application
    - Benefit Forms
    - Contract
  - Doe John
    - Application
    - Benefit Forms
    - Reference Letters

Records & Information Governance

Background

Primary functions of the Records and Information Governance (RIG) office include project management, records management, systems management, and user training. Project records are created during active projects or initiatives. The records retention schedule indicates that disposition occurs five years after a project is closed. Upon completion of a project, files are moved from "Active" to "Closed," and the closed date is added to the folder title. A similar approach is used for system files; those are scheduled for disposition 10 years after a system is decommissioned.

RIG's pilot rollout will include the provision of training for CEO, HR, and RIG staff members. Under RIG's leadership, the pilot electronic file plan structure will be developed, tested, and modified to meet the needs of the participating departments. RIG will monitor and report on permission levels, user experiences, and the inventory of electronic files captured in the structure.

Records and Information Governance File Structure

File Structure

- Projects
  - Active
    - Electronic File Structure
    - Vital Records Review
  - Closed
    - Closed 20101001 Disaster Recovery Planning
    - Closed 20110516 Records Retention Schedule Update
- Records Management
  - Records Retention Schedules
    - 2005_Records_Retention_Schedule
    - 2011_Records_Retention_Schedule
- Systems Management
  - Active Systems
    - Departmental
    - Enterprise
  - Decommissioned Systems
    - Departmental
      - Decommissioned 20120630 CEO Travel System
    - Enterprise
      - Decommissioned 20111231 Payroll System
- Training Programs
  - Disaster Recovery
  - Electronic File Structure
  - Records Management
    - 2005-2006
    - 2007-2008
    - 2009-2010
    - 2011-2012

In collaboration with the pilot offices, RIG will implement changes to rules, roles, and responsibilities of end users. RIG will also monitor levels of resistance to the electronic file plan, with particular focus on end users' attempts to continue previous recordkeeping practices or utilization of non-approved storage space. Enterprise-wide rollout will commence within two years, and the organization expects to be prepared to transition to a document management system within 10 years.

Learn More

Developing Electronic File Structures (ARMA International 23-2013), from which this case study was excerpted, provides implementation-based recommendations for electronic file plan development in organizations. It describes the strategy, techniques, and tools associated with effective electronic file plan development to appropriate electronic file plan management. It is available for purchase in the ARMA International online bookstore at *www.arma.org/bookstore*. **END**

Kathryn A Scanlan, J.D., CRM, can be contacted at kascanlan@hormel.com. *See her bio on page 47.*

MER

The National Conference
on Managing Electronic Records

MAY 19 - 21, 2014

For Expert Training in Managing Your Electronic Records

BE SURE TO ATTEND MER '14

Join us for The National Conference on Managing Electronic Records on May 19 ~ 21, 2014, with a full Day of Pre-Conference Tutorials on the 18th.

Location: The Westin Hotel in Downtown Chicago, on the "Magnificent Mile"

The MER is the only conference exclusively focused on addressing the key operational, technical, and legal issues associated with the life-cycle management of electronic records.

Register Now!
www.merconference.com/register/

Program
www.merconference.com/mer-conference-program/

Speakers
www.merconference.com/speakers/

The MER Conference Site
www.merconference.com

www.merconference.com

@merconference MER.Conference MERconference

Presented by
CohassetAssociates

Co-sponsored by
ARMA INTERNATIONAL

What's your IG IQ?

Find out by earning your

Information Governance Professional Certification

- Showcases your information governance expertise
- Brings professional recognition within your organization, network, and industry
- Extends your professional network to include an elite group of other IGPs
- Increases your potential for career growth

"I highly recommend the pursuit of your IGP by those who either lead or significantly contribute to the management of their organization's information governance framework."

– Nick De Laurentis, IGP,CRM
Technical Analyst, State Farm Enterprise

For more information and to apply, go to ***www.arma.org/igp***.

An International Perspective on Protecting Personal Information

Records and information management professionals have a key role to play in safeguarding the privacy of personal information. The challenge is keeping up with rapidly changing, intrusive technologies and in step with the legislation that often lags behind them.

Cherri-Ann Beckles

The need for privacy as a public policy arose and augmented in the second half of the 20th century with the emergence and use of information and communications technologies (ICTs) to collect, store, and share *personal data*, which is defined by the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* as "any information relating to an identified or identifiable individual (data subject)."

With profound changes in the advancement and utilization of technology and a shift from manufacturing to providing knowledge-based services, ICTs became central in both the public and private sector, facilitating the widespread distribution of information – including personal data – that could be stored, manipulated, and exchanged more easily than ever before. The expansion of state powers and the institutionalization of information over the last 50 years through more complex technology-based recordkeeping systems gave rise to the need to control access to and the use of personal data.

Records and information management (RIM) practitioners, who are likely to deal with vast amounts of personal data captured in records, have a key role in ensuring compliance with privacy and data protection legislation and policies relevant to recordkeeping within their jurisdictions. They must be proactive in managing information privacy in all recordkeeping systems by becoming conversant with relevant legislation and designing RIM program policies and procedures that ensure that their organizations' records are secured against the unwarranted disclosure and abuse of their internal and external customers' personal data.

Defining Privacy

There is no universal consensus on the meaning of privacy, which encompasses diverse concerns, including the right to be left alone; the right to be free from government surveillance,

intrusive police, or other searches, wiretapping, or persistent journalists; and the right to be allowed to make private personal decisions.

The definition of privacy changes according to space (location) and time. Universally, notions of anonymity and security are often associated with privacy. However, the definition that is most relevant to RIM is that privacy is the right for a "living and identifiable" individual to have some control over the collection, storage, and disclosure of his or her personal information held by governmental agencies, financial institutions, medical facilities, educational institutions, and other public and private entities.

In many jurisdictions, privacy is considered a fundamental human right. Yet, it is evident that privacy is not an absolute right and may be denied for what may be considered a greater purpose. For example, with the increase in terrorism on a global scale, the call for improved national security in some jurisdictions has led to what some consider a sacrificing of privacy. However, it is in the interest of governmental agencies to collect personal information about citizens' earnings and income for tax collection purposes and to collect census data so they can make strategic decisions and improve services for the citizenry.

Although there is this need to collect and use personal data, the "right to privacy" as outlined by the Universal Declaration of Human Rights of 1948 is generally accepted and respected across the globe, and RIM practitioners are key players – in many instances on the frontline – in protecting that right.

