VOLUME 3
JUL-SEP 2019

MAGAZINE.ARMA.ORG

CONTENTS

Additional Articles

EDITORS IN CHIEF: NICK INGLIS, CIP, IGP, INFO, & ANN SNYDER | 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 QUARTERLY 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. 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.

FACE

CONCERNS OVER FACEAPP REMIND US THAT USERS MAY NOT FATHOM THE PERMISSIONS THEY GRANT APPS

FACE

Geoffrey A. Fowler, tech columnist for the Washington Post, opens his July 17 article with a question that's pertinent to millions of app users: "When an app goes viral, how can you know whether it's all good fun — or covertly violating your privacy by, say, sending your face to the Russian government?"

In an email response, the founder of Russian-based FaceApp answers Fowler's question: Yaroslav Goncharov asserts user data is not transferred to Russia.

But should Russian servers even be our chief concern?

Fowler's article opens with a focus on that issue – including a link to an article describing N.Y. Sen. Charles Schumer's call for an investigation of FaceApp based on "security concerns and Russian ties" – but his Post piece quickly transitions into more important questions about the company's terms-of-use statement, the routine trust that consumers place in gatekeepers like Google and Apple to vet the app makers, and some of the questions consumers should be asking themselves about any app that uses their personal information.

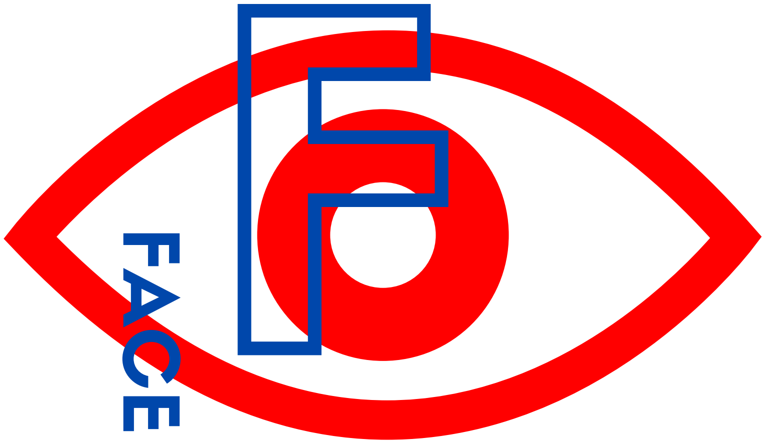
In brief, FaceApp applies artificial intelligence (AI) to photos to illustrate how a person might age. Millions of users have submitted photos of their faces and those of public figures, but few submitters were probably aware of the privacy and other risks involved.

John Koetsier, writing for Forbes.com, also exhibits deep concerns about the FaceApp terms of use, and includes an excerpt of its broad licensing language:

“You grant FaceApp a perpetual, irrevocable, nonexclusive, royalty-free, worldwide, fully-paid, transferable sub-licensable license to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, publicly perform and display your User Content and any name, username or likeness provided in connection with your User Content in all media formats and channels now known or later developed, without compensation to you. When you post or otherwise share User Content on or through our Services, you understand that your User Content and any associated information (such as your [username], location or profile photo) will be visible to the public.”

Indeed, such language should keep privacy advocates awake at night – as well as all consumers of FaceApp and other programs. Most FaceApp users routinely click “accept” to this language, unaware they’re permitting the company to use their images in perpetuity in just about any fashion it wishes. Imagine your image in an advertisement for something you find embarrassing. There are other issues, too, including that you “warrant” that you own the images uploaded, have the right to enter into the terms, and “agree to pay for all royalties, fees, and any other monies owed by reason of the User Content you stylize…” through the app. Were those really your intentions?

Still another concern is that FaceApp accesses other information on a device. In Koetsier’s July 17 Forbes.com article, Rob Le Gesse, former Rackspace manager, says, “To make FaceApp actually work,



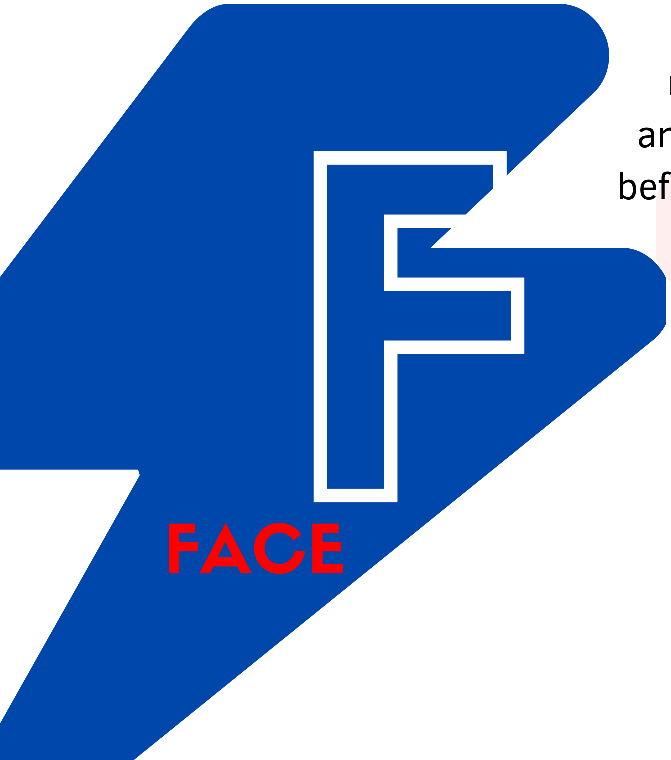
you have to give it permissions to access your photos – ALL of them. But it also gains access to Siri and Search.”

