ARMA

VOLUME 1
JAN-MAR 2019

MAGAZINE.ARMA.ORG

ARMA

CONTENTS

A successful leader has to serve those they are leading, being willing to "pick up a broom and sweep floors right along the side of the people he or she is responsible for."

Programs like Slack, Office 365, & Salesforce bring new challenges, and ediscovery can be daunting when wrestling with this data.

ARTICLES

MAGAZINE.ARMA.ORG

PUBLISHER: JOCELYN GUNTER, IGP, CPA | EDITOR IN CHIEF: NICK INGLIS, CIP, IGP, INFO | MANAGING EDITOR: JEFF WHITED | ADVERTISING ACCT MANAGER: JENNIFER MILLETT | EDITORIAL INQUIRIES: EDITOR@ARMAINTL.ORG | ADVERTISING INQUIRIES: JENNIFER.MILLETT@ARMAINTL.ORG |

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. ARMA INTERNATIONAL (WWW.ARMA.ORG) IS A NOT-FOR-PROFIT PROFESSIONAL ASSOCIATION AND THE AUTHORITY ON GOVERNING INFORMATION AS A STRATEGIC ASSET. THE ASSOCIATION, WHICH WAS ESTABLISHED IN 1955, HAS APPROXIMATELY 27,000+ MEMBERS, INCLUDING RECORDS AND INFORMATION MANAGERS, INFORMATION GOVERNANCE PROFESSIONALS, ARCHIVISTS, CORPORATE LIBRARIANS, IMAGING SPECIALISTS, LEGAL PROFESSIONALS, IT MANAGERS, CONSULTANTS, AND EDUCATORS, ALL OF WHOM WORK IN A WIDE VARIETY OF INDUSTRIES, INCLUDING GOVERNMENT, LEGAL, HEALTH CARE, FINANCIAL SERVICES, AND PETROLEUM, IN THE UNITED STATES, CANADA, AND MORE THAN 30 OTHER COUNTRIES AROUND THE GLOBE.

MAGAZINE.ARMA.ORG 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://MAGAZINE.ARMA.ORG/BECOME-AN-AUTHOR.

OPINIONS AND SUGGESTIONS OF THE WRITERS AND AUTHORS OF ARTICLES IN MAGAZINE.ARMA.ORG 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.

MIGRATING LEGACY RECORDS- A CASE STUDY

UTA FOX, CRM, FAI

Organizations that maintain electronic records systems may at some point need to undertake either a records conversion or migration to address software obsolescence. This article discusses how the Calgary Police Service's (CPS) records and information management (RIM) and information technology (IT) teams collaborated to ensure that nearly four million criminal case file records stored in its legacy system – a system used for more than 40 years – were successfully migrated to a new, off-the-shelf records management system (RMS).

Migrating the criminal case file records presented a number of challenges. First, the migration process, its planning and execution, had to comply with the CPS' recordkeeping requirements as specified in its RIM program. As well, the migration had to preserve the integrity, authenticity, reliability, and usability of the records to be migrated.
Second, it was imperative that CPS' case file records meet legal admissibility requirements for court purposes. Migrations involve risks such as records loss, deterioration, or corruption, which had to be managed to make certain the records admissibility was not jeopardized.

To ensure the recordkeeping and admissibility challenges were met, the RIM team applied two standards to direct the migration process:

- Canadian General Standards Board, CAN/CGSB 72.34-2017, Amendment 1 (October 2018), Electronic Records as Documentary Evidence (CAN/GGSB 72.34).
- International Organization of Standardization, ISO 13008, Information and Documentation – Digital Records Conversion and Migration Process, 2012 (ISO 13008).

LEGAL REQUIREMENTS FOR ADMISSIBILITY IN COURT

CPS' RIM program has been based on CAN/CGSB 72.34 since 2005. The standard's primary principle is that organizations must always be prepared to produce their records as evidence. Additionally, continuous compliance with CAN/CGSB 72.34 is a crucial component of the proof of the integrity of an electronic record or records system:

> **Use of an electronic record as evidence requires proof of the authenticity of the record, which can be inferred from the integrity of the electronic records system in which the record is made or received or stored, and proof that the record was "made in the usual and ordinary course of business" or is otherwise exempt from the legal rule barring hearsay...**

With that said, according to the standard, records can be declared authentic if the integrity of the records system in which the record was made, received, or stored can be proven and/or if the reliability of the recordkeeping processes can be demonstrated.

RECORDKEEPING REQUIREMENTS

Migration preserves digital records. ISO 13008 advises that the migration process must be managed to prevent any degradation or loss in the authenticity, reliability, integrity, and usability of the records. Documenting the recordkeeping requirements is also essential to the migration process. And, equally important, the personnel central to the process must be aware of the organizational requirements so they can ensure the records' content, context, and structure are maintained. According to CAN/CGSB 72.34, the onus is on the organization to make certain its recordkeeping processes are reliable to protect and maintain the evidentiary and admissibility value of the records.

APPLYING STANDARDS TO THE MIGRATION PROCESS

Why were standards applied? Standards consist of principles, procedures, methods, and practices usually developed by industry subject matter experts. Organizations that apply standards to their RIM programs generally do so on a voluntary basis. Standards promote efficiencies and effectiveness, and to the RIM team they signified best practices as the team focused on the required elements and defined the framework to achieve efficiencies, create economies, and improve the quality of the process.

CPS CASE FILE RECORDS CONTEXT

Calgary, Alberta, has a population of approximately 1.3 million. Since 1885, the city's law enforcement has been provided by the CPS, which now employs more than 2,000 sworn and 700 civilian members. The police respond to an average of 500,000 calls for service annually; of those, more than 100,000 calls become case file records, forming one of CPS' most valuable records series.

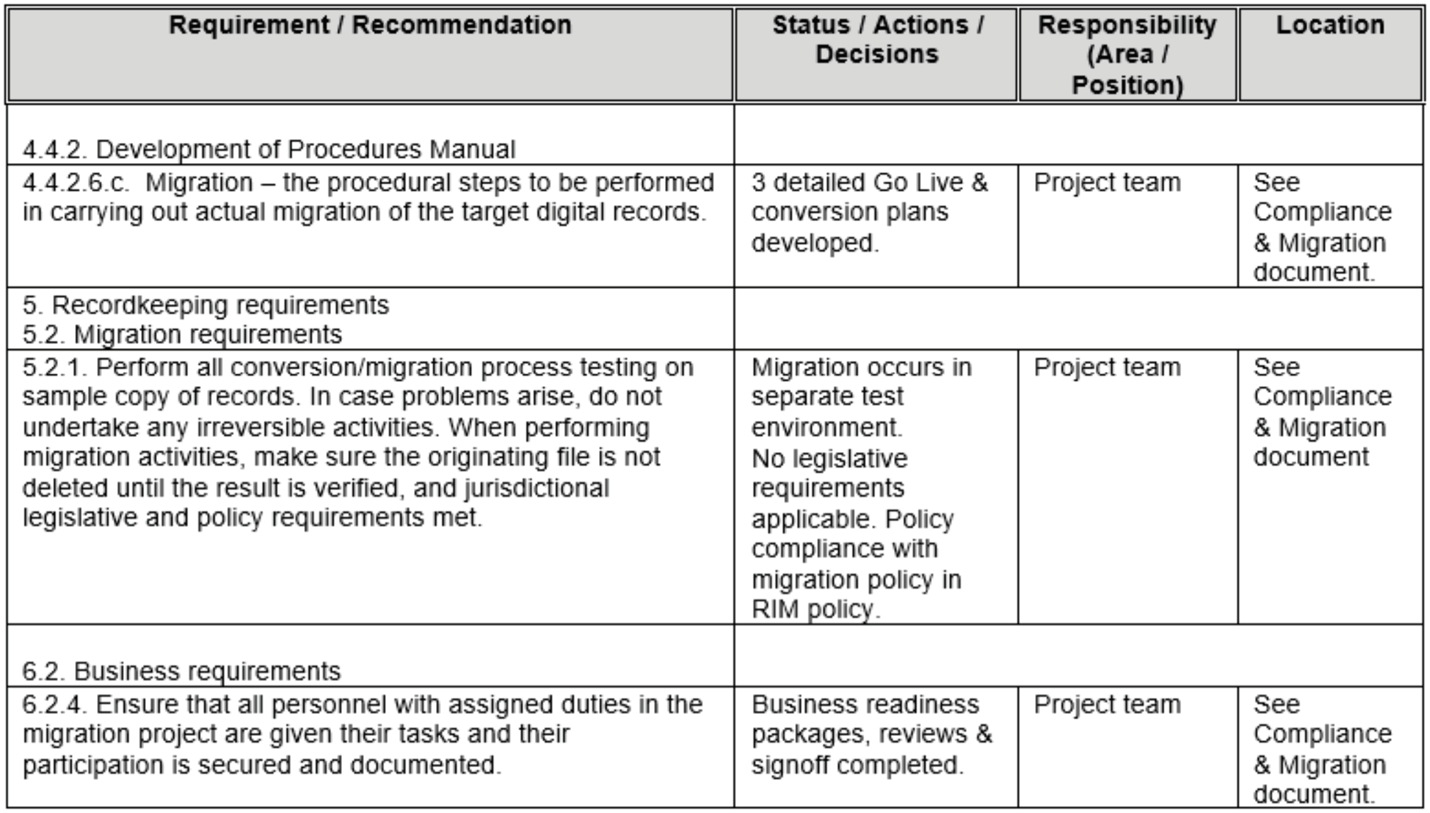
This records series includes victim, suspect, and witness personal identifiable information; the full details of the occurrence, case, or incident; plus arrest reports, vehicle information, court documents, criminal charges, and other relevant information required as evidence. Each criminal case file record is identified by a unique case file number.

The legacy system maintained criminal case file information according to CPS' records retention schedule. Records for major cases, such as homicides, sex crimes, and robbery, are permanently retained. Those for minor cases, such as breaking and entering, criminal traffic incidents, and domestic conflict, have a 40-year retention, while records for minor traffic cases are kept for 10 years. Over the years, IT performed many modifications and upgrades to ensure the collection and preservation of relevant police information was maintained, but some years ago it was evident the legacy system's life cycle was nearing decommissioning and the legacy information would have to be migrated.

THE CHECKLIST APPROACH

How are requirements and recommendations identified in the standards? The language of standards uses "shall," "should," and "may" statements. "Shall" denotes mandatory requirements; "should" is a recommendation; and "may," is an option. The RIM team, which included the records manager and the information management coordinator, designed the spreadsheets to identify the applicable requirements and recommendations in each standard – see Figure 1 – and how the organization responded to them.

In Figure 1, the requirements and recommendations column is followed by columns addressing the status/action/decision required to complete the requirement, who or what area was responsible, and the location of the documentation generated in support of the criteria, such as mapping activities, planning documents, screen shots, workflows, decision documents, flow charts, logs, risk assessments, procedures, and other relevant documentation.



Requirement / Recommendation	Status / Actions / Decisions	Responsibility (Area / Position)	Location
4.4.2. Development of Procedures Manual			
4.4.2.6.c. Migration – the procedural steps to be performed in carrying out actual migration of the target digital records.	3 detailed Go Live & conversion plans developed.	Project team	See Compliance & Migration document.
5. Recordkeeping requirements 5.2. Migration requirements			
5.2.1. Perform all conversion/migration process testing on sample copy of records. In case problems arise, do not undertake any irreversible activities. When performing migration activities, make sure the originating file is not deleted until the result is verified, and jurisdictional legislative and policy requirements met.	Migration occurs in separate test environment. No legislative requirements applicable. Policy compliance with migration policy in RIM policy.	Project team	See Compliance & Migration document
6.2. Business requirements			
6.2.4. Ensure that all personnel with assigned duties in the migration project are given their tasks and their participation is secured and documented.	Business readiness packages, reviews & signoff completed.	Project team	See Compliance & Migration document.

Figure 1: ISO 13008

The IT team: the database administrators, and the project team (composed of the readiness team, data migration team, quality assurance, UAT, etc.), were responsible for updating the checklists, which were completed primarily by the project team. The project team had both internal personnel and consultants. To protect the security and confidentiality of the information and the integrity of the organization, personnel are security cleared and polygraphed.

Revisions to the checklists required both the IT and RIM teams' agreement, with approval from the project manager; final sign-off was given by the superintendent whose area was responsible for the migration. The teams met regularly to discuss the checklist process and any challenges they were experiencing.

If the IT team was not able to speak to a requirement or recommendation, it provided the reason. For example, CAN/CGSB 72.34 specifies organizations are obligated to preserve recorded information as soon as litigation is contemplated or foreseeable. Because there was no litigation, and none was anticipated during the migration process, the IT team correctly noted that this requirement was not applicable.

Both standards require that all phases of the migration process are addressed in an approved procedures manual. CAN/CGSB 72.34 specifies the manual must outline detailed procedures ensuring that the records' structure content, identity, and recordkeeping metadata are captured. ISO 13008 states that the procedures manual is designed to mitigate risks and to control the migration process targeted at preserving the integrity, authenticity, reliability, and usability of the records. In compliance with the standards, the teams documented the planning, testing, migration, validation, sign-off, and documentation phases of the migration process (see the side bar).

APPLYING CHECKLISTS TO THE MIGRATION PROCESS

The IT team depended on checklists to help assure a successful migration and used them as step-by-step tasks to meet the requirements of all phases. Importantly, the components of the lists also revealed what "done" was, which helped the team start with the end in mind, knowing what the project completion should look like. Essentially, the checklists made the final goal accessible.

Figure 1 provides three examples of applying the checklists to the migration process. For example, point 4.4.2.6.c addresses the procedural steps to be performed for the actual migration of the records. The IT team described three detailed "go live" plans, which formed part of the documentation for the migration. These plans, the Soft Go Live, Service Go Live, and Case Conversion, were included in the movement of the historical cases from the legacy system to the RMS.

The second example, 5.2.1, requests that migration process testing be performed on a sample of the records. In response, the IT team created a data conversion environment to test data migration between systems using a small subset of data. The data was migrated to the new environment and tested by the QA team.

According to ISO 13008, the records migration process must address the following phases:

– Planning – the procedural steps, methods, people, and other resources to execute a successful migration.

– Testing – tests required to verify the planned procedures yield a successful migration.

– Migration – procedural steps to be performed to carry out the actual migration.

– Validation – procedural steps used to verify that records are successfully migrated.

– Sign-off – authorizations required to verify the migration was successfully completed in compliance with approved policy and procedures.

– Documentation – details records of the migration during each migration project.

The environment was wiped and a complete remigration occurred.