Relationship to RIM

When exploring the relationship between informational privacy and RIM, it is clear that the rapidly changing technological environment has had a profound impact on both pursuits. This resulted in privacy becoming a public issue and RIM developing as an organizational response to deal with these changes.

Recordkeeping systems had evolved over time, moving from manual, paper-based systems to highly networked, automated systems. By the 1970s, the proliferation of minicomputers and the computerization of organizations, including the introduction of word processing and data processing machines, meant that vast amounts of information, including personal data, was being created, received, manipulated, distributed, and stored electronically.

In spite of this automation, the widespread use of carbon paper and the photocopier resulted in sustained and exponential growth in creating and distributing paper records. By the late 1980s, organizations were working in hybrid recordkeeping environments, with electronic records adding a new dimension to the need to control records.

Another significant development in recordkeeping took place in the 1990s with the advent of the World Wide Web and the Internet, resulting in the ease of moving information seamlessly across local and wide area networks. Personal data became even more vulnerable to unwarranted distribution and possible abuse by unauthorized people.

Another major development was on the horizon in the new millennium. It took the form of the widespread use of e-mail, instant messaging, and social media, including Facebook, Twitter and LinkedIn, via portable digital assistants, smart phones, and tablets. More recently, cloud computing has led to the remote hosting of organizational data, usually by independent service providers.

These new modes for creating, capturing, and storing data have had unimagined and serious implications for managing records' privacy, as evidenced by the increasing occurrences of privacy-related lawsuits against high-profile governmental and private entities around the globe for failing to comply with privacy legislation.

RIM practitioners, according to legislation in some jurisdictions, are considered "data processors" working on behalf of "data controllers" (employers). Therefore, RIM practitioners should not ignore their role as privacy advocates and the promoters of more stringent regulation of recordkeeping privacy.

Key Privacy Principles

One of the greatest challenges of managing information privacy on a global scale has been disparity among countries' national legislation and enforcement. This led to concerns about the risks incurred by allowing the free flow of information across borders.

As part of the first global initiative to safeguard personal data, the Organisation for Economic Co-operation and Development (OECD) sought in 1980 to harmonize its member states' national privacy legislation by setting out seven baseline principles for the legal drafting process.

The OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OCED *Guidelines*) generally seek to address data quality, specification of the purpose and limitations on collecting personal data, required security safeguards, openness, individual participation, and accountability. The principles embodied in the OECD *Guidelines* state that personal information must be:

1. Collected fairly and lawfully
2. Used only for the purpose specified during collection
3. Adequate, relevant, and not excessive to that purpose
4. Accurate and up-to-date
5. Accessible
6. Kept secure
7. Subject to disposal after the purpose is completed

The OECD's principles are not binding, and in some jurisdictions, they have not been implemented in law. However, they have been the basis on which many information privacy laws have since been written, and they can serve as a guide to RIM practitioners regardless of their location.

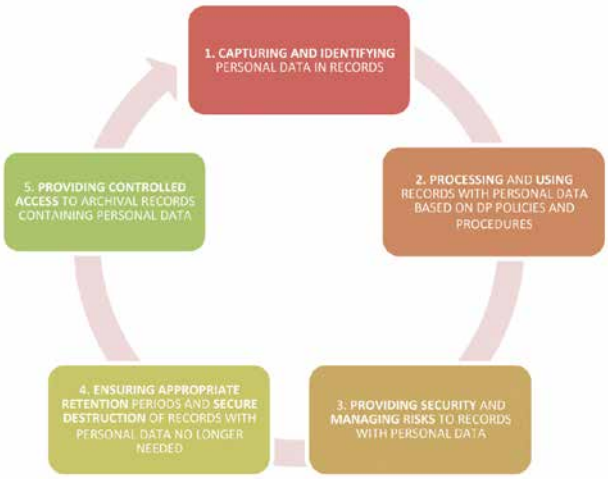


Figure 1: Lifecycle Management of Privacy for Recordkeeping

Key RIM Considerations

Records containing personal data form a significant part of any organization's informational assets and are usually found within the manual and automated systems managed either directly or indirectly by RIM practitioners. Their main activities in regulating privacy/data protection may be summed up in the following three points:

1. Ensuring that data protection responsibilities are clearly identified and assigned
2. Providing RIM services with clearly written policies and procedures that define how personal data is to be processed
3. Ensuring that when obtaining personal information, their methods of collection, storage, destruction and provision of access complies with data protection legislation
4. Following are some specific steps RIM practitioners can take. (See also Figure 1: Lifecycle Management of Privacy for Recordkeeping.")

Identify Sensitive Data

RIM practitioners must be aware of which records contain *sensitive personal data*, which the UK Data Protection Act of 1998 defines as "personal data consisting of information about the racial or ethnic origin of the 'data subject,' his political opinion, his religious beliefs or beliefs of a similar nature, whether he is a member of a trade union, his physical or mental health or condition, his sexual health and the commission or alleged commission of criminal offences."

This type of recorded information is predominately found in records in organizations' human resources,

Key National Privacy Legislation

Privacy acts generally govern how personal information is collected, used, stored, and disclosed. Following are some of the most-often encountered ones for select countries.

Australia: **The Privacy Act 1988:** *www.oaic.gov.au/privacy/privacy-act/the-privacy-act.*

Canada: **Personal Information Protection and Electronic Documents Act:** *http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html.*

China: **Consumer Rights Protection Law:** at *www.wipo.int/edocs/lexdocs/laws/en/cn/cn174en.pdf.*

European Union member countries: **EU Directive 95/46/EC:** *http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf;* **Safe Harbor Data Privacy Framework:** *http://export.gov/safeharbor/*

New Zealand: **Privacy Act 1993:** *www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.*

United States: **Electronic Communications Privacy Act – Title II Stored Electronic Communications Privacy Act:** *www.law.cornell.edu/uscode/text/18/part-I/chapter-121*; **Fair and Accurate Credit Transactions Act:** *www.gpo.gov/fdsys/pkg/PLAW-108publ159/pdf/PLAW-108publ159.pdf;* **Family Educational Rights & Privacy Act:** *www.ed.gov/policy/gen/guid/fpco/ferpa/index.html;* **Health Insurance Portability & Accountability Act:** *www.hhs.gov/ocr/privacy/index.html; www.hhs.gov/ocr/privacy/index.html;* **USA Patriot Act:** *www.justice.gov/archive/ll/highlights.htm*

(See also the article in this issue "Protecting Information Privacy Per U.S. Federal Law" by Virginia Jones.)

finance, and administration sections. Some organizations, such as educational, medical, or judicial institutions, have a higher concentration of records containing personal data because of the nature of their business. Records management programs in these types of institutions need to put additional measures in place to ensure the security of any sensitive personal data.