A second Forbes writer, Thomas Brewster, attempts to add perspective to the FaceApp furor, in his July 17 article titled “FaceApp: Is The Russian Face-Aging App A Danger To Your Privacy?”

He suggests the heightened concern stems from a developer’s tweet that “set off a minor Internet panic.” The tweet mirrors the allegation cited by Rackspace’s Le Gesse – that FaceApp might be taking every photo from your phone and uploading them to its servers.

By and large, Brewster suggests that FaceApp is not unique. By clicking blindly through any app’s terms of use, consumers are giving the programs permission to do more than they may ever realize: “Users who are (understandably) concerned about the app having permission to access any photos at all might want to look at all the tools they have on their smartphone. It’s likely many have access to photos and an awful lot more.”

The FaceApp situation, like those before it and those surely to come, reminds us that it remains the consumer’s responsibility to read and analyze the terms of service for any app before clicking “accept.”

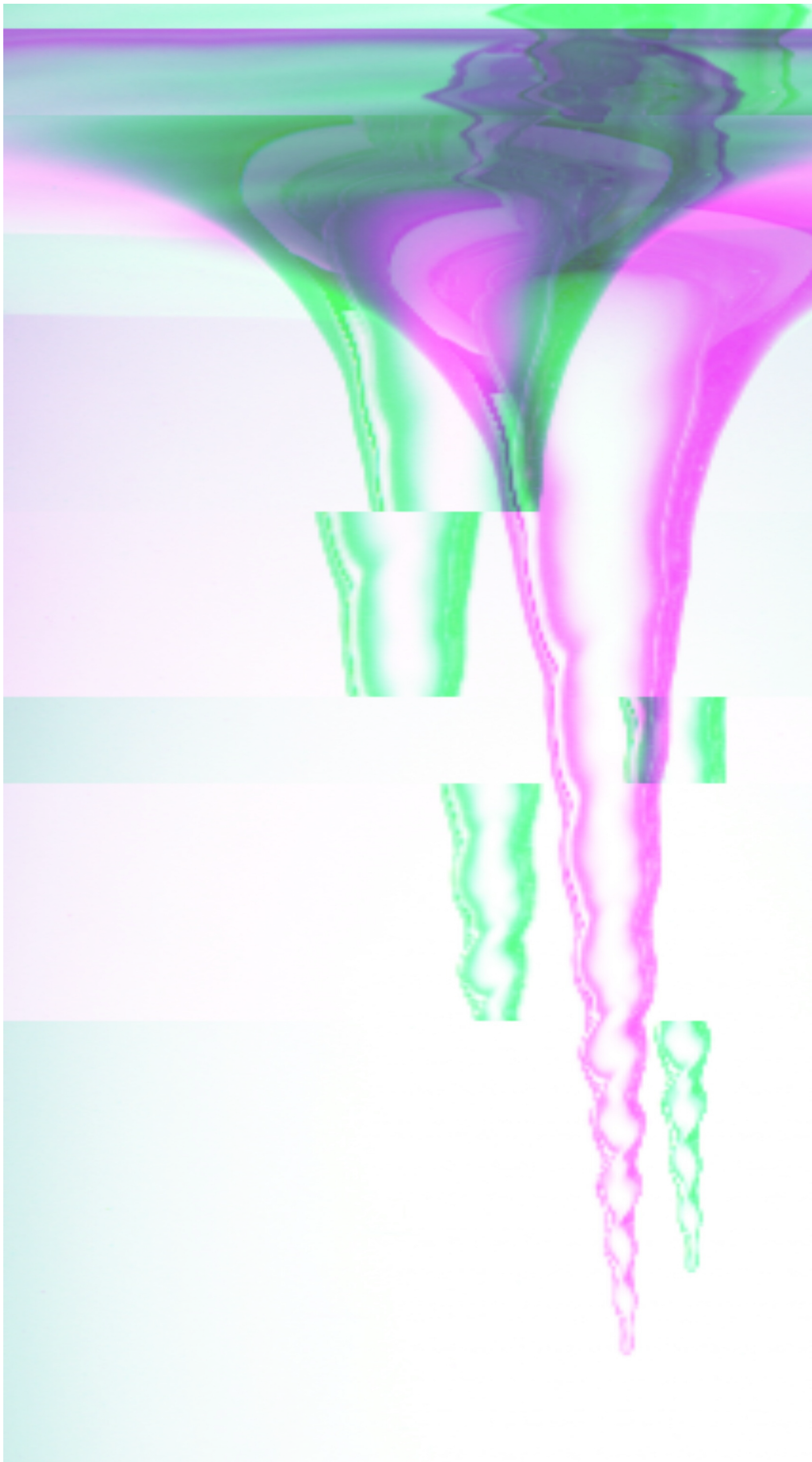


SORTING THROUGH THE WHIRLWIND OF NEWS ON THE PROPOSED EQUIFAX SETTLEMENT AND CAPITAL ONE BREACH

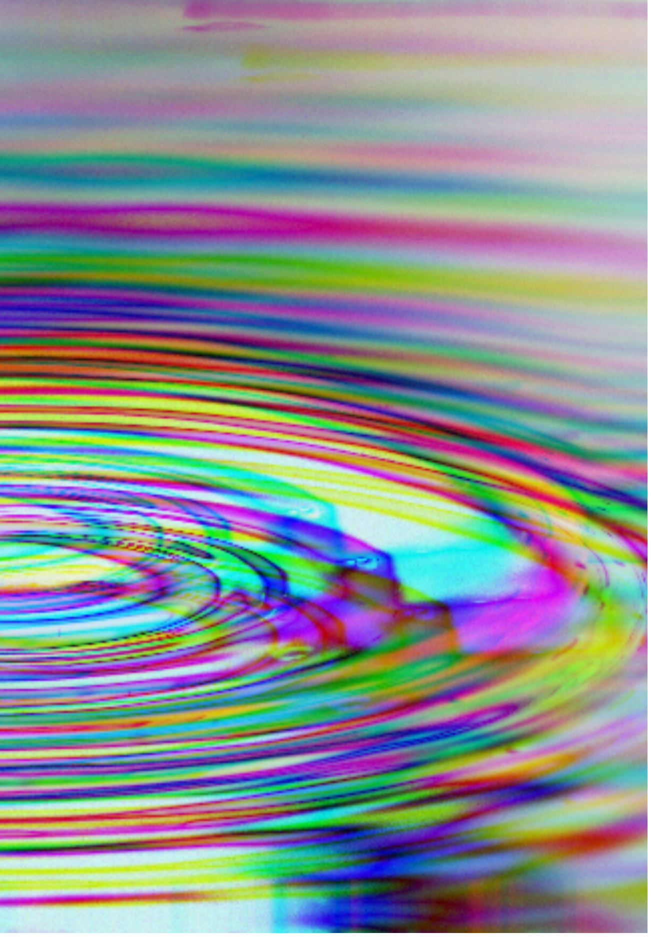
On July 22, 2019, the Federal Trade Commission (FTC) announced that it had reached a proposed settlement with Equifax in connection with a 2017 data breach that exposed sensitive, personal data of around 147 million people. According to the FTC's press release, the data breach included "names and dates of birth, Social Security numbers, physical addresses, and other personal information that could lead to identity theft and fraud." (See FTC press release Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach, July 22, 2019.)

Equifax agreed to pay between $575 million and $700 million in total. The Consumer Financial Protection Bureau (CFPB) will get $100 million of that in civil penalties with another $175 million going to states and territories. Only around $300 million with a possible extra $125 million will go to a "consumer fund" that will be used to compensate those affected by the breach through credit monitoring and various payments.

Checking whether your data was affected and what compensation and services you may be entitled to is fairly easy (to find out, visit www.equifaxbreachsettlement.com), but actually getting reimbursed may be tougher. You will need to provide support for your claim, and funds can run out if there are too many claims. Some payouts will be reduced pro rata if they exceed the amount designated for them. For example, only $31 million is designated for the alternative reimbursement. If more than 248,000 people take this option, you won't get $125. The $31 million will be divided amongst everyone with a valid claim for the payment. If everyone affected chose it, you'd get less than $0.25. To learn more, read the FAQ's at https://www.equifaxbreachsettlement.com/faq; or, if you are ambitious, read the proposed settlement, itself. (In the time this article was being written, the FTC updated its site to explain that the high interest in the alternative payment would lead to consumers getting less than the $125. The option is still available, the FTC says, "but you will be disappointed with the amount you receive and you won't get free credit monitoring.")