At each step of the migration, reconciliation points were required that had to balance between source and target. The balances on reconciliation, data content, and quality were tested by an independent party walking through a manual comparison between the old and new systems. A percentage of different case types was selected randomly for this testing. Finally, a dry run was completed into the actual production environment. The "go live" did not occur until all data was successfully migrated following a detailed cutover plan into production and the process of migrating and verifying was 100% accurate. Once signoff was completed on the dry runs, a go/no go was completed.

Lastly, point 6.2.3 focuses on the stakeholders and users of the records system and their level of involvement. The IT team prepared business readiness packages, reviews, and signoffs ensuring that an example of the packages was included as part of the migration documentation. The team defined readiness as business processes that were validated and accepted by business areas. All employees were trained and able to perform their specific jobs, and, if appropriate, the areas were engaged in testing their specific functions. Stabilization and sustainment measures were developed and implemented through partnerships with the different areas. Communications were prepared to be disseminated throughout the organization when the production environment was ready.

THE MIGRATION PROCESS

All case file information in the legacy system that was to be migrated (for example, victim, accused, and witness names, addresses, telephone numbers, charges, vehicle license plates, and more) was logged and associated to the case file's unique case number. This information was replicated into an SQL database, and counts were taken (total number of names, total number of addresses, telephone numbers, etc.). The populations were compared and tested to the information in the legacy system. Volunteers helped validate the sample quality of the content, creating detailed records of each test. All documents that were generated to describe the migration process were captured in the Compliance-Conversion and Migration document.

In terms of the timeline, the RIM team delivered the checklists to IT in early 2015; the migration was completed in late 2016; and all documentation was finalized by year-end 2017 and permanently stored in CPS' electronic document and records management system. The migration was scheduled for a weekend in order to reduce disruptions to the business. On that day, a systems outage was necessary to execute the process. Due to operational concerns and dependencies on CPS information by the police and its partner agencies, the systems could not be kept down for a long period. Coincidentally, just as the team was about to begin the migration process, a police action occurred and the migration had to be delayed for a short time.

Despite the minor set-back, the migration of more than 3,900,000 case file records was successfully executed. While the checklists directed the process, it was the IT team's efforts, energy, skills, and persistence that ensured the recordkeeping and admissibility requirements were met throughout the process.

SUCCESS ACHIEVED!

The RIM team defined success in a number of ways – for instance, having the legacy records migrated in their entirety, while preserving their integrity, authenticity, reliability, completeness, and usability. All recordkeeping and admissibility requirements had to be met in compliance with the standards, and the risks – such as records loss, deterioration, or corruption – had to be mitigated. Additional signs of success were ensuring that all checklists were referenced throughout the project planning stage and that the required documentation was produced during the testing and execution phases.

Owing in part to the IT team's thorough capture of the requirements and fastidious monitoring of checklists, the RIM team's definition of success came to fruition once the records were migrated according to the foundations the team thoroughly researched and itemized. From the beginning, the RIM team provided clarity of purpose and made recordkeeping processes accessible to the IT team in layman's terms. Providing oversight to the entire process, the RIM team assured and delivered open communications, which clearly resulted in positive long-term effects.

LESSONS LEARNED

In evaluating the migration process, the RIM team found that in its eagerness to capture the requirements of CAN/CGSB 72.34 and ISO 13008 in the checklists, there were elements of repetition because both standards discussed similar requirements. But, since it was vital to capture and address all tasks, the team decided it was more beneficial to over-represent than to under-represent the requirements.

While the entire migration process was an invaluable experience, it demonstrated that the requirements provided in both standards substantiated that there were no gaps in capturing the RIM functionality that addressed recordkeeping and admissibility criteria. IT responded positively in ensuring that the records were court-worthy and their content, context, and structures were in compliance with the standards. The checklists were pivotal to the migration process because they kept the tasks and project work on track, managed the risks, provided the requirements status (whether completed or outstanding), and controlled all processes.

about the author

Uta Fox, CRM, FAI

Uta Fox, CRM, FAI, is manager of the Records & Evidence Management Section of the Calgary Police Service in Alberta. Earlier, she was manager of the Records and Information Management of the police service. Fox has a Master of Arts degree from the University of Calgary.

ARMA PRESIDENT-ELECT SAYS EXPANDED CALIFORNIA PRIVACY BILL 'UPS THE ANTE' FOR IG

California Attorney General Xavier Becerra endorsed a bill last week that expands the state's new privacy act to permit consumers to sue companies over their handling of personal data. The privacy law that was passed in 2018 gave consumers the right to sue only in the case of a data breach. The new bill allows them to sue over any violations.

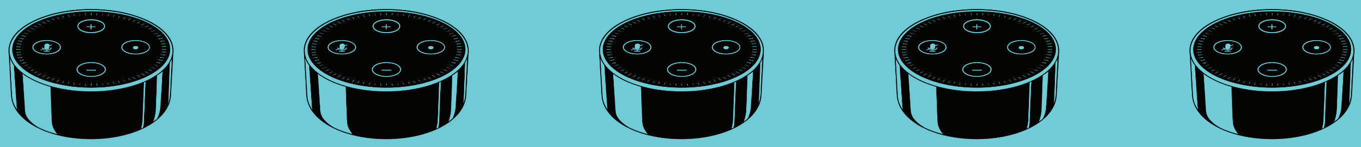
Becerra acted against the wishes of tech lobbyists, according to Reuters.

Jason Stearns, ARMA's president-elect, says the expansion of "the most significant change in the U.S. privacy landscape" heightens the need for a strong IG program within organizations.

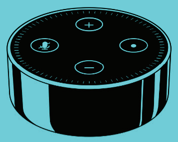
"This proposed bill supported by the AG ups the ante yet again and reinforces the need for organizations to have a robust privacy program that is fully integrated into an overall information governance framework," he told ARMA.

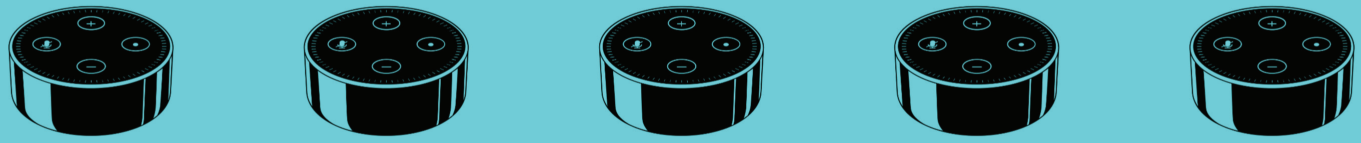
The expanded bill cuts a provision that gives businesses 30 days to "cure alleged violations without penalty. It also says that companies are no longer entitled to seek the guidance of the AG's office on whether they're in compliance. "We do not give out free legal advice . . . paid by taxpayers," said Becerra. Instead, the office will publish general guidance on how to comply.

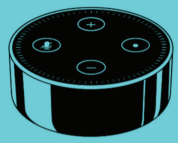
One way to begin to comply, Stearns advises, is to acknowledge that the days of "keep everything" are behind us: "Organizations must be proactive and aggressive in their efforts to identify, control, manage, and ultimately disposition the data they collect and create, particularly personal data." The tech lobby claims that such wide-ranging protections will be "staunchly" fought in Sacramento and Washington. Further, as Reuters reports, many business groups are pushing for a national privacy law that would supersede state legislation before the California Consumer Privacy Act takes effect in January.



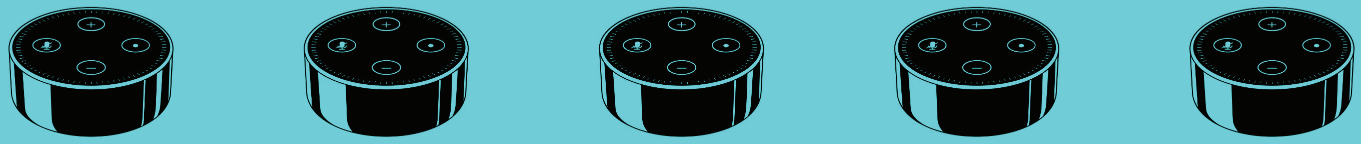
'ALEXA, FIX MY RECORDS!'



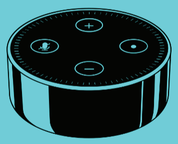


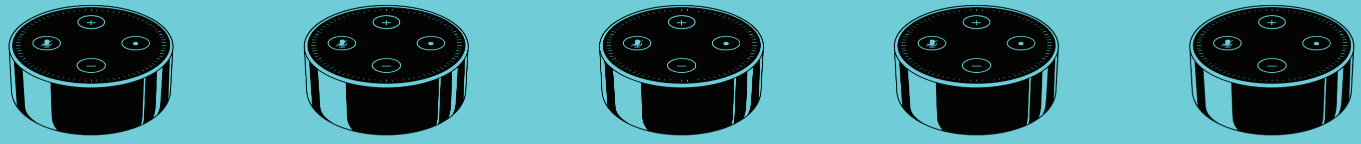


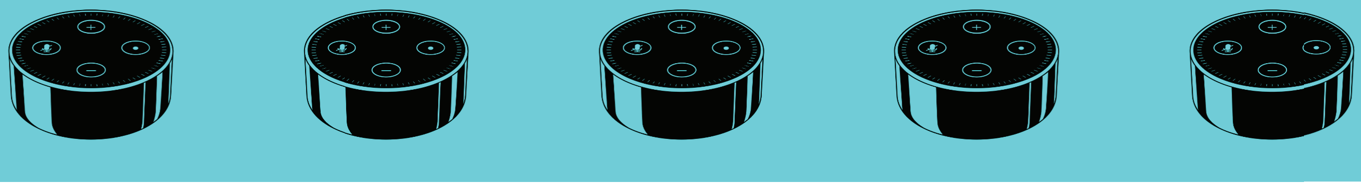
A LOOK AT AI IN THE INFORMATION PROFESSION



JEFF HUTCHINGS







To many people, “artificial intelligence” is a bit of an oxymoron. It is the suggestion that we can create something that then can be creative on its own. If intelligence is the ability to acquire and apply knowledge and skills, requiring a measure of judgement and reasoning, can we create such a thing through mechanical or digital means?

Some scholars suggest that artificial intelligence (AI) isn’t intelligence at all, but rather an advanced machine skill-set that is mathematically driven and facilitated by humans.

We are yet to build a machine that we can ask to complete without human input a task that it has absolutely no knowledge or familiarity with. The process so far has been for human beings to feed AI software a foundation for its processing wizardry.

In contrast, humans will draw on their own non-related past experience and intellect to ascertain how to approach the task with the best results. This is keeping us gray-matter-driven innovators ahead of the bots . . . for now, at least.

Will we get to the point with AI whereby machines eventually become creative and evolve to having their own perceptions, judgements, and reasoning? Renowned physicist Stephen Hawking said there is potential for the machine to become superhuman, and Elon Musk, innovator and chief of Tesla Motors, suggested machines will become superhuman if we can put network infrastructure in place to handle the bandwidth required for such quantum processing.

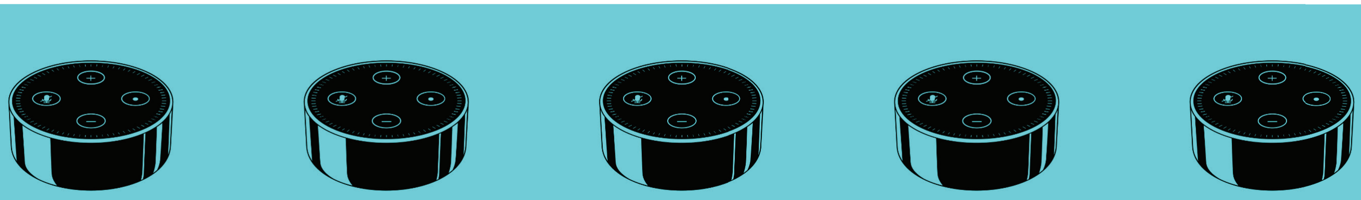
In any case, AI (in some form and with its self-learning potential) is here, and this is where it gets very interesting, even for IM professionals.

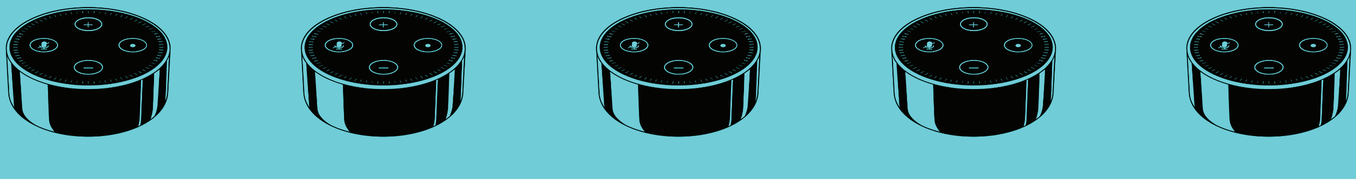
"Alexa, Turn Up the Heat a Little, Please"

In everyday life, we have software (Nest, for instance) that automatically adjusts room temperatures according to data it gathers on our living habits; we have Alexa or Siri providing weather data and advising which highways to avoid on the way to work; we have AI that monitors livestock from satellites; and we have airplane autopilot functions that can respond to environmental and mechanical scenarios.

Some time ago, a computer playing chess would choose among the hundreds of thousands of possible strategic moves that it had been fed. Using layers upon layers of processing, it was able to respond to its human opponent and in many cases win.

Google then took that capability farther. Alpha Zero, Google’s answer to IBM’s Deep Blue chess-playing computer, was fed the rules of chess and nothing else, and yet it was able to make intuitive discernments that





led to masterful move selections, making it even more successful than its predecessors.

This is where machine skills start to look more like intelligence.

"Alexa, What's New in AI?"

In the same vein, machine language translation has evolved in such a way that machines now make inferences about languages. Essentially, a machine can be fed a few basic structures around a language – French, for example – and from that data it can infer the rest of the language translations into English. It isn't perfect, but it's functional – and very fast. In essence, machines have gotten to a place where they teach themselves how to learn.

Another great example of machine advances is the confluence of AI and 3D printing. Industrial manufacturers, for example, can now create a rough prototype of a piece of machinery or a mechanical part and feed this information to a system, along with suggested materials, cost requirements, and usage data. AI then takes these inputs and, using the internet as its brain, comes back with suggestions, alternate material types, alternate design types, and even test results on its findings. The manufacturer can then 3D-print the part onsite – a step that's called “additive manufacturing” – and test its suitability.