Leverage Classification Schemes

RIM practitioners, particularly those working in highly centralized systems, seek to develop omnibus classification schemes to arrange records into categories that facilitate quick retrieval and comprehensive control. Classification schemes that group record series containing personal data in logical, functional categories, could be used as the foundation on which sound data protection strategies are built.

Know Legal Requirements

Additionally, RIM practitioners need to re-examine and rethink their formulation of records retention and disposition schedules, bearing in mind the requirements of privacy principles and/or legislation that relate to the retention of personal data. Careful attention must be paid to the provision of access to records containing personal data to ensure that this information is safeguarded from unauthorized use. Measures such as redaction and/or pseudonymization as well as encryption to anonymize personal data in records should be employed wherever necessary when dealing with requests to reproduce records. (See sidebar "Key National Privacy Legislation.")

Enhance Security

RIM practitioners should also seek to ensure the physical and intellectual security of the records within their care. Physical records should be protected in their storage areas, especially in instances where they are transferred for deposit in records centers and archival repositories, relocated to a new site, or sent for destruction.

Comply with Codes of Ethics

Some jurisdictions have either written or considered formulating a code of practice to guide RIM practitioners in managing privacy in their RIM programs. Notably, guarding personal data is not only a legal issue for RIM practitioners but an ethical one; therefore, it should not be overlooked or ignored. The *Code of Professional Responsibility for Records Management* as developed by ARMA International states that "records and information managers [should] affirm that the collection, maintenance, distribution and use of information about individuals is a privilege in trust: the right to privacy of all individuals must be both promoted and upheld."

The International Council on Archives in its *Code of Ethics for Archivists* states that "archivists should respect both access and privacy, and act within the boundaries of relevant legislation." Hence, the responsibility of the RIM practitioner to understand privacy legislation and adopt measures to protect personal data held within public and private organizations is unquestionable.

Develop a Good Communications Strategy

A good communications strategy is critical for sound data protection

management in RIM programs across all organizations, especially large and dispersed ones. Many breaches have occurred across jurisdictions as a result of human error or malicious intent by staff members. Training and orientation of staff in matters relating to privacy/data protection in RIM programs is absolutely crucial to maintaining a well-ordered, well-functioning, enterprise-wide program while reducing the risk of breaches. RIM practitioners should work with human resource experts to incorporate training and awareness about data protection legislation, policies, and procedures in the training programs for staff at every level of the organization.

Step up to the Challenge

Because RIM practitioners are at the heart of the organization as it relates to how its informational assets are managed, safeguarding records and information should be at the center of their work. They must recognize and accept that their role is weightier than ever before, as privacy/data protection legislation will continue to lag behind fast-developing, intrusive technology. Establishing forward-thinking, adept RIM programs inclusive of well-planned data protections policies, procedures, and measures should enable their organizations to stay ahead of the ever-changing compliance landscape. **END**

Cherri-Ann Beckles can be contacted at cherri-ann.beckles@cavehill.uwi.edu. *Her bio is on page 47.*

The Principles in Practice in a New RIM Program

Julie Gable, CRM, CDIA, FAI

Editor's Note: This article is the first in a series highlighting how the Generally Accepted Recordkeeping Principles® (Principles) and the Information Governance Maturity Model (IMM) can be used to initiate, develop, and grow records and information management (RIM) programs in a variety of situations. Access these at www.arma.org/principles. *Using case studies as illustrations, the series will examine how the Principles and the IMM have been applied in different industries and regulatory environments by organizations of all sizes and by people with varying backgrounds. The case studies are composites of actual organizations. Their names have been changed, but the challenges they faced and the creative solutions they found are real.*

A small financial services firm and an oil and gas exploration company were both facing challenges with the need for new records management programs. As we will see, their similarities stem from the productivity and operational aspects of managing records to support business processes – the basic reason that records exist. What differs is how knowledge of the Principles and the IMM influenced their respective approaches to establishing a new records and information management (RIM) program, particularly the crucial decisions of where to begin and how to continue.

Case Study 1: Small Investment Advisory Firm Wants Document Management System

The Arbor firm offers investment services to individuals. It is regulated by the Securities and Exchange Commission, the Dodd-Frank Act, and the usual blend of state and local laws. It must comply with specific guidelines regarding its records.

The firm opened less than 10 years ago, and as a small business it strives to use technology for a competitive advantage. Many client account records begin as paper documents with original signatures, but they become images once certain business processes are complete. The firm does not have standard file naming conventions, and most client records are scanned within the business process to a shared drive, sometimes more than once in the course of completing their workflow. Evidence of trading activities and various reports exist only as electronic records.

The firm has a compliance officer and has documented its policies and procedures for many of its regulatory requirements, including information privacy and security. It has an executive committee that includes the compliance officer, the CEO, and the CFO, with legal advice provided by a third-party firm.

Arbor has never destroyed anything, believing it is better to have proof of what was done than to be unable to produce a record. During a routine audit, however, it became apparent that multiple copies of the same documents existed under different names on various shared drives, making it difficult to identify the re-

cord copy of any document that an auditor requested. Searching was also a challenge because identical documents had different descriptive information on various spreadsheets. To ensure that it never has to face another audit that resembles a scavenger hunt, Arbor wants to implement a document management system for all of its records. Arbor recognizes that it needs help with records classification and standardized metadata. The question is, where does it start?

The Principles to the Rescue

Even though the Principles are arranged as a list, and it is tempting to move down them item by item like stepping stones, they are actually more like a starburst (see Figure 1). Some principles have a distinct regulatory flavor – for example, the Principles of Compliance, Protection, and Transparency. These focus on how the RIM program appears to those outside the business, including regulators, auditors, and litigators. Other principles have an operational context, such as the Principles of Accountability, Integrity, Availability, Retention, and Disposition. These touch more closely on how information is created and used internally for the ongoing functioning of the business, although, of course, they do have implications for external parties as well.