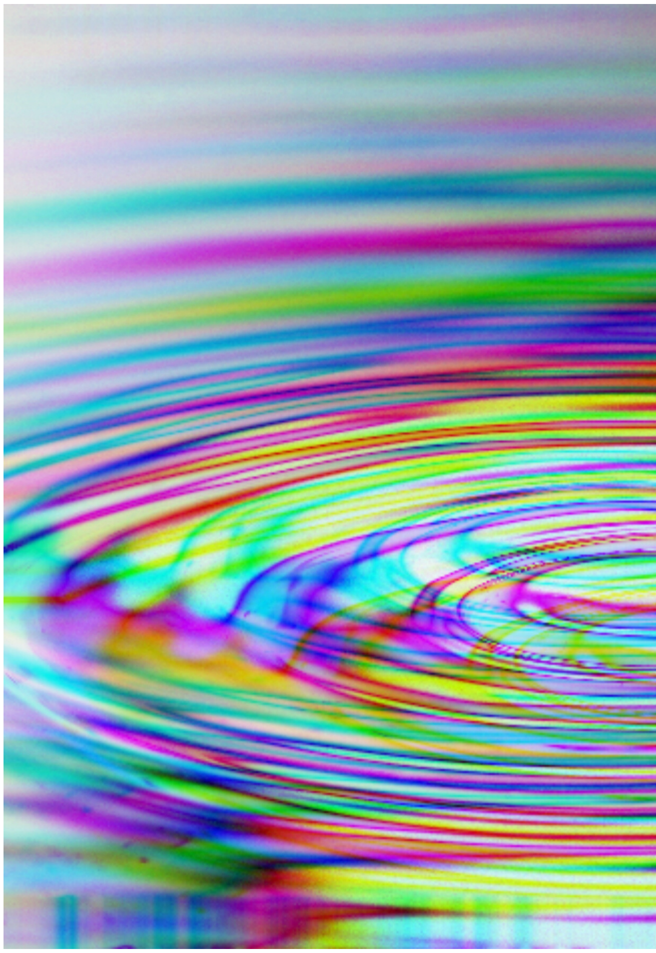


The details of the event are evolving, but Capital One issued a statement of its understanding so far. (See https://www.capitalone.com/facts2019/ Overview and Frequently Asked Questions.) According to the statement, Capital One explained that there was an "unauthorized access" exposing the personal information of around 100 million U.S. and 6 million Canadian individuals. The actual breach occurred at the end of March; the potential vulnerability was reported to Capital One through its "Responsible Disclosure Program" on July 17; and the vulnerability was investigated and fixed by



July 19. In contrast, the timeline in the Equifax incident is quite different. In its complaint, the FTC alleges Equifax received notice of a software vulnerability from the United States Computer Emergency Readiness Team (US-CERT) in March of 2017, did not apply the patch in the months to come, and finally identified and addressed the vulnerability after suspicious activity was noticed. By then, the breach had already occurred.

What was exposed in the Capital One incident? As with the Equifax breach, some highly sensitive information. According to Capital One, this included information collected during credit card applications, “including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income.” Though Capital One reports that it encrypts its data as a standard practice, the data was de-encrypted during the breach. The company also reports using tokenization for certain fields (e.g., Social Security numbers) and says that such tokenized data was not exposed. Even so, some 140,000 Social Security numbers, 1 million (Canadian) Social Insurance numbers, and 80,000 linked bank account numbers were exposed. The good news is that Capital One currently thinks that it is “[u]nlikely that the information was used for fraud or disseminated…” by the person who accessed it, and the person believed responsible was quickly identified and apprehended.



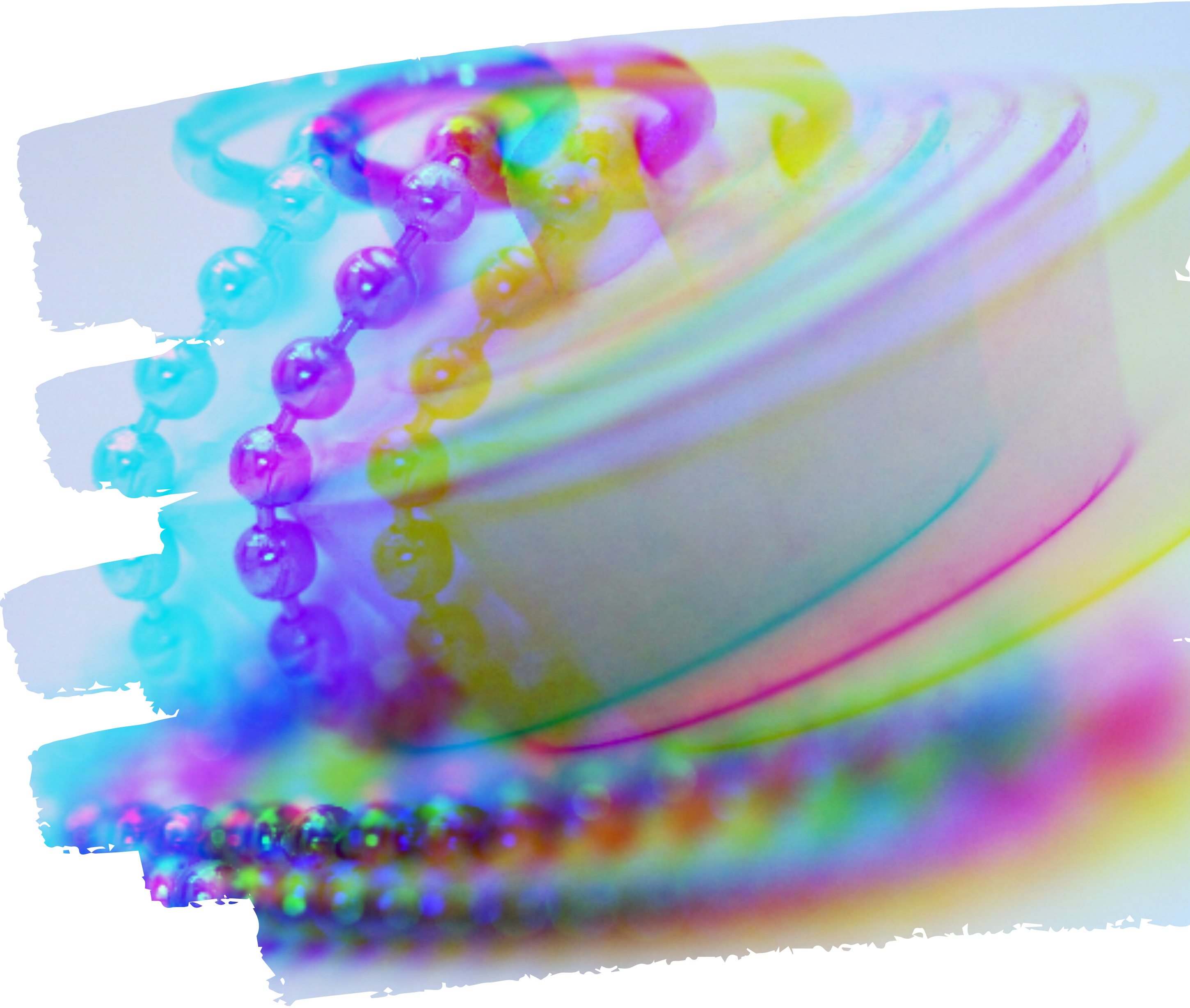
Capital One reports that it immediately reached out to the FBI. By Monday, July 29, when the breach was announced, the FBI had arrested Paige A. Thompson in connection with the incident. (See Department of Justice press release, Seattle Tech Worker Arrested for Data Theft involving Large Financial Services Company, July 29, 2019.) Thompson allegedly accessed the data, stored on a cloud-based server, “through a misconfigured web application firewall that enabled access to the data.” Thompson allegedly posted information about accessing the data on GitHub. A user seeing it reported it to Capital One. The complaint against Thompson charged her with computer fraud and abuse. If convicted, she could face five years in prison and a $250,000 fine.