“Alexa, Show Me What We Have on Asset Management for Our Latest Infrastructure Project”

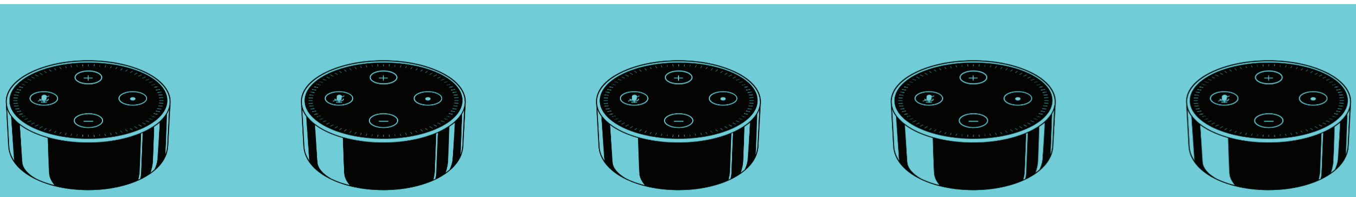
Given the fact that AI is emerging virtually everywhere, especially in the technology we use every day in our work and play, it's not surprising then that the information profession is also undergoing some radical changes and adjustments due to AI.

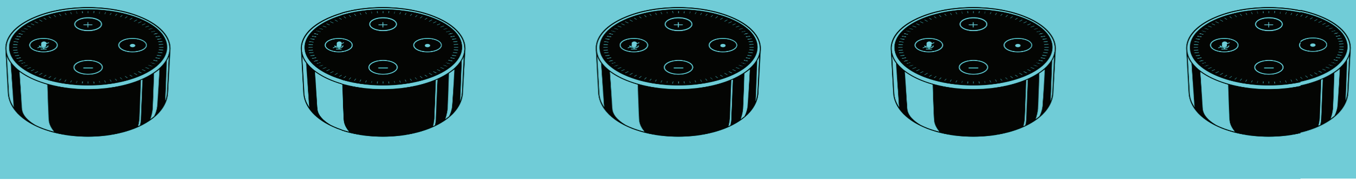
Currently, multitudes of companies are adopting AI-driven solutions (machines and software) that are compiling and managing their information. Such technology is cross-platform, media neutral, astonishingly intuitive, and easy to use. In fact, we may soon rethink our notions around collecting, analyzing, and storing information.

Those like John Mancini suggest that the IM world needs to get away from thinking that data should be housed in a single repository, as well as to start focusing more on the value and role of metadata.

“Alexa, Search Outlook and My Network Folders for Anything on the ‘Acceptable Use of the Business Network’ Policy”

AI in software – M-Files, for example – is making it possible to work with information on virtually any platform in any location.





Analysts and proponents of these solutions are referring to them as intelligent, repository neutral, and metadata driven.

A single search for a type of information can draw accurate results from Outlook, SharePoint, shared drives, cloud storage, and an electronic document and records management system (EDRMS), to name a few. There is no need for data migration because the software provides a contextual view of the information while leaving it in place.

Search results are available in practically any format, highlighting and bringing to the forefront virtually any subsets of information.

Cross-references can be made between a multitude of media types, from images to PDFs, and this data can be compiled and analyzed in many ways through a very user-friendly interface. AI uses labels, key words, or even patterns to compile inventory information. Such software can also compile and save relationships between information that exists in different physical locations.

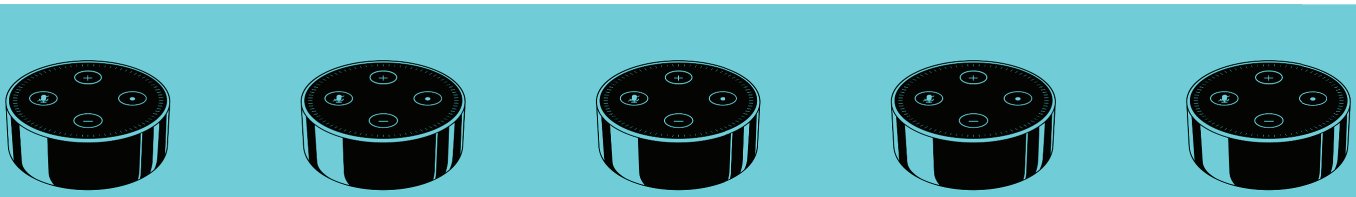
Imagine the implications for audits and inquiries.

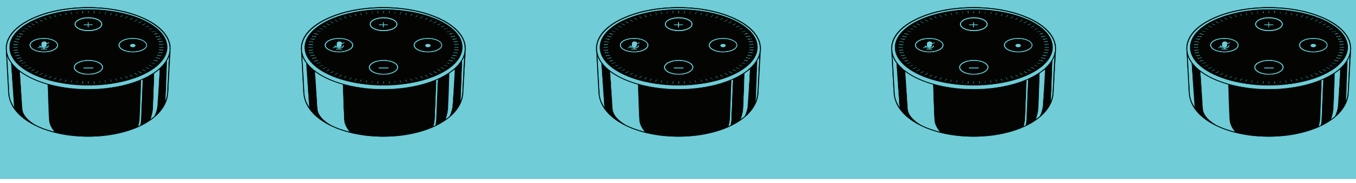
"Alexa, Read This for Me, Please"

Thanks to recent AI advances, existing information can be automatically analyzed and enhanced. Recent advances in AI development mean that machines can now read information in natural language, meaning it is "understanding" what it is reading and is then able to make determinations and inferences from the same. AI reading a case study, as an example, can now identify what factors led to a particular outcome or decision.

In other words, instead of organizing data to run through predefined equations, these "deep learning" capabilities set up basic parameters about the data and train the computer to learn on its own by recognizing patterns using multiple layers of processing. Machine learning algorithms can comb through unstructured text and learn about the format and the content as they go. Law firms, for example, are now having AI tools read thousands of pages of legal precedents and case law to give them succinct analyses and reports on matters of litigation. The time-saving is enormous.

This means our IM software can read a document, identify and fix data discrepancies, highlight information around retention schedules such as disposal dates, and add to (or correct) the existing metadata. The software is also programmed to be on the lookout for duplicate information as it compares the data it's examining with what it has processed in the past. Accordingly, AI may mean that redundancy will become a





thing of the past.

Many images that have been loosely classified without much background information can be enhanced as AI performs image recognition and pulls information about the photo or image from any repository at its disposal. It's like holding your phone up to a landmark and having it tell you the story of what's in your camera frame. In essence, using Google as its brain, AI then writes the more concise metadata for your photo.

"Alexa, File This for Me, Please"

The advances in AI also have parallels in the information profession.

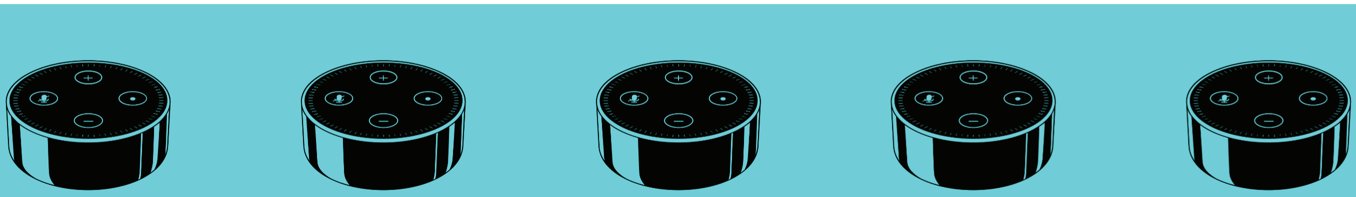
As for new information we intend to hold or new records we're creating, AI can process and manage these with amazing accuracy and efficiency. We simply classify a few of the incoming records and their relevant metadata and then let the software do the rest. Then we scan the subsequent information, or create it as is done in the normal course of business, and have the software name, describe, categorize, and file it. Additionally, AI software tags the information so it becomes discoverable under several categories. For example, a record on litigation concerning a failed overpass can be tagged in such categories as construction company information, cement manufacturer, environmental conditions, and litigation outcomes or errors.

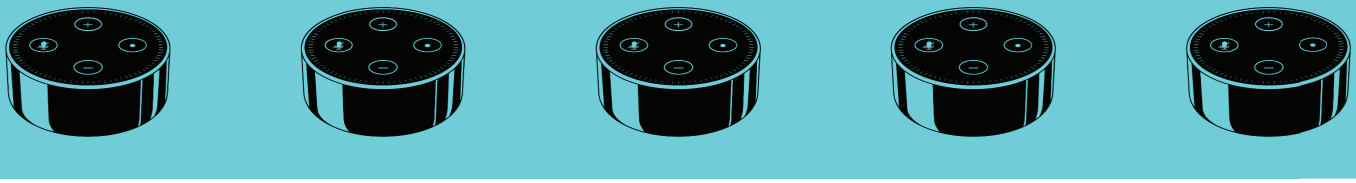
Interestingly, AI is not simply copying the classification methods it was taught in the initial stages; it's actually analyzing each lot of information and enhancing the categorization or metadata where it sees fit.

In this process, AI is in analysis mode and can monitor new records for discrepancies, missing data, or redundancy. It's also mining existing information for direct or indirect relationships with other stored information. Such checks and balances are proving to mitigate errors in client transactions as well as augment information integrity – and are exponentially speeding the auditing process.

An access-to-information request goes from mining a half-dozen information holdings individually to a single, carefully orchestrated search that pulls data from any and all digital repositories in the organization. This information is then presented according to the wishes of the search requestor.

Once stored, queries of the data can range from key words to much more complex combinations of desired results. Programs like M-Files are proving they can accurately pull anything from anywhere. Given that the AI queries look at file names, metadata, titles, and content, the results can come from email, draft documents on a network or shared drive, official records from an ERDMS, and



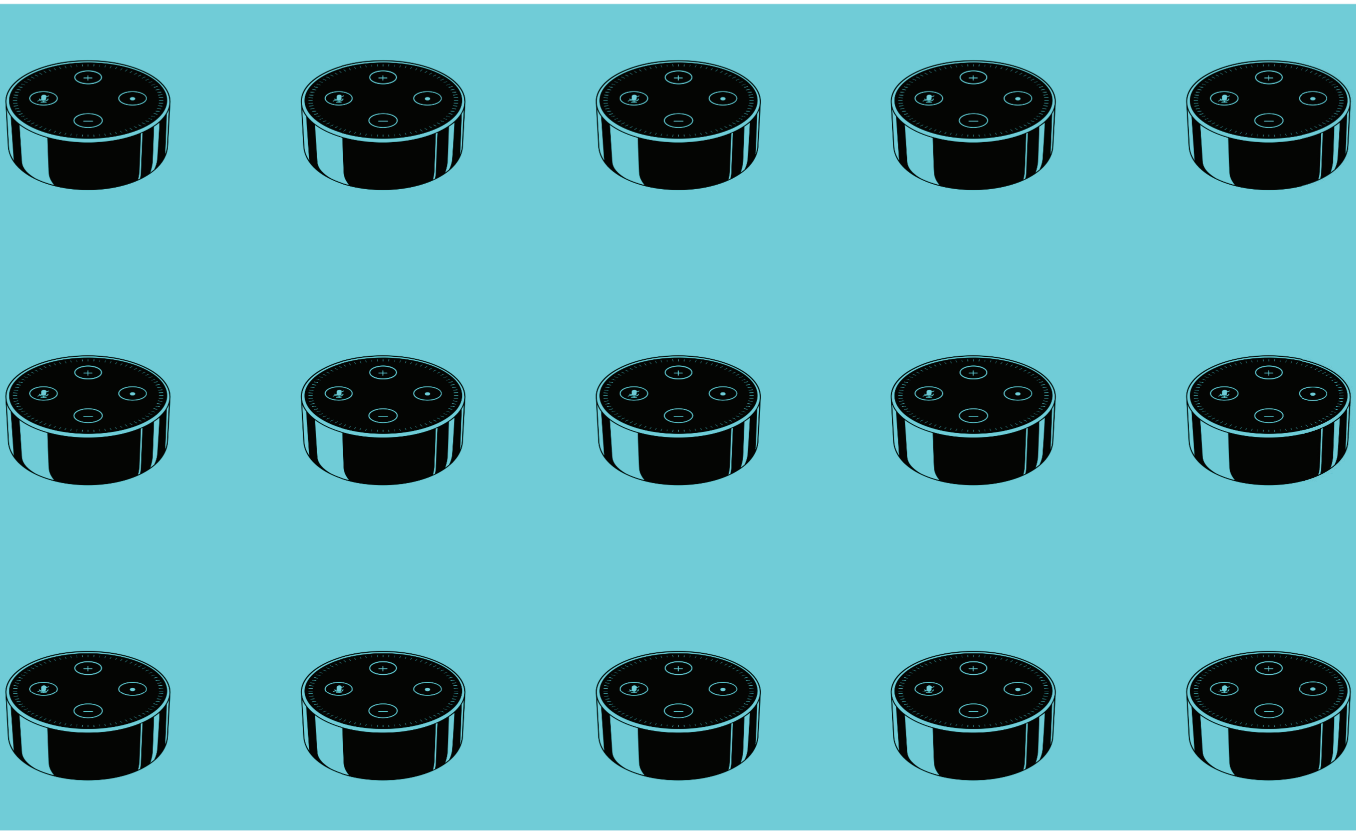


images from a hard drive – in one fell swoop. Such solutions also capture all the changes to the version history and are equipped to keep a full audit trail of changes.

Hence, it appears that AI is helping information managers meet their quality and compliance requirements more easily.

However, let's just hope that AI innovators are working to enhance and augment the human experience, not replace it.

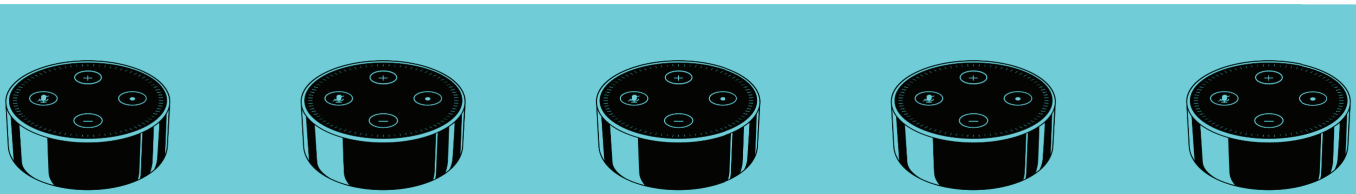
"Alexa, I'm gonna need another coffee."



about the author

Jeff Hutchings

Jeff Hutchings is an IM Professional with the Government of Newfoundland and Labrador, a published author, blogger, and avid Martial Artist. Jeff's study and teaching of Shotokan Karate involves the practice of mindfulness as it relates to daily living.