A small business in a highly regulated industry will likely concentrate its scarce resources first on areas that pose the most risk. Using the IMM as a guide, Arbor is at maturity level 2 (In Development) or at level 3 (Essential) in these areas. For example, in reference to the Principle of Compliance, Arbor has identified key laws and regulations and has a code of business conduct, as well as specific, measurable goals for compliance, but there is no hold process because Arbor has never destroyed anything.

In the context of the Principle of Protection, there is a written policy with well-defined confidentiality and privacy considerations because client documents contain Social Security numbers, bank account numbers, and other sensitive data. Employees are trained in how to handle such information, access restrictions are in place, and a workflow is defined.

In reference to the Principle of Transparency, Arbor's business processes are documented, but RIM practices are spotty where they exist at all, with some formalized in writing and others largely *ad hoc*.

From an operations context, Arbor is most likely at a level 1 (Substandard). Integrity is not at a high level principally because the *office of record* – that is, the function responsible for the final, official record – is not clear. Hence, there are difficulties with multiple scanned images of the same documents stored under different file names. The Principles of Retention and Disposition are at level 1 because there are no retention policies or schedules; there is no sanctioned policy or methodology for careful, considered disposition in the due course of business; and there is no mechanism for applying legal holds or other holds to records that may be needed for legal or tax matters.

What Arbor Did

Arbor was convinced that work on retention schedules would provide the classification scheme necessary for its planned document management system. Because they are part of RIM policies and procedures, retention schedules would have to be written and would cover such topics as retention, disposition, and legal holds.

The executive committee and the compliance officer reviewed the draft policies. The types of records were identified through meetings with individuals in all areas of the company to understand business processes and to analyze workflows. An important finding from the process and workflow analysis was learning how users search for documents. This discovery, in turn, helped Arbor develop standard metadata that could be used to store documents and to help develop the planned document management system.

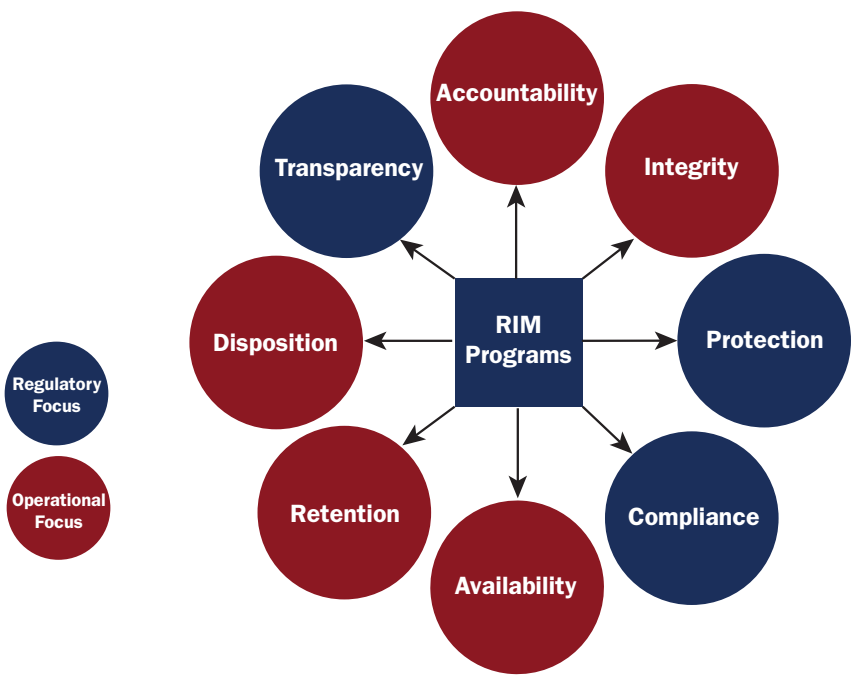


Figure 1: The Generally Accepted Recordskeeping Principles® Focus

Once workflows were understood, Arbor was able to identify who should be responsible for the official record copy – that is, the one that should be retained and available for regulators and auditors. Retention schedules that identified records classes and descriptions were devised, and retention times were applied by referencing the compliance officer's regulatory requirements and the business users' needs. Arbor also developed a basic records training program.

When all elements of the program were approved, Arbor achieved improvements in the Principles of Integrity, Availability, Retention, and Disposition, and the firm was able to map how it would move forward with a training program for all employees and an audit of the records program to determine how well staff was complying.

Case Study 2: Oil and Gas Exploration Firm Needs Room for Growth

OGE is an energy company engaged in exploration. Its work regularly involves deeds, leases, and contractual rights to access, enter, and drill on various properties, so the management of land records is critical. Like all utilities, OGE must comply with state regulatory commissions and with many layers of federal, state, and local environmental laws. In addition, the firm's records support its business objectives by enabling research on potentially rich new exploration areas and by supporting the writing of mutually beneficial contracts. Realizing this, the company established a RIM function very early in its history.

Since its inception, OGE has experienced rapid growth. The company retains paper for original records but also produces imaged renditions that allow ease of access for authorized users from the many offices nationwide.

The initial focus of RIM activities has been operational: making sure the right information is available to the right people at the right time. OGE has also instituted radio frequency identification (RFID) tracking for paper files because its records are highly active and circulate frequently. A staff of four records technicians provides support for about 30 researchers. A records manager was promoted from within the ranks and now oversees the team.

A major challenge has been space – both electronic and physical. Space for onsite paper records vies with space needed to accommodate additional employees. Some inactive files are stored offsite, but many more are retained onsite. The quest for additional space is ongoing and time consuming.

OGE is aware of the Principles, but as is common with many growing businesses, it has not had the time or the resources to use them in a formalized way.

Businesses that are growing need to balance what must be done to comply with external demands and what must be done to support efficient and effective operations.

A Quick Assessment

OGE nonetheless could use the Principles and the IMM to determine what to do next. From an operations standpoint, the company has already achieved some of the goals associated with the Principle of Accountability at a Level 3 (Essential), such as having executive awareness and sponsorship, having a records manager, and including electronic records in the RIM program.