While Thompson is being widely reported as a former Amazon Web Service (AWS) software engineer, the cloud provider Capital One was apparently using, the complaint filed against Thompson does not refer to AWS by name. While the breach appears to be the result of a misconfiguration rather than a flaw in the cloud service itself, the incident has some people raising questions about cloud security more generally. In his article Capital One Breach Casts Shadow Over Cloud Security, Wall Street Journal tech reporter Robert McMillian notes that Capital One "was an early adopter of cloud-computing among financial institutions as many other banks hesitated to move customer data out of their data centers."

In the same piece, Chris Vickery, the director of cyber-risk research and security from UpGuard, Inc., is quoted as saying "It's easy to misconfigure things and it's easy to have catastrophic results from those misconfigurations." So far,

that appears to be what happened here. Configuration mistakes are not uncommon, but these issues are not limited to cloud-computing. What should give us pause is that this mistake happened to a tech-savvy, fintech company like Capital One.

As the details of the Capital One breach and the investigation into Thompson continue to evolve, it is possible we will learn that other entities were also exposed. In the complaint against Thompson, the FBI says that, in addition to items related to Capital One, agents saw “files and other items” related to “other entities that may have been the targets of attempted or actual network intrusion…” (See U.S. v Thompson, Case No. MJ19-0344, July 29, 2019.)



MANAGING LEGACY PAPER FILES IN THE DIGITAL ERA

Addressing your organization's legacy paper files and capturing them in your digital information ecosystem may feel like a daunting task. As discussed in our recent white paper, ***capture*** is the first step in the information lifecycle and is essential for achieving digital transformation and enabling the strategic alignment of information activities envisioned by information governance (IG). Paper files are effectively "dark," inaccessible to your organization's digital information ecosystem ***until*** they are captured through scanning, either imaging or digitization.[1]

Like many organizations, you are probably facing a mountain of file cabinets and boxes, years' worth of records and documents, with a level of uncertainty of what information lies within. This begs the question ***Where do I even start?***

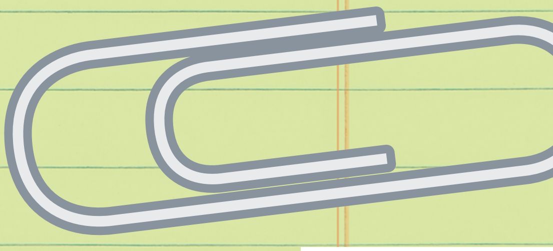
Here are a few things to keep in mind as you plan a scanning project.

Break Down a Scanning Project by Prioritizing Which Paper Files Should Be Captured First

If you have a specific driver for your legacy paper file scanning project, like e-discovery in a legal case, it's pretty clear which files you should target—those relevant to the matter. But, if you are scanning legacy paper as part of a more general effort (e.g., "going paperless"), a starting point may be less clear. Most organizations have enough legacy paper that a "scan everything" approach, without prioritization, can be hard to get off the ground and can quickly overwhelm budget limits and other resources. Where possible, break down a massive backfile scanning project into smaller, more manageable (and fundable) steps.

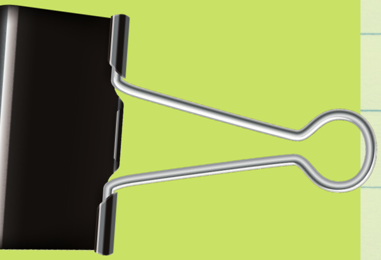
Consider starting with paper files that are accessed most frequently and tiering subsequent phases by frequency of access. Files stored on-site are likely candidates for a starting point. They may be on-site specifically ***because*** they are used often, but confirm this assumption with their owners before you scan.