BEYOND COMPLIANCE: EIGHT STEPS FOR USING PRIVACY BY DESIGN TO DEVELOP A PRIVACY PROGRAM

ELSE KHOURY

Governments globally are passing strict information privacy laws and regulations, and organizations are being hard-pressed to comply with them or suffer stiff penalties. Using the principles of Privacy By Design, organizations can design a privacy program to meet this challenge.

Mandatory privacy breach reporting. Privacy impact assessments. Access to information requests. The right to be forgotten. If these terms, which pop up in regulations like the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act, and Canada's Personal Information Protection and Electronic Documents Act strike fear in your organization, it's not alone. Identity theft, reputational damage, and class action law suits are just some of the known results of data breaches.

UNDERSTANDING PRIVACY IMPACTS

In 2013, when Edward Snowden revealed the extent of government surveillance over private citizens by the U.S. National Security Agency, the conversation about privacy began its slow crawl from the tin-foil-hatted conspiracy theorists hiding in off-the-grid cabins to the average suburban living room. Suddenly, regular citizens were beginning to question the extent of their vulnerability and the vast amounts of personally identifiable information (PII) they have given away, willingly or not. Six years later, questions on privacy and security increasingly demand attention. The privacy conversation has even permeated the pop culture bubble: where would the plot lines of television's "Mr. Robot" or the Bourne movie trilogy be without it?

Adding fuel to the fire, an abundance of global data breaches has exploded, taking corporate bottom lines and personal privacy down with them. While the Equifax, Yahoo, and Ashley Madison breaches resulted in heavy losses to their parent companies and damage to the vendor-client relationships, it is easy to lose sight of the fact that privacy breaches cause real, individual, human harm. In Canada alone, two individuals affected by the 2015 Ashley Madison breach were known to have taken their lives immediately after client data was posted online: in a very real sense, privacy breaches ruin lives.

Against this backdrop is an evolution in the general public's understanding of and demand for privacy rights. Both the UN Declaration of Human Rights and the International Covenant on Civil and Political Rights recognize privacy as a basic human right. Some argue that without the right to privacy, other rights are moot. Globally, governments have been seeking to create or amend their own privacy legislative frameworks in response to the changing landscape of digital data and risks associated with conducting business on the Internet.

While the introduction of new laws certainly increases accountability, for organizations unused to a framework of rigorous privacy compliance requirements, the demands can feel overwhelming. But the alternatives are worse: with fines of up to 2% of annual turnover under the GDPR, non-compliance is a non-option.

PUSHING PAST COMPLIANCE

Privacy compliance requirements, with their complex accountability structures and processes, require a great deal of time and consideration to implement. The question then becomes: How can an average organization improve privacy compliance without shutting down business or placing a complete stranglehold on productivity?

Perhaps the best way to get started is to take the view that compliance is a continuous process of change, not a singular effort like developing a privacy officer position or drafting a privacy policy. To ensure that compliance happens, privacy needs to be addressed as an ongoing, corporate-wide, behavioral shift. Fortunately, there is a methodology that can help organizations get to compliance, and even push past it by integrating its principles into the organization's culture.

USING PRIVACY BY DESIGN

Privacy By Design is the brainchild of Ann Cavoukian, Ph.D., Distinguished Expert-in-Residence and Leader of the Privacy By Design Centre of Excellence at Ryerson University in Toronto, Canada. "Privacy By Design was developed at my kitchen table," Cavoukian recalls of her time as Ontario's information and privacy commissioner. "I wanted to find a way to build privacy into the design stages of technology."

Privacy By Design was a revolutionary concept when it was unveiled by the Office of the Information and Privacy Commission during Cavoukian's tenure. It's a surprisingly accessible methodology that focuses on balancing productivity with the end goal of protecting privacy, in what Cavoukian has repeatedly described as the "positive sum" paradigm. "Privacy By Design takes a positive-sum position in order to accommodate all legitimate interests," she said. "We don't talk about privacy versus security, for example, but how to accommodate both."

Creators of the GDPR used Privacy By Design as a foundational principle when developing the regulation, and the same approach can be applied in an organization that is attempting to become privacy compliant. Privacy By design focuses on a preventative approach, which is probably the greatest shift an organization will have to make: thinking about putting privacy-protective measures in place before something bad happens. If an organization is really committed to ensuring that it doesn't end up as a national headline, this is where it needs to start: establishing a privacy compliance infrastructure that develops the tools necessary to take the organization to compliance and beyond.

BUILDING A COMPLIANCE INFRASTRUCTURE

Building a privacy compliance infrastructure requires organizations to take the following eight actions:

1. UNDERSTAND REGULATORY / COMPLIANCE OBLIGATIONS

Before looking at implementing any kind of privacy program, an organization needs to understand what its obligations are. This begins with a simple question: What enables the organization to do what it does? In health care, for example, there are regulations or standards that define the boundaries of the services an organization provides, such as vaccinations or palliative care. These laws define the limits of service, which means the organization can collect, use, share, store, and eventually destroy information only for those purposes. This is called consistent purpose, and it is the basis for all further privacy considerations. Any information that that does not fulfill that purpose has no place in the organization unless it has been collected with the information subject's consent.

2. IDENTIFY THE ORGANIZATION'S INFORMATION AND WHERE IT'S LOCATED

It is imperative for an organization to ensure that it doesn't have PII that does not meet the definition of consistent purpose. This can be tricky; in the age of mass data proliferation, many organizations do not have a complete view of the PII they hold or where it is located.

But, organizations can't begin to implement protections on personal data until they know where to find it. There are many tools available to help identify and locate digital information, but organizations must "go deep" to ensure that they have considered information in all formats, including paper.

3. GAIN EXECUTIVE SUPPORT

The role of management is fundamental in ensuring the success of any privacy program. Unless the organization's board of directors or executive management team has vocally confirmed its commitment to privacy, it's likely that compliance at other levels of the organization will be sub-par. That commitment must be demonstrated by executive management's funding, championing, and participating in the privacy program; they need to walk the walk. A privacy program without devoted staff and a budget is doomed to fail.

4. ESTABLISH ACCOUNTABILITY FOR THE PROGRAM

To be clear, efforts toward implementing an infrastructure of privacy compliance will not work without accountability being established. At the bare minimum, an organization must identify a privacy officer (called a data protection officer or DPO under GDPR) or someone else who holds accountability for privacy within the organization. But accountability should not be limited to a single individual who receives and processes privacy complaints; it extends to every individual who interacts with any piece of information that could meet the definition of PII, which includes any of the following:

- Contact information (address, telephone number, email address)
- Employment history
- Gender, race, religion
- Financial information
- Medical information

This means staff in human resources, finance, client relations (depending on what the organization does), and probably other departments have accountability for privacy.

Considering the extent to which personal information may be collected, used, shared, and stored in the organization, what privacy compliance considerations have been put in place? Does the organization conduct regular privacy training by an experienced professional familiar with the compliance landscape? Once that training has been completed, has staff undergone testing to ensure that they understand their responsibilities? Are policies and procedures in place to deal with, among other things, privacy audits and a privacy breach response?

5. DEVELOP POLICY AND TRAINING

It's basic, but it works: developing policies and standards of practice, building privacy into processes, and providing context and direction to all staff are imperative to the success of a privacy program. The key is to make sure that the right information is delivered to the right people. Target the information to the audience, make it useful for them, and follow training with testing (with recorded results) and annual policy review.

6. ENSURE THIRD-PARTY COMPLIANCE

"You can't outsource accountability," Cavoukian said about third-party handling of PII. All third parties that have access to an organization's PII must be made aware of any privacy obligations the organization has and should be required through contracts and agreements to honor those obligations. To help ensure compliance, be transparent about these obligations by building privacy requirements into the scoring stage of the procurement process.

7. INTEGRATE THE PROGRAM INTO GOVERNANCE

Finding a prominent place for the program within the organization is critical for privacy compliance. Senior management should provide the support to ensure that privacy is woven into the fabric of your organization. Without a seat at the right tables, the accountable people may not be aware of new initiatives or projects that contain a privacy risk element.

8. IMPLEMENT PRIVACY IMPACT ASSESSMENTS AND MITIGATION PLANS

Privacy impact assessments (referred to as Data Privacy Impact Assessments in the GDPR) are still the most effective (albeit time-consuming) methods to prevent privacy risks from manifesting in organizations. Together with the infrastructure elements listed above, they will complete a privacy program.

If a privacy breach should occur, an organization must have a formal response in place to contain the damage and control the messaging afterward. As the last line of defense, a strong privacy response plan will doubtlessly save an organization from the misery of the having the breach discovered and disclosed by a member of the public – or worse, by the media.

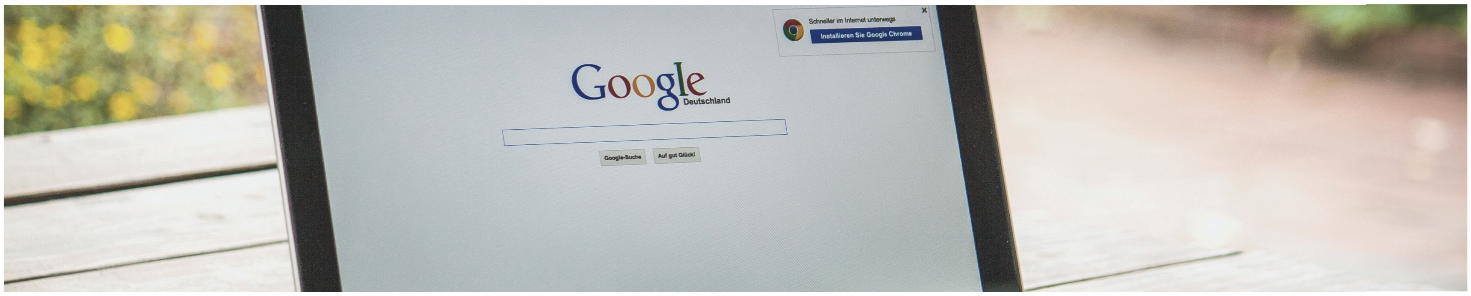
PUTTING IT ALL TOGETHER

Putting a strong and effective privacy program in place is no mean feat. It requires ongoing time, commitment, and support. By using the principles of Privacy By Design as a model, an organization can break down the necessary steps to reach – and push past – compliance.

about the author

Else Khoury

Else Khoury is the Deputy Clerk at The Township of West Lincoln in Ontario, Canada, an instructor at the University of Toronto School of Continuing Studies, as well as Principal Consultant at Seshat Information Consulting



GOOGLE IS FINED $57 MILLION, FIRST MAJOR PENALTY UNDER EUROPE'S DATA PRIVACY LAW

The New York Times was among the many sources recently reporting that the French data protection authority fined Google about $57 million for "not properly disclosing to users how data is collected across its services – including its search engine, Google Maps and You Tube – to present personalized advertisements."

It's the largest penalty given for violating the General Data Protection Regulation (GDPR). According to the Times, it "shows that regulators are following through on a pledge to use the rules to push back against internet companies whose businesses depend on collecting data."

The ruling hits at Google's basic practice of turning user data into carefully targeted ads. France's CNIL, its data protection group, said Google didn't get proper consent from users before processing their data.

The article says that U.S. policymakers are closely watching Europe's experience as a U.S. federal law is possibly under consideration. ARMA International continues to follow these developments closely.

Soo Kang, of Zasio Enterprises, and a member of ARMA's content editorial board, provides the following commentary on the news item:

"While this fine under the GDPR is the largest to date, the significance is not the amount of the fine itself, but the message sent through one of the biggest companies in the world. Even though Google is appealing the decision, the ruling places companies on notice that the data protection authorities are ready to strongly enforce the terms of the regulation. As data protection authorities take note of CNIL's actions, and complaints against other tech giants await resolution, companies must take stock of their respective data privacy practices and assure that it is not merely a paper framework for compliance. Inability to demonstrate effective implementation only serves to expose companies to risk, which is expanding with the ripple effect of GDPR influencing change to privacy regimes around the world."

FELLOWS FORUM

MASTER LEADER OR MASTER SERVANT?

By Dave McDermott

Starting with his role as a team captain on the football field, Dave McDermott set out to become a good leader. From that experience, his father, workplace mentors, and an enlightening book he learned that a successful leader has to serve those he is leading, being willing to "pick up a broom and sweep floors right along the side of the people he or she is responsible for."

Many, many years ago I was fortunate enough to be promoted to the supervisor position within the records management department where I worked. It was an exciting time for me because the promotion was one of my first goals in my quest to become a leader, namely a director. But before we start, let me take you back to the beginning of my leadership journey.

Learning to Lead

During my younger years, I watched how my father managed his construction crews. I admired how he was able to navigate the complexities of managing his framers, finish carpenters, roofers, and other crew members. I grew to appreciate how the men and women respected his strong work ethic and his industry knowledge, and I did my best to emulate him.

Dad was driven to be the best in his field, and he would often say, "To build a good house, you need to be deadly accurate." I think this somewhat applies to our profession, too: to build a strong information governance (IG) program, we need to be accurate and always strive for best practice.

On the Field

My first opportunity to be a leader came on the football field. As team captain, I made decisions about accepting or declining penalties, making shifts in the line, and, most importantly, backing up the other players on the field. I think that's when I started to realize that one of the most important aspects of being a leader is to support the other players. I was always trying to make the right decisions, the right shifts, and the right calls, while also checking the sideline to make sure that I was communicating with the coaches.

At Work

This football experience was important when I took my first position in the IG world as a records analyst for a large corporation headquartered in Boise, Idaho. The position didn't have any management responsibility, but it required teamwork and cooperation with the other staff members. I relied on my work ethic and what I had learned about being a team player.

I saw for the first time where leadership could make a difference in team morale and spirit, and that's when I knew I wanted to do more than be just an employee. To be honest, I thought I would be a better supervisor than my own supervisor. How arrogant was that? I quickly learned that sometimes you must accept and follow the direction of leadership, even if you don't agree with it.

My work ethic paid off in this position, as I was promoted to a record systems analyst. This is where I experienced my first leadership role in project-based work – and I fell flat on my face. I realized that leading people wasn't an easy task. That's when I started thinking about what my dad did to get the best out of his crew, and my thoughts on leadership started changing.