Availability also approaches a Level 3 because there are standards for how records and information are stored, such as procedures for digitizing records. Also, established mechanisms promote timely retrieval, and such systems and infrastructure as RFID contribute to the availability of records.

A good next step would be to strive for conformity with the Principles of Retention and Disposition. Doing so would help ease the ongoing space problems by providing strong, documented guidelines for how long records must be kept and when they may be disposed of in due course, as long as no litigation or investigation is pending or imminent.

Disposition, in particular, would also encourage policies on holds, an element that shouldn't be overlooked in industries that rely on contracts and want to avoid or easily resolve the disputes that often arise in such situations.

As with many organizations with young records programs, OGE has much work ahead of it, but the Principles and the IMM can provide an excellent framework for how to proceed. Businesses that are growing need to balance what must be done to comply with external demands and what must be done to support efficient and effective operations. Meanwhile, the new records manager and staff can continue to add to their records knowledge by tapping into their local ARMA chapters and by making use of ARMA International's educational and networking resources.

Key Take-Aways

The key lessons from the two scenarios are as follows:

1. Address regulatory requirements first because non-compliance poses a real risk to the business. Do what is necessary to avoid risk, especially those risks that could result in sanctions, tarnished reputation,

and the ability to continue doing business.

2. Recognize that the Principles and the IMM comprise a framework, but there is no need to address each element in a linear fashion. Once the Principles of Compliance and Accountability are addressed, the next areas to conquer depend on the organization's operational needs. For Arbor, it was records classification and metadata standards, both of which resulted from beginning a records retention and disposition program. For OGE, it was information availability.
3. You can't do it all at once, so it's good to have a larger plan. Such a plan can also show insiders and outsiders how the program started, what is in development, and what is still to come. It indicates that you are aware of the deficits and have begun to address them. The Principles and the IMM are an orderly, methodical approach based on international standards. They make a strong basis for any new program's development plans.

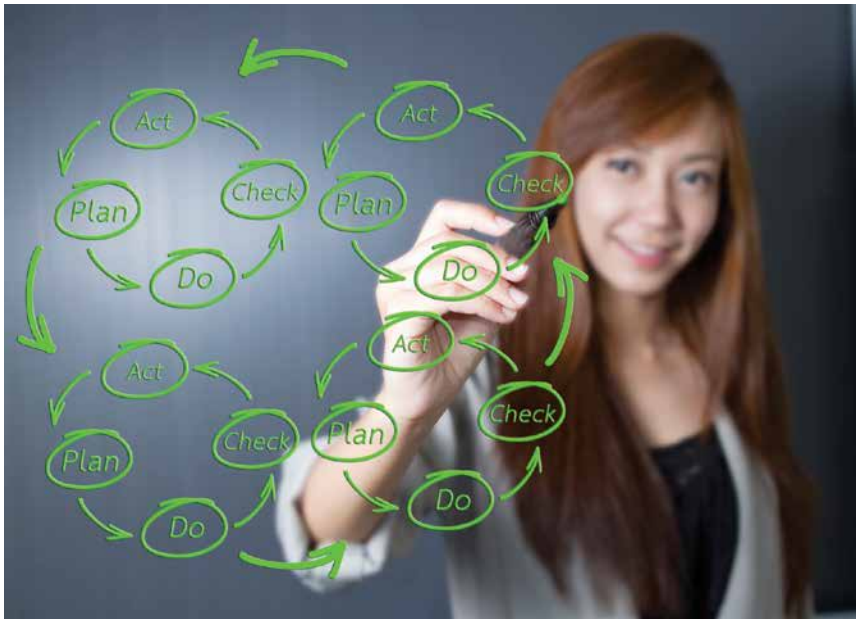
Of course, the program isn't the only thing that will change. As it states in the Principles, "As a program progresses, the personnel charged with its management will likewise progress through a spectrum of increasing competence and effectiveness." Daunting as it may seem, starting from scratch can be highly rewarding – personally and professionally – for those involved in implementing a new RIM program or new program components.

Arbor and OGE are as different as can be – different industries, different regulations, and different approaches. Yet, by using the Principles and the IMM as guiding tools, both offer valuable lessons for organizations that are trying to establish a records program amidst fast growth. **END**

Julie Gable, CRM, CDIA, FAI, can be contacted at juliegable@verizon.net. *See her bio on page 47.*

Elements to Be Assessed in a RIM Audit

ARMA International Standards Workgroup



The classic 20th century teachings of W. E. Deming, Ph.D., heralding the "plan-do-check-act" continuous feedback loop remain a bulwark of management science, despite the passing of many decades. Today, through the audit process, records and information management (RIM) professionals can heed Deming's imperative by monitoring the organization's compliance with RIM program policies and procedures. Opportunities for quality and performance improvement are brought to the fore, and the organization's risk exposure level is assessed. The RIM program and the organization can jointly benefit from these activities.

The Focus of the RIM Audit

In accordance with the approved RIM audit plan, data, documents, records, and other items are gathered during the course of the RIM audit. The audit should focus on an assessment of:

- The completeness of RIM policies and procedures with consideration of all records, regardless of format/media, as managed throughout the lifecycle
- The currency of RIM policies and procedures per RIM standards and best practices
- The efficiency/effectiveness of RIM-related software/hardware/systems
- The organization's compliance with RIM policies and procedures and legal obligations
- The organization's RIM-related risk exposure
- Recommendations for areas possibly benefitting from changes/improvements

For the RIM program, these findings and quality-focused suggestions are essential facets of the audit, providing stepping stones to a higher level of functioning. At the audit's conclusion, all results (including findings and suggestions) are included in the written audit report.

Legal Considerations

Legal Requirements

An organization can be subject to many legal mandates relative to its RIM program, including laws, statutes, regulations, and ordinances. As a result, professional legal advice may be warranted prior to undertaking a RIM audit. While the audit cannot always determine whether an organization is compliant with *all* relevant legal requirements, it is an opportunity to make a "good faith effort" to identify such requirements and document the organization's attempts to fulfill its responsibilities. The audit should also assess the adequacy of the organization's mechanisms and protocols to monitor ongoing compliance with related processes, such as legal holds and e-discovery, in its day-to-day operations.