For files stored off-site, review the access logs to determine which boxes are recalled most frequently. Prioritizing the scanning of paper files by their frequency of access will target those files that are in the more active phases of the information lifecycle, and it can result in immediate and measurable gains as improved ease of access, more effective collaboration, and reduced costs in recalling files from storage, to name a few.



Prioritizing by access frequency is one approach. Consider what makes the most sense for your organization (e.g., Would it make more sense to prioritize by department? Or, by some combination of factors?). The key is breaking down a seemingly insurmountable endeavor into smaller, more manageable projects, and tackling them in an order that makes sense for the priorities of your specific organization.

Understand Your Legal, Regulatory Compliance, and Business Needs with Respect to Your Information ***Before*** You Scan



An effective IG program applies a consistent lifecycle for all information in your organization, no matter its form or system. Consult your retention policy, schedule, and relevant stakeholders to understand what obligations you have for information that exists in paper form ***before*** you begin scanning. (If you identify gaps in your understanding or current approach, a scanning project is an opportunity to address these issues.) If you do not understand what information you have, why you must retain it, or for how long, scanning may effectively replicate information management problems that exist in your paper files into your digital information environment. This can be costly and increase risk.

An obvious example is scanning files you no longer need or that are nearing the end of their lifecycle. If, after consultation with relevant stakeholders (e.g., legal, RIM, business, etc.) and consideration of applicable policies, holds, and your retention schedule, it is determined that there is no legal, regulatory compliance, or business need to retain specific files, scanning only creates another copy of information that should properly be a candidate for defensible deletion. Similarly, if files are about to reach the end of their lifecycle in the near term and will be eligible for defensible deletion soon, it may make more sense to manage them for the remainder of their life *as paper*. Scanning is expensive in terms of time and resources and scanning documents at or near the end of their lifecycles can be a costly and avoidable mistake. Scanning also creates a copy and increases the risk that your information won't be consistently handled because it exists in more than one place and form. Here, you would have a paper and electronic form to delete.

Scanning creates a digital copy of your paper files, but it is the information itself that must be governed. Understanding what is in your paper files and your obligations with respect to that information allows you to include that information in the digital systems in which you are capturing those scanned files (e.g., tagging or extracting metadata to establish retention categories and trigger dates allows you to enforce your retention schedule in the digital system). While it might be possible to shred paper after a conversion project, in many cases organizations are obligated to, or choose to, keep paper files along with the digitally captured copy. Making sure that paper file tracking and management information is up to date helps ensure that your information is handled consistently according to your organization's legal, regulatory, and business needs, in both paper and digital form. If you maintain information in paper and digital forms, consider cross-referencing to ensure that changes in legal, regulatory compliance, and business obligations are reflected consistently across both.

Consider Shredding Unnecessary Paper or Finding Better Storage for What You Keep

A scanning project creates an opportunity to destroy unneeded paper. If you have determined that you have no reason or obligation to keep specific paper files or paper copies of what you have scanned, getting rid of boxes offers obvious savings in terms of storage costs and effort in double-bookkeeping, described above for information that exists in multiple forms. Consider ***securely shredding*** what you no longer need, again, ***only after*** you have determined you may do so, and confirm the approach your organization wants to take. For remaining files, move them to secure storage.

Learn More About Capture

The above are just a few things to keep in mind as you start a legacy paper file scanning project. To learn more about capture and considerations for imaging and digitization of paper, download the free ARMA/Access white paper, ***Effective Capture: The Foundation of Information Governance and Digital Transformation*** (http://bit.ly/captureIG) or view the ARMA/Access webinar "***Information Governance and Digital Transformation Must Begin with a New Understanding of Capture***" (https://youtu.be/ugQp3H7Zqf0).

Footnote 1: Imaging is scanning to a picture-based format. Digitization is scanning with some type of additional text or metadata extraction. See ARMA Capture Framework.

WILL GOOGLE PLAY FAIR IN THE 'PRIVACY SANDBOX?'

On August 22, Justin Schuh, a director on Google’s Chrome Engineering team, introduced the company’s plans for a “privacy sandbox,” a colorful title for its initiative that purports to strengthen web privacy. The news appeared on Google’s blog in an article titled “Building a more private web.”

According to Schuh, the need for a privacy sandbox stems from certain data practices that “don’t match up to user expectations for privacy.” He suggests that when other browsers allow the blocking of cookies, it actually undermines privacy “by encouraging opaque techniques such as fingerprinting.” The fingerprinting technique consists of developers harvesting small bits of data that are unique to users and that collectively can generate a unique identifier that’s available across sites. Schuh claims that Google Chrome wishes to prevent such a practice: “Unlike cookies, users cannot clear their fingerprint, and therefore cannot control how their information is collected. We think this subverts user choice and is wrong.”

In his August 26 article on ArsTechnica.com, Timothy B. Lee helps demystify the concept of a privacy sandbox for the rest of us: “Under this approach, the browser would impose a hard cap on the amount of information any site could request from the browser that might reveal a user's identity. If a site exceeded the cap, the browser would either throw an error or it would return deliberately inaccurate or generic information.”