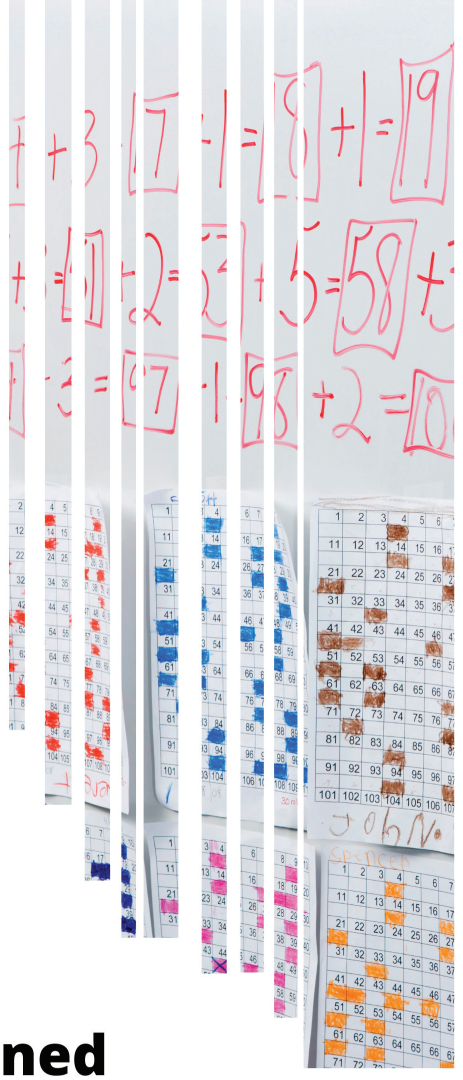
As the years passed, I had several, mostly project-based work – and I fell flat on my face. I realized that leading people wasn't an easy task. That's when I started thinking about what my dad did to get the best out of his crew, and my thoughts on leadership started changing.

As the years passed, I had several, mostly project-based, leadership roles. I was driven and visibly not happy when the folks I was leading couldn't keep up. I learned a hard lesson about the inappropriateness of expressing this emotion from my manager during performance reviews. That's when things started changing for me: I realized that being driven and having a solid work ethic weren't the only qualities I needed to be a successful leader. Far more important is to serve the people you lead and to focus on your staff's needs over your own – but more on that later.

Leading a Team

Let's fast forward to my first supervisor role. When I was promoted, I thought I had the world by the tail. I was finally going to lead people as a true supervisor. I had a staff of five people, all very competent in their roles and very hard working. Boy, did I learn quickly what working with five different personalities was all about!

I was fortunate enough to have a manager (and later a friend) who saw some potential in me and became my mentor. Fred was very patient, while giving constructive criticism and pushing me to be a better supervisor. He would often say, "A good supervisor isn't afraid to pick up a broom and sweep floors right along the side of the people he or she is responsible for." Hmm... this reminded me of my dad's workplace example. I wondered if that was why he was a respected boss and if I was going about this leadership thing all wrong.



Early Lessons Learned

I learned several things during my first few years as a leader:

- **Don't micro-manage. Set realistic goals and let people perform.**
- **Never discount opinions or feelings. Just because you think something is trivial or petty, remember that the person who brings you a problem sees it as a major issue. (That lesson was hard to learn.)**
- **Let your people do it their way. Just because you wouldn't do something a certain way doesn't mean that it won't work. After all, it's about letting them be successful.**
- **Don't lead with an iron fist. Treat employees with respect and listen to them.**

I was happy doing my thing as a supervisor, learning not to lead with an iron fist and adding humor and fun to unpopular projects. But most of all, I was learning to understand my staff members' needs and wants and to treat them with respect. I wasn't always successful, but I was always willing to listen and was quick to offer an apology if I made a wrong decision. Through all this, I never lost my goal of leading the entire department.

Taking on a Larger Role

My manager (another dear friend) thought it was important that I round out my leadership experience by getting involved as a volunteer on the local ARMA Boise Valley Chapter board. (In fact, you could say my two friends set me up.) I learned through this that taking advantage of the opportunities that come with being involved with a professional organization is an essential way to advance your career. This also shows your employees the importance of this type of involvement.

This is not where my professional volunteerism would end. I eventually worked my way up to be elected to the ARMA International Board of Directors (BOD) and then as the BOD president-elect, which meant I moved up to serve as president and, ultimately, as the chairman of the BOD in 2005. I later followed the same steps of involvement with the Institute of Certified Records Managers (ICRM).
My manager told me later that he hadn't wanted me to run for ARMA's president-elect because of the time it would take away from my work duties. But, knowing that I wanted the opportunity to lead ARMA, he reached out to our senior vice president for his input and approval, which was wholeheartedly given. I later learned that my manager postponed retirement for three years so I could complete my leadership terms on the ARMA BOD. His sacrifice taught me a lot about serving the people who work for you.

Lessons Learned Through Experience

- **Sometimes you have to serve your employees, even if it means sacrificing your dreams.**
- **Sometimes you have to let go of people to achieve a better end goal.**
- **Check your ego at the door when dealing with professionals.**
- **It's okay to reach out to your colleagues and peers for advice about difficult decisions.**
- **If you don't provide a clear target, you have nothing to aim at.**
- **Setting functional goals is a key to success.**
- **If you want people to follow you, remain positive; leave the negativity at the door.**
- **Be enthusiastic about decisions, even if you disagree.**
- **Constructive criticism, no matter how painful to receive or give, is valuable for growth.**
- **Know and understand your team members' personalities.**
- **Communication means everything.**

Leading Is Serving

I had more opportunities as a leader when I served as ARMA International's president-elect and then president. The first lesson I learned was leading a paid staff is very different than leading a group of professionals who are accomplished leaders themselves and have diverse personalities, opinions, and experiences. Arrogance or ego wasn't going to win the day here. Was I in over my head? Yup! Did I run from the challenges instead of face them head-on? No way! Not only was I the leader of the ARMA board and membership, I learned that I needed to become their servant, too.

Fellow ARMA BOD members Rick Weinholdt, Juanita Skillman, Cheryl Pederson, and I often talked about the complexities of leading an organization of volunteers and what it would take to be successful. Weinholdt gave me one of the greatest gifts I have ever received, Shar McBee's book To Lead is to Serve: How to Attract Volunteers & Keep Them. The book provides great insight into running a volunteer organization, but, more importantly, it shows how to serve people in a leadership role. I recognized that many of the leader qualities listed in the book were ones I strived for in leading my paid staff. Could it be that leaders are servants to their staff?

I read McBee's book with an open mind and applied many of the things I learned from it to leading ARMA and to serving and setting goals for my paid staff at the company that provided my paycheck. I liked the book so much that I purchased a copy for each ARMA board member, as I relied heavily on them to help ensure we were serving our members and volunteers.

Lessons from 'Leading to Serve'

Some of the values learned from Shar McBee's book To Lead is to Serve: How to Attract Volunteers & Keep Them -

- To attract volunteers, become attractive.
- Clear out negatives.
- Treat staff and volunteers like brothers and sisters.
- When we take good care of what we have, more comes to us.
- Enthusiasm is contagious.
- Individual work is weak. Teamwork is strong.
- Communicating means winning.
- Where there is friction between people, the work becomes weak.
- People want to be heard.
- Be open to suggestions.
- Know your audience.
- Hold back your opinion and simply listen.
- Patience means putting the brakes on strength.

Setting Goals Is Key

Setting foundational goals is key to navigating the waters of serving and leading. McBee's advice for reaching those goals is to "follow the example of water." She explains, "Water reaches its goal by flowing on. When water comes upon a rock, it flows over it or around it. If the water stops flowing it becomes stagnant. If volunteers or staff become stagnant, you never accomplish your goals."

As I navigated the leadership waters of ARMA, we set and accomplished many goals, perhaps the most important being to:

- Create a transparency model for communicating to our members
- Implement an annual strategic planning meeting that included our ICRM partners, the Fellows of ARMA International (FAIs), and others who could help us strategically position ARMA as the leading records management association.

We also made some difficult decisions as a board, including changes in ARMA headquarters and regional leadership. The hard lesson learned from this is that sometimes you have to ask people – even volunteers – to step down to keep the waters of progress from becoming stagnant.

Leading Volunteers Is Different

I came to appreciate the similarities and subtle differences in leading volunteers and leading paid staff. Both must be motivated and passionate about what they are doing, and they need to feel valued and appreciated for their efforts. The latter is perhaps more important for volunteers, who do not have the reward of a paycheck that might keep them engaged, making it much easier for them to quit. At the other end of the spectrum, letting go of a volunteer or a paid staff member who wants to stay is equally difficult, but leaders recognize that sometimes they are left with no other choice.

Leading by Example

I reached my goal of managing an enterprise IG department in the winter of 2006. But I realized after several years of directing the department, that managing people wasn't really what I wanted to do. I discovered that I want to lead by example, serving in a capacity where I can motivate people and provide opportunities for improvement. So, I made the courageous decision to start my own consulting company, providing IG support and best practices to organizations; this includes galvanizing organizations to consider IG as a strategic initiative.

Leading to Success

I encourage anyone who is in or pursuing a leadership role to read McBee's book. It validated how I wanted to lead, and it truly made me understand that even though I may be the leader, my job is to serve the very people I lead. That is what I strived for in my roles as a paid leader and as a volunteer leader for ARMA and the ICRM. I know I wasn't perfect – my eye rolls and body language still get me in trouble at times. Many years ago, ARMA International's president at the time, Ken Hopkins, asked me how I would know if I was successful as a leader. I answered, "If I could help one person come out of their shell and face their challenges, I would be successful." I hope I have done that; I truly do live to serve.

about the author

Dave McDermott

Dave McDermott, CRM, FAI, is an independent consultant, providing information governance guidance and best practices to organizations. With more than 35 years' experience in almost every facet of records and information management, he is a Certified Records Manager, Fellow of ARMA International, and past president and chairman of the board for both ARMA International and the Institute of Certified Records Managers. McDermott can be contacted at idahomcd@gmail.com.

MERGERS & ACQUISITIONS

Dropbox Buys HelloSign, Adds its Coveted Workflow Capabilities

Dropbox has announced its acquisition of HelloSign, an organization that provides document workflow and e-signature services.

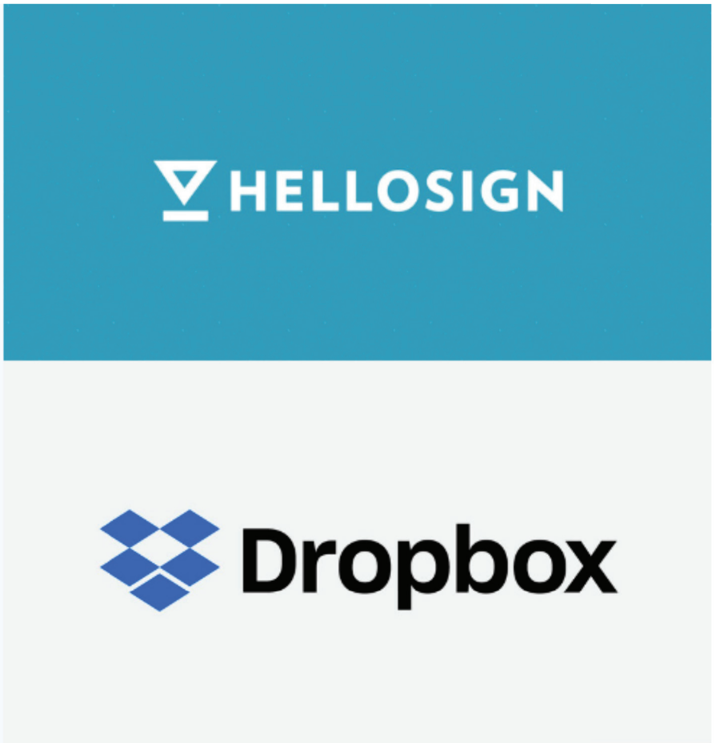
Whitney Bouck, COO of HelloSign, told ARMA International that the company is “thrilled to be joining the Dropbox family.” She said, “With so many similarities between our products, business models, and cultures, it’s a natural fit. This move will accelerate our mission to give customers a better way to get work done.”

Quentin Clark, Dropbox’s senior vice president of engineering, told TechCrunch that the workflow capabilities were integral to the acquisition:

“What is unique about HelloSign is that the investment they’ve made in APIs and the workflow products is really so aligned with our long term direction. It’s not just a thing to do one more activity with Dropbox, it’s really going to help us pursue that broader vision.”

That vision, as noted by TechCrunch, involves extending the storage capabilities that are at the core of the Dropbox solution.

> "This move will accelerate our mission to give customers a better way to get work done."
>
> WHITNEY BOUCK
> COO, HELLOSIGN



Stuck in Rewind? Dynamic E-Discovery for Cloud Data

Tim Anderson

An array of new cloud-based digital sources has emerged across the corporate landscape: chat tools, collaboration platforms, cloud productivity suites, and more. Programs like Slack, Office 365, and Salesforce bring many new and exotic challenges to corporations trying to organize, control, and produce data from these programs, and e-discovery can be particularly daunting when wrestling with the unique characteristics of this data.

In many cloud-based platforms, documents are saved approximately every 30 seconds to ensure that the user's working data is never lost. What results is a string of versions from the original save to the final copy, requiring anyone looking at the export of that data to essentially rewind the document and see each iteration across its life cycle.

Stuck In Rewind

Just as in the days of having to rewind a VHS tape to find the right point in a video, it is time-consuming and frustrating to parse through numerous versions of a cloud-based document to find the one that is relevant to the time frame of a matter. It also introduces a range of stumbling blocks across the discovery phases of collecting, processing, analyzing, and reviewing the information.

Because data is stored in cloud systems this way, documents collected from Office 365 or other cloud sources are essentially dynamic databases, making it increasingly difficult to apply standard workflows and produce accurate results in these types of scenarios. Teams working under tight deadlines to produce a dataset from these sources are increasingly challenged to determine how to pull the information from the cloud and navigate the dynamic and fluid nature of that data. Many are finding themselves stuck with no option but to slowly rewind from document to document.

Breaking Free

Fortunately, advances in e-discovery technology and processes are emerging to address some of the issues brought forth by broad cloud adoption. Teams dealing with e-discovery requests for cloud-based data will benefit from creating standard workflows that specifically navigate the nuances of cloud data sources. This includes leveraging application programming interfaces (APIs) and implementing cloud data connectors to dynamically conduct e-discovery within these platforms, as well as involving experts and using repeatable processes.

Additional steps information management (IM) professionals can take to tackle these challenges – and prepare for future e-discovery requests – include:

- Lean on internal knowledge from the IT experts who helped implement the existing systems and applications, so cloud data sources can be incorporated as part of the organization’s data map.
- Establish a collaborative dialogue with IT to improve future decisions about cloud providers and apps, giving IM and e-discovery teams the opportunity to examine whether cloud providers have export or data interface capabilities that meet e-discovery needs.
- Work with in-house counsel to ensure new data sources are incorporated into legal hold policies and clearly described in litigation hold notices. Similarly, counsel, IM, IT, and information security teams should align around policies that govern and monitor the security and retention/deletion permissions within cloud collaboration and chat platforms.