Sources of legal mandates affecting the RIM program may include, but are not limited to:

- International laws or treaties
- Federal law
- State, municipal, and/or local statutes, regulations, and ordinances
- Standards and best practices and/or guidance advisories developed by certifying or licensing bodies and/or specific industry or sector-related groups

Other organizational departments are commonly affected by legal requirements, necessitating collaboration with RIM professionals to facilitate appropriate recordkeeping. As a result, representatives from diverse departments or units, such as those listed here, often participate in RIM

audit activities:

- Accounting and Taxation
- E-commerce
- Finance
- Human Resources/Labor Practices
- Insurance/Risk Management
- IT (information technology security, privacy, and confidentiality)
- Legal and Compliance
- Physical Facilities/Environmental Management

Legal Holds. In the United States, when an organization faces potential litigation, preservation of appropriate paper and electronic records and nonrecords is an obligation per the *Federal Rules of Civil Procedures* (FRCP). Organizations should have legally defensible policies and procedures regarding legal holds and should monitor ongoing compliance. Failure to monitor and comply with a hold order can result in spoliation and/or sanctions ranging from monetary penalties to investigation by various government entities.

Areas examined during the RIM audit and pertaining to legal holds usually include:

- Documentation of the legal hold process in RIM policies and procedures
- Electronic systems used for recordkeeping and legal holds activities, e.g., electronic records management systems, electronic document management systems, or other specialized electronic information management systems utilized in legal settings
- Identification of individual(s) responsible for the legal hold process, i.e., establishment of a "point of contact"
- Method(s) by which the legal hold is initiated and rescinded
- Method(s) by which the legal hold is confirmed by the recipient
- Method(s) by which records and nonrecords, as applicable, are identified for legal hold
- Method(s) by which records and nonrecords, as applicable, are tracked when multiple holds are in place
- Preservation of paper and electronic records and nonrecords, as applicable, during the legal hold period
- International, federal, regional, industry, and/or sector-specific laws, statutes, regulations, and ordinances affecting legal holds

Given their importance, legal holds should be included in the RIM audit. A representative sample of cases involving legal holds may be investigated to ensure they were managed in a compliant manner. Alternatively, if the volume of legal hold cases was small, all cases could be examined as part of the audit. The organization's RIM professional(s) should work closely with the auditor(s) to ensure there is an adequate understanding of the legal hold process.

Given their importance, legal holds should be included in the RIM audit.

Benchmarking against industry best practices for legal holds allows the auditor(s) to pinpoint areas where improvements are recommended. *The Sedona Conference® Commentary on Legal Holds: The Trigger and the Process* and the ARMA International guideline *Records Management Responsibility in Litigation Support* provide further guidance.

E-Discovery. E-discovery is the process by which electronically stored information (ESI) is uncovered and extracted for evidentiary purposes. ESI should be preserved and protected from loss.

Business Continuity, Disaster Management Planning, and Vital Records

The RIM program should incorporate strategies for business continuity/disaster management planning, including vital records management. The RIM audit should investigate these program components, assessing their viability and conformance with recognized and accepted RIM standards and best practices. The auditor(s) should also evaluate the organization's RIM-related system(s) and make recommendations, as needed, pertaining to business continuity/disaster management preparedness.

RIM professionals should update planning documents on an ongoing basis, communicating revisions to the appropriate individuals within the organization and conducting training, as needed.

Vital records are needed for the everyday functioning of the business. These are the records that are essential to the continuity of the organization. The audit can determine whether vital records have been thoroughly identified and if they are being managed appropriately per the program's policies and retention schedule(s). Backups are recommended for all vital records, regardless of record format and storage media. For instance, many organizations now use electronic storage options, such as cloud-based services, to provide redundant, offsite preservation. The audit should examine all vital records backup policies and procedures.

Well-formulated business continuity/disaster management planning allows for any number of contingencies or unforeseen events—both natural or man-made, intentional or unintentional.

Depending upon the business setting, the auditor(s) may need to address organization-specific characteristics when evaluating disaster management/business continuity preparedness including, but not limited to:

- Applicable legal mandates
- Socio-political, economic, and/or cultural considerations affecting the organization's operations on a temporary or long-standing basis

- Special or unique processes, specific to an organization's business or its setting, required for record retrieval or restoration
- The organization's physical location(s) and topography/ geography
- The type of organization, i.e., for-profit, not-for-profit, or government

ARMA International provides an American National Standard on the topic of vital records management: *Vital Records Programs: Identifying, Managing, and Recovering Business-Critical Records* (ANSI/ARMA 5-2010). The National Fire Protection Association (NFPA) and Underwriters Laboratories, Inc. (UL) have produced standards focusing uniquely on fire protection: *Standard for the Protection of Records* (NFPA 232, 2012 Edition) and *Standard for Tests for Fire Resistance of Vault and File Room Doors* (ANSI/UL 155:2009).

In addition, various disaster preparedness topics are covered in online information available from the Disaster Recovery Institute International (DRII), the Federal Emergency Management Agency (FEMA), the Library of Congress, the National Archives and Records Administration (NARA), and the Northeast Document Conservation Center (NDCC).

Secure Records Storage

Records need to be secure (protected) to ensure their authenticity, integrity, and reliability; this is a hallmark of an effective RIM program. All records, regardless of format, should be protected against loss, misuse, and inappropriate/unlawful alteration. In addition, records containing personal or confidential information are subject to special handling and enhanced security measures.

Records security encompasses in-place safeguards designed to thwart physical damage (e.g., fire or other acts of nature) and virtual hazards (e.g., inappropriate access or malicious code infections).

Accordingly, the RIM audit should examine the RIM program's applicable security operations, including procedures, according to industry standards and best practices in the areas of:

- Levels of protection offered to different types of records, e.g., Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations require specific access and storage requirements for health records
- Physical protection of paper records including, but not limited to, procedures/tools/ construction materials applicable to buildings, e.g., records centers; records storage-related equipment, e.g., file cabinets and vaults; and monitoring devices, e.g., temperature/humidity control instruments and surveillance cameras
- Virtual protection of electronic records including, but not limited to, access procedures/tools, cloud storage-related activities, malware prevention/detection processes, and software/systems design and functioning

The RIM audit should examine the RIM program's security operations.

The RIM audit should examine the organization's ability to secure its records according to RIM program policies and procedures and RIM/non-RIM standards and best practices, as well as applicable legal mandates.