Google’s Schuh also claims the blocking of cookies has a steep effect on income for publishers; he says that when ads are made less relevant, such revenues decrease by an average of 52%.

In addition to taking steps to block fingerprinting, Google is developing open standards that purport to “advance privacy, while continuing to support free access to content.” The development of these standards is ongoing and open to comment; a separate article in the Chromium blog includes a summation of the steps.

In the ArsTechnica piece (“Google defends tracking cookies – some experts aren’t buying it”), author Lee suggests browser privacy “has emerged as an important differentiator for Google’s rivals in the browser market.” For example, in the article he notes that Apple has for years provided measures to prevent tracking cookies, Mozilla’s Firefox will soon block such cookies “by default,” and Microsoft is taking steps to place similar protections in the Edge browser.

The nub of the skepticism can be traced directly to revenues, of course. Lee writes: “But Google has a problem: it makes most of its money selling ads. Adopting the same aggressive cookie blocking techniques as its rivals could prevent Google's customers from targeting ads—potentially hurting Google's bottom line.”

A rather blunt criticism of this privacy-sandbox initiative is found on a Princeton University blog called Freedom To Tinker, in a piece titled “Deconstructing Google’s excuses on tracking protection” (August 28). Authors Jonathan Mayer and Arvind Narayanan spare no words in their opening salvo: “Blocking cookies is bad for privacy. That’s the new disingenuous argument from Google, trying to justify why Chrome is so far behind Safari and Firefox in offering privacy protections.”

The writers go on to carefully spell out their skepticism, saying that the blocking of cookies does not undermine privacy; that no solid evidence shows that tracking-based ads are more effective; that Google doesn’t know how to balance privacy demands with ad revenue demands; and that, ultimately, Google is simply stalling – “attempting a punt to the web standardization process, which will at best result in years of delay.”

NEW COHASSET / ARMA BENCHMARKING REPORT SAYS ‘WE AREN’T THERE YET’

ARMA International and Cohasset Associates are excited to announce the 2019 Information Governance Benchmarking Report. In 1999, Cohasset Associates launched the survey, which has tracked the evolution of the information profession over the past two decades. In that time, more than 14,000 respondents have helped chronicle the evolution to information governance (IG).

On its title page, the newly released edition of the Information Governance Benchmarking Report asks this question: “Are we there yet?”

The answer, according to Carol Stainbrook, executive director of Cohasset Associates, “is a resounding no.”

But we’re getting there. That’s a conclusion drawn from the responses of 900-plus respondents, consisting of ARMA members, Cohasset clients, Iron Mountain customers, and Records Management Listserv members.

“The number of organizations that have or are developing an IG program is at the highest level it has been since we started the survey,” says Stainbrook.

According to the report’s abstract, metrics from the February-March 2019 survey are used to examine “the state of IG advancement, achievements and the obstacles resulting from and impacting IG, and actions and strategies that facilitate effective and efficient information lifecycle management.”

The report highlights three specific findings and provides recommendations for action: (1) culture is a substantial barrier to the advancement of IG; (2) organizations benefit from interdisciplinary IG; and (3) automated processes and tools make IG more effective and efficient.

Among its uses, the report can be a benchmarking tool; a guide that sheds light on the real-world challenges and benefits of IG; and an instrument for IG advocacy. In any event, Stainbrook urges that it be used:

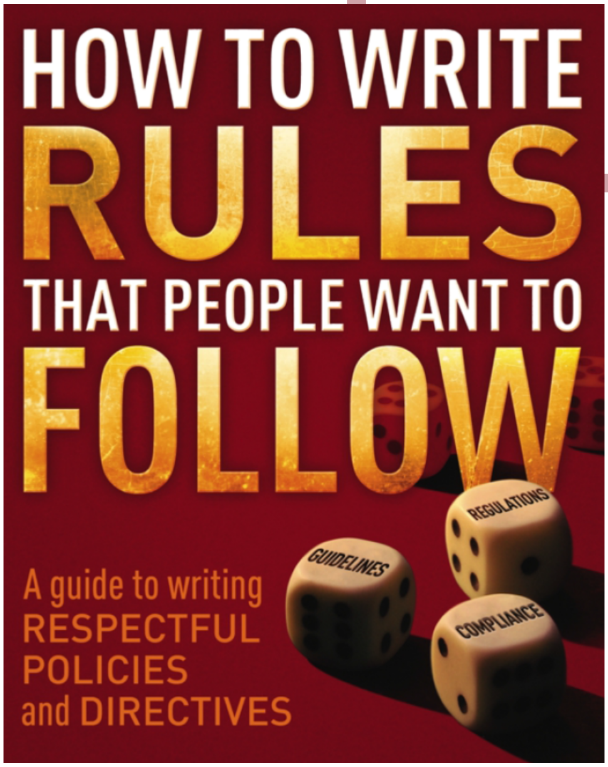
“If you are not moving forward, you are falling behind,” she says. “The time is now to take action. Don’t let change pass you by.”

Nick Inglis, executive director of content & programming for ARMA, encourages information professionals to make use of the report as well:

“This report highlights some of the ways we are making great strides, and it points us towards potential areas of weakness. It’s a critical report that we believe all people within the information profession will genuinely benefit from reading and embracing the findings.”