- Work with in-house counsel to ensure new data sources are incorporated into legal hold policies and clearly described in litigation hold notices. Similarly, counsel, IM, IT, and information security teams should align around policies that govern and monitor the security and retention/deletion permissions within cloud collaboration and chat platforms.

- Take a holistic approach, collecting information across all business units about the various ways collaboration and chat tools are used and training all users on how to use them within the boundaries of organizational data policies.

Two Cases In Point

The two examples below describe where these challenges came to life.

De-Duping in G Suite

Heading up e-discovery for a client involving more than 88,000 documents from G Suite, the team found that many the documents in the collection – particularly among those in Google's equivalent of Word, Excel, and Power Point formats – appeared to be duplicative or displayed very minor variations from document to document.

The six custodians under discovery had a high volume of data that needed to be reviewed, and the team was seeing false positives across thousands of documents. With a little digging, the team found that G-suite saves documents by making a copy of the data every few seconds, which for the custodians of this matter led to more than 20 versions of each document and more than 60% duplication of unique documents.

Every version saved was collected, and because there were only minor variations among them, the e-discovery software's de-duplication features did not work properly. To deal with this, the team produced only the last current version of each document as of a particular date. Using this method, we reduced the original set by approximately 96% and avoided the rewind review of tens of thousands of duplicative document versions.

Using APIs to Crack Salesforce Collection

Data from Salesforce can be especially critical to e-discovery given the roadmap it provides to sales contacts, internal owners of various relationships, how they are all connected, and other market intelligence that can be relevant to a case. In a government investigation, the team was tasked with collecting from Salesforce under a short timeframe.

The platform does allow export of data, but like many cloud solutions, it can be much slower and more complicated to get information out than it is to import it. Because of this, the team was working to use the "front door" to collect the data and found that it would take more than a month and a half just to complete the collection.

Given the tight deadline for the matter, the team needed a more efficient approach, so it instead used APIs to connect to Salesforce and download the records needed. This was exponentially faster, allowing the team to collect approximately 20 million documents in just eight hours. Ultimately, the team completed the collection and subsequent review by the regulator's deadline.

Three 'Ps' for Solving Problems

Office 365 and other cloud-based solutions are solving a lot of problems, making storage more manageable, and increasing efficiencies, but as outlined in the examples above, the e-discovery "gotchas" are just starting to emerge. An approach that leverages the practical tips that are given above and balances between people, process, and technology can help achieve efficient e-discovery on cloud datasets in the following ways.

The Right People

Any e-discovery matter that involves cloud data should be led by experts with hands-on experience in legal discovery. The team should include professionals with a deep understanding of how to use and manage APIs and extract, transform, load (ETL) processes for database usage and data integration. It is also important that those working with the cloud data are familiar with the matter's key metadata, including which dates, people, organizations, and sources are likely to lead to both relevant and duplicative documents.

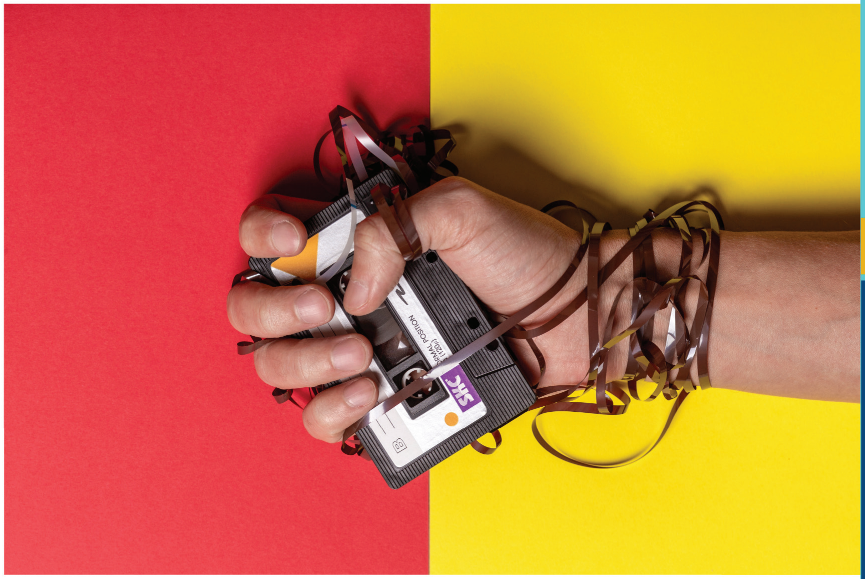
The Right Processes

Systems must be set up for API discovery and data profiling, with workflows standardized around these processes. Standard documentation can be put in place to maintain consistency across all matters. Workflows must include a quality testing model for quality assurance and a maintenance protocol to enable teams to replicate workflows across all matters.

The Right Platform

Platforms must have the capability to leverage APIs to ensure versatile, scalable, and secure data integration. It is critical that counsel be able to view the data in a meaningful way; developers may be familiar with extensible markup language (XML) or javascript object notation (JSON), but lawyers see only blocks of text with illegible letters and symbols.

The platform must also allow integration of the cloud data with other e-discovery sources so all evidence can be reviewed holistically. Rapid development of reusable data connectivity components is another important feature that will allow workflows to be standardized across an organization's entire cloud e-discovery portfolio.



Keeping Pace with Technology

Cloud data is yet another item on the continuum of e-discovery and part of the ongoing struggle attorneys and other e-discovery professionals face to keep practices and workflows apace with evolving technology. As adoption of Office 365 and the emergence of new digital data sources continue to skyrocket, those involved in e-discovery must understand the challenges and be prepared to adjust their standard e-discovery approaches accordingly.

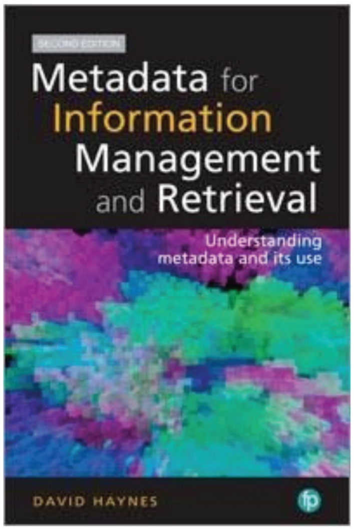
about the author

Tim Anderson

Tim Anderson is a managing director in the FTI Technology segment based in San Francisco. He has more than 15 years of legal technology experience as an application development manager, programmer, systems integrator, and consultant. He specializes in developing strategies for preserving, collecting, analyzing, reviewing, and producing electronically stored information in enterprise data sources, ranging from traditional repositories to cloud-based systems. Anderson can be contacted at Tim.Anderson@FTIConsulting.com.

Professionals in Data Collection and Management Will Find Value in New Edition of ‘Fundamentals’

ANA ROSA BLUE, M.L.S.


SECOND EDITION
Metadata for Information Management and Retrieval
Understanding metadata and its use
DAVID HAYNES
fp

TITLE: FUNDAMENTALS OF COLLECTION DEVELOPMENT AND MANAGEMENT, FOURTH EDITION
AUTHOR: PEGGY JOHNSON
PUBLISHER: ALA EDITIONS
DATE: 2018
LENGTH: 432 PAGES
PRICE: $85.00 | ALA MEMBERS: $76.50
ISBN: 13 978-0-8389-1641-4 (SOFTCOVER)
SOURCE: ALA STORE

Peggy Johnson describes her book Fundamentals of Collection Development and Management (fourth edition) as “a comprehensive introduction for students, a primer for experienced librarians with new collection development and management responsibilities, and a handy reference resource for practitioners as they go about their day-to-day work.” Indeed, those tasked with collection development and management and those responsible for securing, managing, or analyzing company data will find many topics in this book relevant to their work.

Johnson, an adjunct professor in the Graduate School Library and Information Science Program, St. Catherine University, Saint Paul, Minnesota, has more than 30 years of experience in U.S. universities and therefore writes largely from that perspective. Nevertheless, her narrative does weave examples from public, school, and special libraries to make her points, and she sprinkles in some international practices as well. In an ALA Editions blog interview, Johnson says she consulted other librarians in preparation for this edition. The result is a thoroughly researched book that encompasses building and managing library collections regardless of format, genre, or origin.

The author begins with a history of how collection development and management evolved as a specialty within the profession in public, academic, and special libraries. She writes that librarians who provide the highest quality materials to users are “arbiters of quality,” a description this reviewer believes could apply to “all information professionals” as well. Johnson’s book will resonate with information professionals in other settings because she has an appreciation for the significance of managing legacy print collections. If your organization has a combined library, archives and/or records center, this book will be useful.

The notion of amalgamating libraries with archives is not new. For example, according to Dr. Guy Berthiaume, librarian and archivist of Canada, in 2004 Canada was one of the first countries to combine its national library and national archives. Glenstone, in Maryland, has integrated its library, archives, and museum collections into one information management system. More recently, “50 Things You Can Do” to support collections as data was published, by the Andrew W. Mellon Foundation. Any one of those 50 “things” could apply beyond a library setting. There is no doubt that collections and acquisitions managers are dealing with similar issues, regardless of what the collection is or how it was obtained.

Acquisitions/collections professionals have a wide breadth of responsibilities in addition to the selection and acquisition of materials. For example, collections are searchable through finding aids or cataloguing. Further, managing and maintaining a collection is as important as its development. In her book, Johnson addresses issues of weeding, storage, and preservation. For example, she asks if you are weeding for withdrawal or for transfer to storage or elsewhere?

Additionally relevant to any information professional is the book’s discussion of ways to protect your collection from deterioration, theft, mutilation, and disaster. Information professionals will also find value in her discussions of these topics: budgets; ethics; security; selecting access methods for digital resources; ways to identify and solicit materials for inclusion in a digital repository; preservation reformatting and copyright law; mass digitization; preservation plans and collection protection; and marketing and research.

The discussion on vendor relations, negotiations, and contracts is particularly interesting. Johnson has said that “vendors are trained in selling and promoting their products and especially in negotiating effectively.” She maintains that it is equally important for information professionals to acquire parallel skills.

Johnson’s book will be best used as a reference tool. Every chapter contains new suggested readings and fictional case studies to stimulate discussion. Readers are directed to previous reading lists and case studies. The glossary and appendices have been updated and all URLs were valid as of fall 2017. This inevitably means that recent information will not appear in the print edition. Notably, her third edition has been on the curriculum for collection development courses at Indiana University and the University of British Columbia.

Johnson’s new edition is ideal for those starting out in information studies and for seasoned professionals alike. It provides a solid foundation and support to those who bring a wealth of knowledge, skills, and abilities to their collection development and management tasks. You are an “arbiter of quality” if you are responsible for collections at your institutions, and you will benefit from this book accordingly.

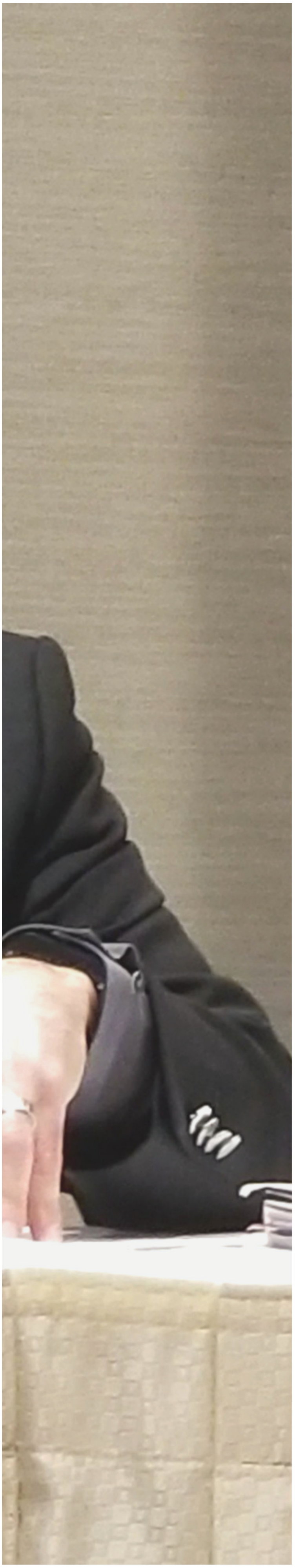
about the author

Ana Rosa Blue, M.L.S

Ana Rosa Blue, M.L.S., has a Master of Library Science degree from the University of British Columbia and a Records Management Practice Certificate from the University of Toronto. She has considerable experience working with corporate, legal, medical, post-secondary, and public information resources and in art galleries as well. She is an Accredited Court and Medical Interpreter (of Spanish) in British Columbia.

Isaza Responds to Illinois Supreme Court Ruling on Biometric Privacy

In January, the Illinois Supreme Court ruled an individual does not have to plead an actual injury or harm, apart from the statutory violation itself, in order to sue under the Illinois Biometric Information Privacy Act (BIPA), as reported by Jeffrey Neuburger of Proskauer. The long-awaited decision stems from Rosenbach v. Six Flags Entertainment Corp.



According to Neuberger's account, because the BIPA statute does not define "aggrieved," many legal arguments and amicus briefs have tried to influence the Court as to its meaning.

John J. Isaza, Esq, of Rimon P.C., tells ARMA International the issue is not necessarily settled: "Despite the fact that this ruling is by the highest court of the State of Illinois, the issue of damages is far from settled. This ruling directly conflicts with, say, the ruling of the 7th Circuit which held that the term 'aggrieved' means there has to be a cognizable injury."

Neuberger of Proskauer writes that the Court looked to prior Illinois decisions and the "commonly understood and accepted meaning" of the term "aggrieved" in stating that it generally means "suffering from an infringement or denial of legal rights."

Importantly, the Court also said that BIPA "compliance should not be difficult," and that the risk to a party's biometric privacy outweighs any expense a business might incur to comply with the law.

Isaza tells ARMA what he thinks may happen next:

"In the interim, there may be a rush to the courthouse with filings from plaintiffs, including aggrieved employees, who simply need to show a BIPA violation without having to establish actual harm for standing to sue and claim $1,000 to $5,000 per violation."

The impact on information managers?

"For records and information governance professionals," says Isaza, "the defense will come down to what data management practices and consent processes are in place to determine if there was a violation of BIPA, and, if so, whether the violation would be deemed negligent or intentional, the latter of which carries the higher penalty." For a more extensive look at BIPA and the issue of biometric screening vs. privacy, see the Information Management article Understanding Biometrics' IG Obligations, by Judy Vasek Sitton.