Further standards and best practices guidance on security matters related to RIM practices, including cloud-based storage, internal and external environmental factors for records stored on physical media, and records center operations, may be obtained from ARMA International's *Guideline for Outsourcing Records Storage to the Cloud* and *Records Center Operations* (ARMA TR 01-2011).

Other sources include: the International Committee for Information Technology Standards (INCITS), the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), and the National Institute of Standards and Technology (NIST).

Secure Records Storage During the RIM Audit

An onsite room or office, with a lock for security purposes, should be provided for the auditors' use during the RIM audit. Records used by the auditor(s) may be kept in that space until the audit's close. A checklist or log should be maintained to track the location and utilization of physical records examined as part of the audit. Electronic records stored in various automated systems, databases, or other locations may be involved in audit activities. Computer access to records should be password protected with appropriate safeguards, such as encryption, to ensure records' continuing authenticity, integrity, and reliability. For electronic records, access-related metadata should be logged and retained. Upon completion of the audit, the chain of custody detailing the transfer of physical and electronic records to/from the auditor(s) should be documented in the audit report and retained per the retention schedule.

Electronic Records Management Systems Design

ARMA International's *Glossary of Records and Information Management Terms*, 4th edition (ARMA TR 22-2012) defines an *electronic records management system* (ERMS)—which is sometimes referred to as an electronic recordkeeping system or electronic records management application— as "a system consisting of software, hardware, policies, and processes to automate the preparation, organization, tracking, and distribution of records regardless of media."

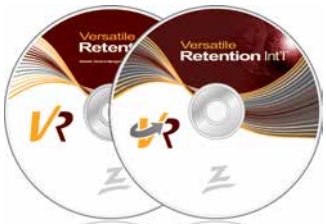
BULLETIN BOARD

Privacy+ is an international certification program open to all companies providing outsourced storage and protection of hard-copy records and off-line removable computer media. Participation in Privacy+ is voluntary and allows companies to publicly demonstrate their commitment to protecting the privacy of information entrusted to them by their clients. Privacy+ certification is owned and administered by PRISM International (Professional Records & Information Services Management), the not-for-profit trade association for the commercial information management industry. Look for the Privacy+ logo, ask for it in your RFPs, and expect your records and information management partners to have it. For more information, please visit ***www.prismintl.org***.

NAID is the non-profit trade association for the secure destruction industry, which currently represents more than 1,900 member locations globally. NAID's mission is to promote the proper destruction of discarded information through education, the NAID 'em initiative, and encouraging the outsourcing of destruction needs to qualified contractors, including those that are NAID-certified. ***www.naidonline.org***.

ZASIO

Zasio Enterprises, Inc.
Versatile Retention™
Versatile Retention Int'l™



Get your hands on Zasio's latest version of Versatile Retention. With over 40,000 legal citations containing records retention requirements, this intuitive software will help you keep your retention schedule — whether domestic and/or international — up-to-date, easily accessible, and legally compliant.

To learn more about the latest release of our retention management software solutions, visit: ***www.zasio.com/company-news-releases.asp.***

RSD is proud to be one of the official charter supporter of the Information Governance Initiative (IGI) to advance the adoption of information governance. IGI is a cross-disciplinary consortium of industry experts and vendors establishing a think tank focused on advancing IG practices across all vertical industries. The IGI will publish research, benchmarking surveys, and guidance for practitioners as well as provide an online community designed to foster discussion and networking among practitioners of IG.

To learn more, visit ***www.rsd.com/en/information-governance-initiative***.

rsd Your Information. Governed.

Recall Holdings Limited (ASX: REC), a global leader in information management, announced that it was awarded ISO/IEC 27001:2005 Management System certification by SRI Quality System Registrar on December 19, 2013. Recall is the first information management company to achieve ISO27001 Certification for all global operation centers. ISO/IEC 27001:2005 is a process-based certification recognizing organizations that can link business objectives with operating effectiveness. Recall's Global ISO27001 Certification demonstrates excellence in Information Security Management System (ISMS) planning, deployment, and provisioning services that support IT infrastructure to protect information and enable the associated secure service delivery processes to Recall employees and customers.

recall™
Your Information. Securely Managed.

The definition also notes that such a system includes retention scheduling and disposition capabilities. The way(s) organizations choose to design and implement these systems are examined in the RIM audit. While other types of information systems proliferate, including those uniquely designed for content and/or document management within the organization, this discussion is limited to systems characterized as ERMS.

As part of the audit … ERMS issues should be considered.

As part of the audit, these ERMS issues should be considered:

System Scope:

- Do policies and procedures delineate what records should—and should not—be stored in the system, as well as who should file them and when they should be filed?
- What steps are taken to ensure that policies and procedures are properly executed?

Records Identification:

- Does the system allow for the designation of a file stored in the system as a record (i.e., one file equals one record)?
- Does the system allow for the designation of a set of files stored in the system as one or more records (i.e., one file contains multiple records, multiple files contain the components of one record, or multiple files contain the components of multiple records)?
- Can the system demonstrate, via report generation, that every file and/or record in the system is associated with one or more record(s) and/or file(s)?

File Plans:

- Are file plans in place?
- Does the system allow every record to be linked to an item in a file plan?
- Can the system demonstrate, via report generation, that every record in the system is linked to an item in a file plan?

Records Disposition:

- Does the system allow every record stored in the system to be linked—either directly or via the file plan—to disposition instructions?
- Can the system demonstrate, via report generation, that every record and/or file stored in the system is linked to disposition instructions?
- Can the system identify, via report generation, all records and/or files subject to a particular set of disposition instructions?
- Can the system ensure that every file associated with more than one set of disposition instructions is retained for the longest retention period in any of those disposition instructions?
- Are policies and procedures in place to ensure that only authorized personnel can execute disposition instructions within the system?
- Is the system monitored to ensure disposition instructions are properly executed for all records in the system?

Legal Holds:

- Does the system allow for the suspension of disposition instructions for records subject to a legal hold?
- Are policies and procedures in place to ensure that no records under a legal hold order are destroyed?

Conversion/Migration Strategy:

- Can the system easily export records and their associated metadata if conversion to another system is necessary?
- Are policies and procedures in place to periodically assess the need to migrate records and associated metadata to a new system?