Legalweek 2019 Kicks Off With Former United States Attorneys General Loretta Lynch and Alberto Gonzalez Focused On Cybersecurity

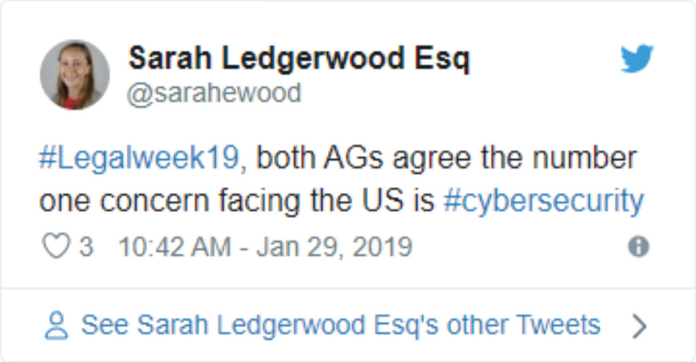
Nick Inglis

Two former U.S. Attorneys General helped kick off Legalweek 2019 by sharing their thoughts on such pressing issues as cybersecurity, privacy, civil rights, and more.

Former attorneys general Albert Gonzalez and Loretta Lynch spoke frankly in a discussion attended primarily by attorneys and moderated by ALM's Molly Miller. (ARMA International, a track sponsor of Legalweek 2019, was represented in the audience as well.)

Miller, the chief content officer for ALM, asked Gonzalez and Lynch to describe what the U.S. government should be most worried about today. Both former officials responded without hesitation that cybersecurity was the most pressing threat.

Gonzalez had earlier noted that there's a "cyber component" to nearly every case these days: "The computer is often the means of carrying out the crime." he said.



Sarah Ledgerwood Esq
@sarahewood

#Legalweek19, both AGs agree the number one concern facing the US is #cybersecurity

♡ 3   10:42 AM - Jan 29, 2019

See Sarah Ledgerwood Esq's other Tweets

Accordingly, Lynch encouraged attorneys to better acquaint themselves with technology. "You don't have to be the IT guy, but we need to train lawyers to have mental flexibility and become comfortable with technology," she said.

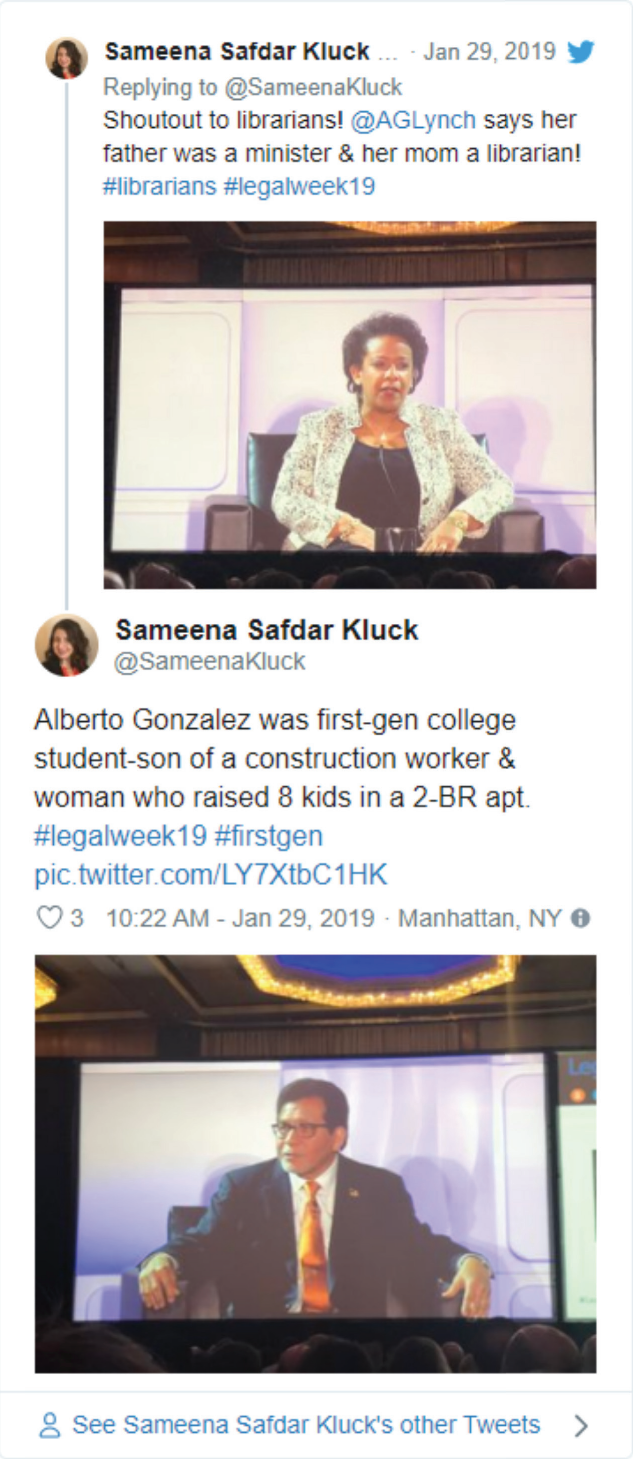
Gonzalez agreed: "You've got to learn technology, folks."

The topic of privacy led to a discussion about the Justice Department's suit against Apple for refusing to help disclose data on the encrypted iPhone that belonged to the 2015 San Bernardino mass shooter. Lynch said that “Technology companies don’t get to decide for all of us how we control and access our data. People have ceded more control of very private data to industry without even thinking about it than I could ever get as part of the government.”

Lynch expanded the discussion to civil liberties by discussing the 2015 Freddie Gray case (in which a suspect was found dead after being transported in a Baltimore police department van) and her role in helping to make police departments more responsive to their communities. She furthered that point in discussing the balance of civil liberties in cases involving terrorism: “We never viewed civil liberties as something that couldn’t be upheld when fighting terrorism . . . we cannot give in to fear.”

Gonzalez served from 2005 to 2007, during the second term of the George W. Bush administration. Lynch served during the final two years of the Obama presidency.

The ARMA International track at Legalweek 2019 was called “Innovative IG,” and it consisted of three sessions during the conference.



Sameena Safdar Kluck ... · Jan 29, 2019

Replying to @SameenaKluck

Shoutout to librarians! @AGLynch says her father was a minister & her mom a librarian! #librarians #legalweek19

Sameena Safdar Kluck
@SameenaKluck

Alberto Gonzalez was first-gen college student-son of a construction worker & woman who raised 8 kids in a 2-BR apt. #legalweek19 #firstgen pic.twitter.com/LY7XtbC1HK

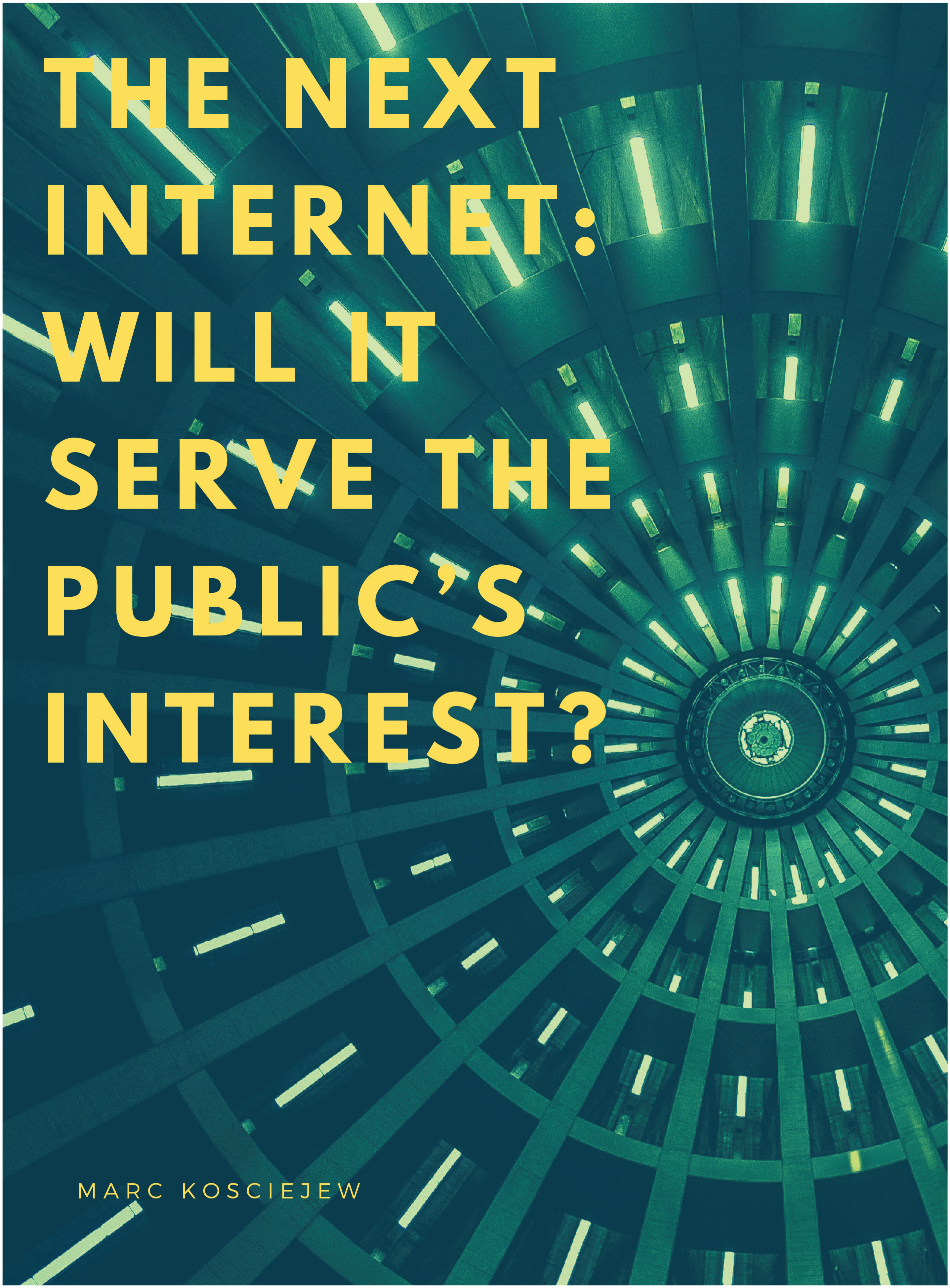
♡ 3 10:22 AM - Jan 29, 2019 · Manhattan, NY

See Sameena Safdar Kluck's other Tweets

about the author

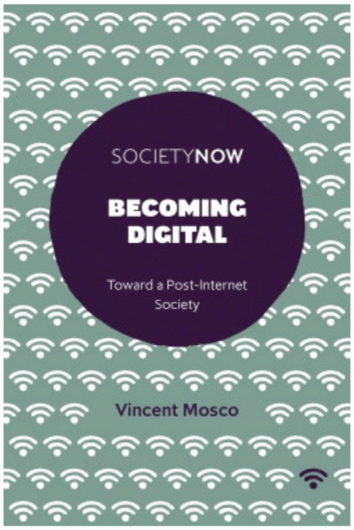
Nick Inglis

Nick Inglis is Executive Director, Content & Programming at ARMA International (formerly President of the Information Coalition, before the two organizations’ merger). Inglis is the author of ‘INFORMATION: The Comprehensive Overview of the Information Profession.’ Mr. Inglis is a recipient of the Providence Ambassador Award and was named a 2018 Rhode Island “50 on Fire” for his work with both the information profession and his public advocacy. Mr. Inglis’ writing has been featured in U.S. News & World Report, The Providence Journal, Yahoo! Finance, CMSWire, and others.



THE NEXT INTERNET: WILL IT SERVE THE PUBLIC'S INTEREST?

MARC KOSCIEJEW



TITLE: BECOMING DIGITAL: TOWARD A POST-INTERNET SOCIETY
AUTHOR: VINCENT MOSCO
PUBLISHER: EMERALD PUBLISHING LIMITED
DATE: 2017
LENGTH: 248 PAGES
ISBN: 9781787432963
PRICE: €23.99
SOURCE: HTTPS://BOOKS.EMERALDINSIGHT.COM/PAGE/DETAIL/BECOMING-DIGITAL-VINCENT-MOSCO/

The Next Internet has arrived. The Internet of previous years has been replaced by a new iteration that is profoundly changing the digital landscape. In 'Becoming Digital: Toward a Post-Internet Society', Vincent Mosco introduces the Next Internet by analyzing the three pillar technological systems that constitute it, namely cloud computing, big data analytics, and the Internet of things. The central argument is that these three pillar technological systems “comprise an increasingly integrated system that is accelerating the decline of a democratic, decentralized, and open-source Internet.” The Next Internet, instead, is serving corporations’ profit interests and governments’ social control initiatives at the expense, literally and figuratively, of individuals and their personal information.

These converging technological systems represent a new stage in digital development in which an ontological shift is underway insofar as the relationship between humans and digital machines is concerned. The Next Internet has deepened and extended the tendency to experience our lives and wider world through greater technological mediation. While the Internet’s previous iteration required an external device, such as a computer or laptop, to use, log on to, connect, and communicate, “the Next Internet’s digital networks are embedded everywhere, including inside us. They are enabling constant and ubiquitous connections to sensor-equipped objects, and to the scanners worn on, and placed in, our bodies.” The Next Internet significantly expands the virtual realm’s reach and influence over our lives and, in so doing, is helping further our integration with Internet-enabled machines, objects, and other digital technologies.

Understanding the Next Internet requires more than describing these technological systems. It also requires critical reflection upon its diverse implications for our lives and world. Mosco therefore applies a mixed methods approach combining political economy and cultural studies perspectives to the Next Internet. The political economy perspective helps illuminate the power relations shaping the digital landscape. The cultural studies perspective helps make sense of the Next Internet and its promises and perils. Combined, these perspectives offer important insights to better understand the Next Internet’s central features including its three pillar technological systems, the institutions shaping them, the problems it creates and exacerbates, and potential ways in which it could be harnessed for the interests of the public.

The book approaches the Next Internet through six interrelated chapters. The first chapter introduces the Next Internet and how it emerged with the growth of cloud computing, big data analytics, and the Internet of things and through their subsequent convergence. This new iteration of the Internet hastens “the arrival of what might reasonably be called the post-Internet world.”

The second chapter delves into detailed descriptions of the Next Internet’s three pillar technological systems, illuminating the patterns of their development and convergence. Put simply, “the Cloud provides essential storage and processing [of information]; Big Data offers new opportunities for adding value to this stored information; and the Internet of Things collects mountains of data for analysis.” Each contains great technical power that is multiplied through their convergence with one another as well as with objects, people, and nature.