Within the past two decades, the U.S. Department of Defense (DoD) created DOD 5015.2-STD, *Design Criteria Standard for Electronic Records Management Applications*. This *de facto* standard provides advice for ERMS deployment, and the U.S. National Archives and Records Administration (NARA) supports its use by all federal government agencies. ARMA International's technical report *Using DoD 5015.2-STD Outside the Federal Government Sector* (ARMA TR 04-2009) offers assistance when using this standard in other types of organizations.

Increasingly, organizations are amassing large collections of data and information, whether via social media tools, electronic messaging applications, and/or cloud-based platforms. Sometimes, these content caches exist beyond the boundaries of traditional ERMS. In conducting an audit, it is important to investigate how the RIM program handles these other data and information sources to ensure that all records are properly identified, managed, and stored, regardless of point of origin.

ARMA International's American National Standard *Implications of Web-based Collaborative Technologies in Records Management* (ANSI/ARMA 18-2011) and its related technical report *Using Social Media in Organizations* (ARMA TR 21-2012) are useful reference publications for this purpose.

Learn More

For a comprehensive discussion of auditing a RIM program, see the technical report *Auditing for Records and Information Management Program Compliance* (ARMA International TR 25-2014). It is available for purchase at *www.arma.org/bookstore*. **END**

The ARMA International Standards workgroup leader was Sandra Broady-Rudd, CRM; members were Mark Conrad; Michelle Ganz, CA: Glenn P. Gercken, CRM; Sharon Llewellyn: Daniel McCormack, CA: Tanya Marshall; and Bernard Reilly. *See their bios on page 47.*

Contact Information

AUTHOR INFO

BECKLES GABLE JONES SCANLAN

Protecting Information Privacy Per U.S. Federal Law Page 18

Virginia A Jones, CRM, FAI, is the records manager for Newport News (Virginia) Department of Public Utilities. An adjunct graduate course instructor in the School of Library and Information Science for Wayne State University, Jones has authored numerous RIM-related books. She is a fellow of both AIIM and ARMA International and has served on the Institute of Certified Records Managers' Board of Regents. Jones can be contacted at *vjones@nngov.com*.

Procedures for Developing an Electronic File Plan Page 24

Kathryn A. Scanlan, J.D., CRM, is supervisor of records and information management (RIM) for Hormel Foods Corporate Services LLC. Active in the RIM profession for more than five years, she holds a law degree and a master's in archives and records administration from the University of Wisconsin-Madison. Scanlan can be reached at *kascanlan@hormel.com*.

Others that contributed to *Developing Electronic File Structures* (ARMA International 23-2013), from which this case study was excerpted, include workgroup leader Deborah Juhnke, CRM, Husch Blackwell LLP; and workgroup members: Jeanine L. Baron, PMP, Streamliners Inc.; Michael DeVanna, CRM, Blue Cross Blue Shield of Massachusetts; Jessica Fairchild, San Diego County Regional Airport Authority; Vincent E. Ferguson, CRM, CIP, Southeastern Pennsylvania Transportation Authority; and Kathryn Scanlan, CRM, Hormel Foods Corporate Services LLC.

An International Perspective on Protecting Personal Information Page 33

Cherri-Ann Beckles is the Assistant Archivist at The University of the West Indies (UWI) Cave Hill Campus in Barbados. She holds a master's degree in records and archives management from the University College London and a master's degree in history with heritage studies from The UWI. She has been working in archives and records management since 1999, including as a lecturer at UWI since 2004 and a consultant since 2007. She can be contacted at *cherri-ann.beckles@cavehill.uwi.edu*.

The Generally Accepted Recordkeeping Principles® The Principles in Practice in a New RIM Program Page 38

Julie Gable, CRM, CDIA, FAI, is president and founder of Gable Consulting LLC. She has more than 25 years of experience specializing in strategic planning for electronic records management, including business case development, cost-benefit analysis, requirements definition, and work plan prioritization. Gable has authored numerous articles and frequently speaks at national and international conferences. She holds a master's degree in finance from St. Joseph's University. Gable can be contacted at *juliegable@ verizon.net*.

RIM Fundamentals Series Elements to Be Assessed in a RIM Audit Page 42

The ARMA International Standards Workgroup leader was Sandra Broady-Rudd, CRM, an operational risk consultant at Wells Fargo, Madison, WI. Workgroup members were: Mark Conrad, archives specialist in the Applied Research branch of the Office of Information Services at the National Archives and Records Administration, Rocket Center, WV; Michelle Ganz, CA, archivist at Lincoln Memorial University, Harrogate, TN; Glenn P. Gercken, CRM, records manager with Ungaretti & Harris, LLP Chicago, IL; Sharon Llewellyn, business consultant with Global Business Solutions, Sterling, VA; Daniel McCormack, CA, archivist/records manager for the Town of Burlington, Burlington, MA; Bernard Reilly, president of the Center for Research Libraries, Chicago, IL; Tanya Marshall, state archivist for Vermont State Archives & Records Administration, Montpelier, VT; and Natasha Zwarich, professor of archival science at the Université du Québec à Montréal, Quebec, Canada. They can be contacted via *standards@armaintl.org*.

AD INDEX

		Contact Information
27	**HP/AUTONOMY**	*www.autonomy.com*
9	**Institute of Certified Records Managers**	518.463.8644 – *www.ICRM.org*
BC	**Iron Mountain**	*www.ironmountain.com*
31	**MER – The National Conference on Managing Electronic Records**	*www.merconference.com*
5	**NAID**	*bit.ly/AAAnotification*
34	**PRISM**	*www.prismintl.org*
IBC	**Recall**	888.RECALL6 – *www.recall.com*
IFC	**RSD**	*www.rsd.com*
21	**San José State University**	*slis.web.sjsu.edu/mara*
3	**Zasio**	800.513.8000 – *www.zasio.com*

With our leading edge technologies, proven protocols and top notch information management expertise, we put you in **TOTAL CONTROL** of your information.

recall™

Your Information. Securely Managed.

INFORMATION GOVERNANCE
Total governance. Total control.

DATA PROTECTION
Guarantee Business Continuity

SECURE DESTRUCTION
Mitigate Risks

DOCUMENT STORAGE
Ensure Compliance

DIGITAL SOLUTIONS
Improve Workflow

Step into the **NEW GENERATION OF INFORMATION MANAGEMENT** with recall™

Learn More: recall.com | 1.888.RECALL6