This power is being exploited by corporations and governments, which is explored in depth in the third chapter. The Next Internet's political economic context and power structure are "represented primarily by the corporations and government institutions that shape the production, distribution, and use of digital technology [and information]." The dominant global tech industry leaders – led by mainly American-based corporations, particularly Apple, Amazon, Facebook, Google, and Microsoft, but also Chinese-based companies such as Alibaba, Baidu, Tencent, Huawei, and Wanda – have monopolized the Next Internet for their profits. Further, these corporate giants share intimate relationships with governments, especially Washington and Beijing, that not only benefit their operations and profits but also enable greater political control over individuals and societies.

These practices of control and commodification are further analyzed in the fourth chapter's focus on the Next Internet's penetration into every aspect of people's lives and social relationships. The Next Internet's ubiquitous presence and increasingly in everything enables the "measuring and monitoring [of] nearly all aspects of human physical and mental functioning." It facilitates the tracking and quantifying of an individual's movements and routines in addition to the performance of one's bodily organs and functions. This personal data is gathered and stored in the cloud, that is in turn subject to big data analytics to draw conclusions, develop algorithms, and

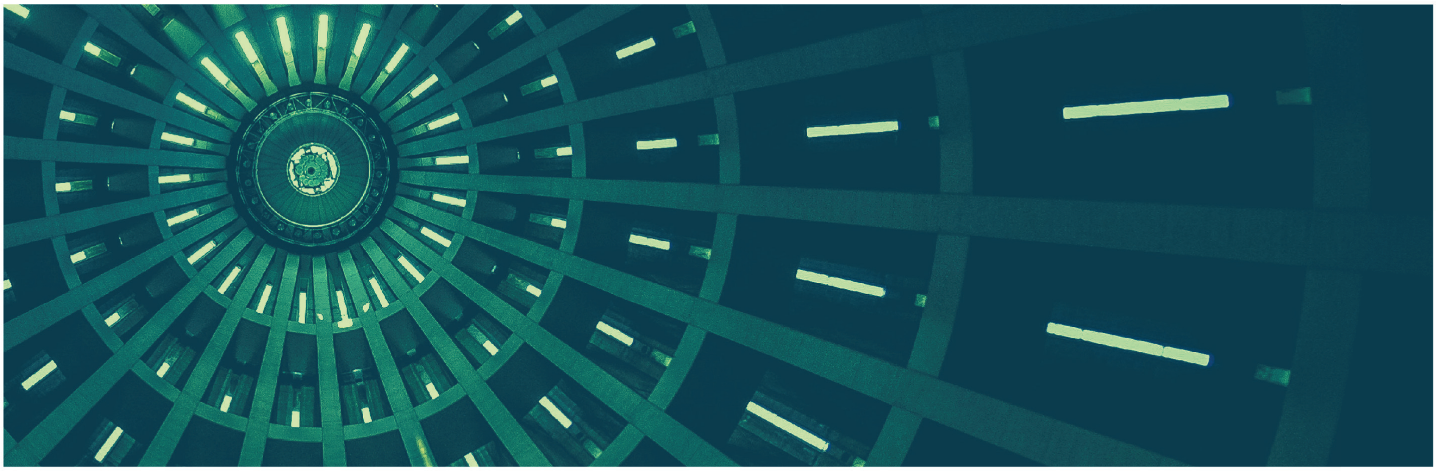
make predictions. A quantified self consequently emerges that is further commodified by corporations for profits and monitored by governments for control.

While the previous chapters gesture to the Next Internet's many problems, the fifth chapter specifically addresses them. It illuminates the complex political, economic, sociocultural, environmental, and personal vulnerabilities unleashed by growing dependence upon this digital landscape controlled by private corporations, monitored by governments, and driven by commercialization and militarization. The Next Internet’s environmental costs are particularly alarming, posits the author; it is highly polluting and wasteful. For example, its hardware contains toxic substances such as lead, mercury, cadmium, tin, and bromide dioxins. Its continuous operations require enormous energy supplies of electricity, diesel generators, and lead acid batteries. Its contribution to e-waste is staggering with its never-ending cycle of disposal and consumption. Left unchecked, the Next Internet will be a major and constant contributor to environmental degradation.

There is reason for optimism, however, as the Next Internet holds the promise of expanding democracy, personal opportunities, and social equality. Mosco argues that these promises can be realized with more public control over the Next Internet, accompanied by more individual control over our personal data that largely fuels it. He convincingly argues for applying the public utility model to the Next Internet in which it would be treated as an essential resource, much like water and electricity. The Next Internet as a public utility is an alternative to the present status quo of corporate and government control, commodification, and surveillance. It would help enhance democracy, enable universal and equal access to open networks, support public control over systems and platforms, and provide more diverse opportunities to address its many problems. Mosco states that “we now have the technical capacity to achieve these goals. It remains to be seen whether we can build the social movements essential to bringing about a more democratic and egalitarian post-Internet world.”

The convergence of cloud computing, big data analytics, and the Internet of things not only makes up the Next Internet, but also presents serious implications for our Internet-dependent lives and societies. This book serves as a timely response to this major transformation of the digital landscape by providing a critical examination of its technological convergence and implications. It will be of interest not only to information professionals working in diverse information-intensive settings and scholars studying information-related questions, but also to everyone who relies on the Internet for professional and personal purposes.

Presently, the Next Internet is establishing global networks of unprecedented power that are enlarging the commodification, militarization, automation, and surveillance of the world. These perils are compounded by the monopolistic control of the Next Internet by a handful of powerful information technology corporations and their close connections with governments and security services. These perils, however, are not inevitable outcomes. With carefully considered political and public-minded policy interventions, the Next Internet can be harnessed to expand democracy, empower individuals, provide greater life opportunities, and advance social equality. As a public utility, the Next Internet promises to serve the public interest.

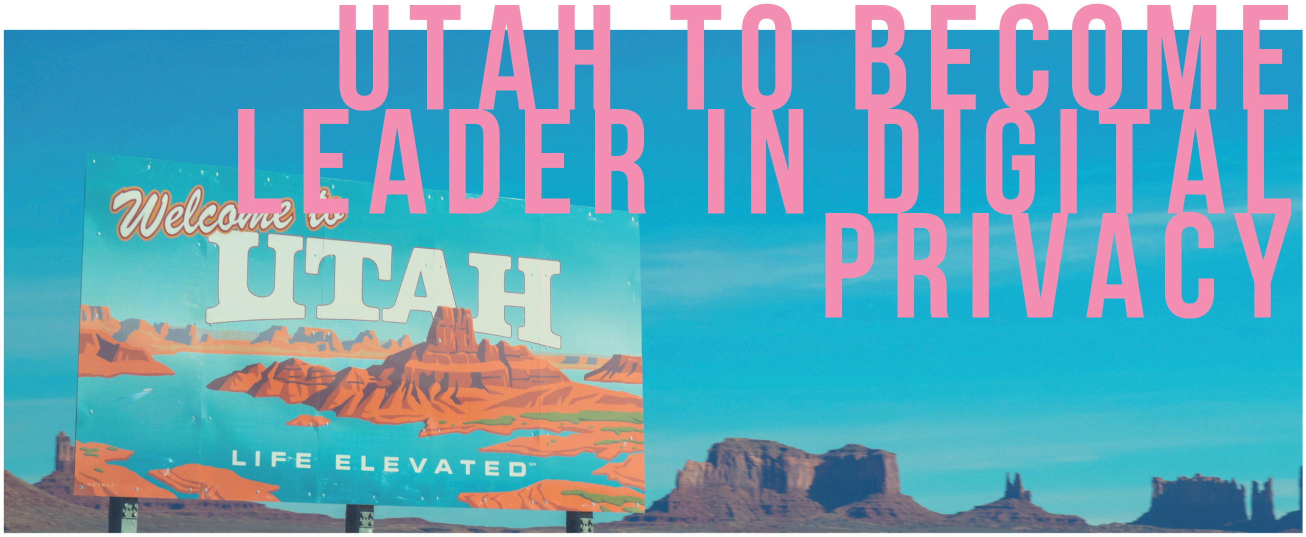


about the author

Marc Kosciejew, PhD

Dr. Marc Kosciejew is a Lecturer and former Head of Department of Library, Information, and Archive Sciences at the University of Malta. He has been published in scholarly and professional journals, lectured in Europe and North America, and presented worldwide from Canada to China at diverse universities, institutions, and events from MIT to the National Archives of Sweden to Malta's National Book Festival. He is also the winner of ARMA International's prestigious Britt Literary Award for 2014 for his article on personal data rights.

UTAH TO BECOME LEADER IN DIGITAL PRIVACY



The Utah legislature just passed landmark legislation in support of a privacy law that protects private electronic data stored with third parties (like Google and Facebook) from free-range government access.

Molly Davis, in an opinion piece on Wired.com, applauds the move:

“Prosecutors and law enforcement may argue they need the power of data collection to protect the public from potential criminals. But individual liberty protections are far more important than perceived safety risks. If there is a legitimate safety concern requiring access to a person’s data, law enforcement will still be able to obtain a warrant. Without that warrant requirement in place, private data is left vulnerable to fishing expeditions that are rife for abuse.”

According to Davis, the bill requires law enforcement to get a warrant before accessing “certain electronic information or data.” If Governor Gary Herbert signs the bipartisan bill, Utah will be the first state in the nation to lawfully protect the electronic information that individuals entrust to third parties.

The federal government and law enforcement from the 49 other states can get your data through third-party channels, with no standard of accountability because of the “third party doctrine,” a by-product from when the Supreme Court held that individuals have no reasonable expectation of privacy when they share their data with a third party.

In the courts, Davis writes, third-party data protections have made some progress. Last year, the Supreme Court ruled 5-4 in Carpenter v United States to uphold third-party data privacy, saying that law enforcement could no longer access cell phone location data from a third-party phone provider without a warrant. Banking data, texts, emails, and other phone data are still accessible, however. That’s why Chief Justice John Roberts encouraged state legislatures to pass their own legal protections. Davis writes that the rest of the country is lagging behind Utah’s progress: “Without specific laws to address new technology, courts are left to make loose constitutional interpretations.”

WHY INFORMATION ARCHITECTURE IS VITAL TO INFORMATION GOVERNANCE

KEVIN PARKER

Whether you are migrating petabytes of content from an obsolete enterprise content management (ECM) platform to a modern content management system (CMS) or just looking to make your intranet less awful, it's time to get started with information architecture (IA).

You know that information volumes, varieties, and velocities are ever increasing in today's fast-paced digital world. This has created a growing urgency in not only managing all our content and data, but in actually governing it. Organizations need to intelligently leverage their information assets and empower collaboration while protecting that information from bad actors and from loss. This is the very essence of information governance (IG).

With advances in technology, are we reaching a point in which the tools and systems can govern our information for us? Yes and no. Without advanced technologies, it is already impossible to effectively manage and govern all our content and data. But how does the technology know how to do it correctly?

Enter IA.

What is Information Architecture?

IA applies information science to designing structures and systems for organizing, labeling, navigating, and searching information. The goal of IA is to make information findable and understandable. When this is done with skill and care, IA acts as connective bridges between all our information, our technology, our customers, and our staff.

How do you recognize IA? When you go to a website or application that is hard to understand and its information is difficult or even impossible to find, you are experiencing bad IA. Conversely, when a website works superbly, is intuitive, and conveniently delivers what you need, that is the result of information architects doing amazing work in the background. You can't fix IA problems with pretty design and advanced technology alone. Rather, it is vital that design, technology, and architecture work together to provide amazing user experiences and enable reliable and scalable IG.

IA and IG

You may already be doing some IA in your IG program. When you create categories and labels, file plans, and records schedules, you are creating IA systems for organizing and labeling. Build on that foundation to create a more holistic IA and you can see great benefits.

IA is vital to strategic IG in several ways:

- It can improve information findability and understanding for staff and customers.
- It can enable better eDiscovery and (for the public sector) FOIA responses.
- It can facilitate data privacy protection and compliance.
- It can enable people and technology to capture, present, preserve, protect, organize, and manage information assets to fulfill their mission.

IA and Advanced Technologies

There is a common misconception—perpetuated by some vendors—that advanced content and data management products based on artificial intelligence (AI) and auto-classification tools will eliminate the need for doing IA work. Reputable technology vendors, however, recognize that IA is essential and may even offer expert help in doing this work through their own professional services teams or through consulting partners.

AI needs IA just like humans do for identifying relevant information stores, priorities, labels, categories, and connections that are important to the specific organization. Auto-classification and analytics tools can process and index enormous amounts of information with greater speed and consistency than humans, but they still depend on processes, information stores, content types, categories, and labels defined by the business.

Some AI tools can be used to analyze enormous stores of structured and unstructured data (often called "big data") and then suggest categories and connections based on what they find. Even this relies on some pre-existing patterns in the data. These tools can be a great help in building content models, but it is important that human information architects and subject matter experts validate and adjust the models. Otherwise, you not only risk missing important things, but also risk introducing major problems into your business, such as unchecked AI bias (which is learned from human biases that are often inherent in human-generated data).

At a recent local ARMA event, I was pleased to hear some vendors emphasize the need for IA groundwork to make good use of their auto-classification and governance products. As I said, reputable vendors get this. Pay attention to that.

With or without AI, you will still be working with CMSs, and these need the right IA to do their jobs well.

How to Get Started with IA

To take advantage of the many benefits of solid IA, follow this path:

- Take a current inventory of your information stores and systems.
- Conduct a maturity assessment of your IA and governance.
- Develop and refine your IA models, including your content model and metadata model.
- Apply the new IA to your systems and processes.
- Make IA a part of corporate and

Most of the IA work for new systems must be done up front, and it can be advantageous to get expert help from outside for this phase. IA still needs to be maintained and governed after launch, and it will need to be refreshed at least as often as you refresh your tech tools. So even with some outside help at the beginning, it is good for companies to bring on knowledgeable information architects and/or cross train their information professionals with IA skills.

When people can find the information they need, when they can collaborate effectively, when content and data are preserved appropriately, and when your information assets are securely managed, you can be sure that your fresh IA is well worth the investment.

about the author

Kevin Parker

Kevin Parker is an award-winning technology executive, information architect, keynote speaker, and a recognized leader in the information governance profession. He works with Holly Group as a consulting architect on client projects. Kevin is also the founder and CEO of Kwestix, a digital consulting agency based in Northern Virginia. He was previously CIO of an Inc. 500 consulting firm and has over 20 years of information and technology leadership experience.