The free report is available on ARMA’s site. Iron Mountain provided financial support for this important project.

EISEN'S BOOK ON RULE-WRITING DELIVERS ON ITS 'HOW-TO' PROMISES



A review by Jeff Whited

Usually I pick up a how-to book only if it's in the way of a book I want to read, but Lewis S. Eisen's How to Write Rules That People Want to Follow (Pixley Press) conquered my bias rather quickly. Here are four reasons I'd recommend the book to anyone in the workplace:

First, the topic is fresh and pertinent. Few would argue against his view that rules too often sound crabby and aggressive and are frequently unclear. In the opening pages, he writes "Well-written policies don't sound like angry parents talking to naughty children. Well-written policies sound like adults talking respectfully to adults." And, he continues, this aggressive tone is ironic “because most organizations genuinely care about respect in the workplace.” The problems with rules, policies, and directives, he writes in Chapter 1, are lack of clarity, lack of focus, and lack of respect. Accordingly, throughout the book, Eisen provides examples that are clear, focused, and respectful.

Second, the book delivers on the promise of its title. Too many instructional products contain exhaustive descriptions of the problems – essentially reminding the audience of what is wrong in the first place, almost to the point of “rubbing it in." But what the audience really wants are solutions. Here, Eisen provides specific answers all the way through. Of particular value are his distinctions between policies and guidance: “The failure to distinguish policy statements from guidance statements is the critical flaw in the policy instruments of most organizations.” When the crafters of rules and policies grasp this distinction, their guidance documents – which are what most of us actually see – should improve notably.

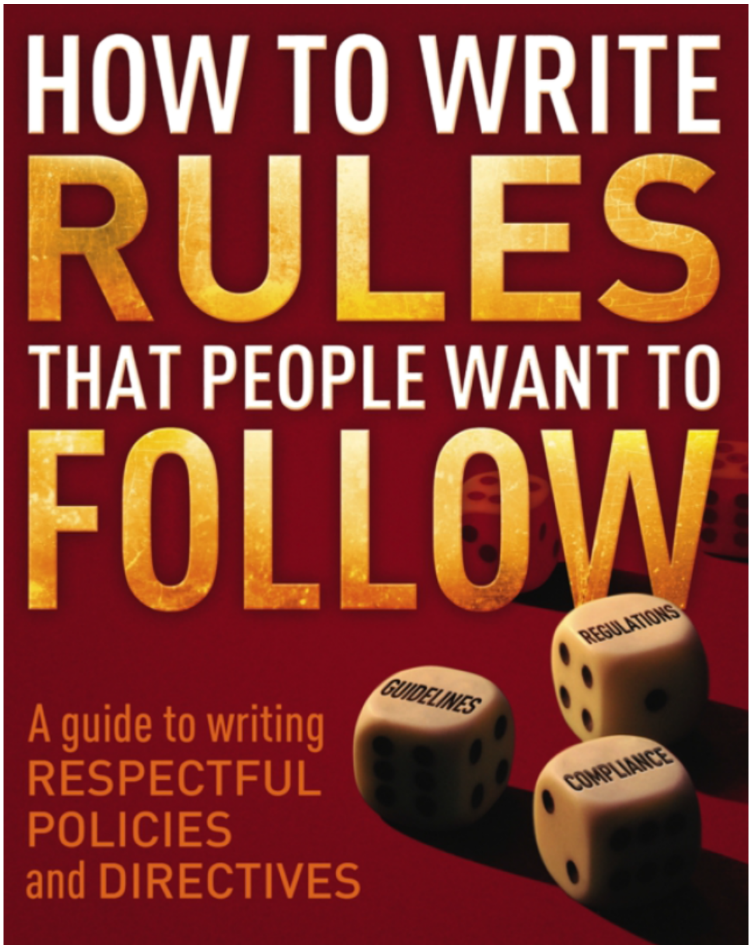
Third, it passes the “YouTube 50-Percent Test.” If you’ve ever clicked YouTube videos that promise to solve your household problems, you know it’s safe to skip the first half because that’s how long it takes the presenters to introduce themselves and any house pets that stray into view, and then to blithely describe the frustrations of having a leaky toilet or a spasmodic garage door, indifferent to the fact that your hardware store closes in twenty minutes. Eisen’s book has no maddening “fast-forward” sections, except perhaps for its very brief summaries of what each chapter will entail – and, again, these are very brief.

Fourth, the book is easy to read. The words on the page don’t try too hard; you know you’re in pretty good hands. This excerpt from the

Introduction, for instance, typifies the conversational feel even as it gives you a glimpse of what's ahead: "This book will not tell you what your rules should be; you need to decide that yourself. This book is about how to convey that decision once it's made. We're not going to be distracted by how to vote or reach consensus, who to consult, or how to manage the rule-making process."

How to Write Rules That People Want to Follow can be purchased on the author's site. See also Eisen's August 2019 ARMA magazine article, "Can Information Management Policies Be Both Clear and Concise?"

Purchase your copy of Lewis Eisen's ***How To Write Rules That People Want To Follow*** at https://amzn.to/346vVUo (affiliate).



Lewis Eisen

CAN INFORMATION MANAGEMENT POLICIES BE BOTH CLEAR AND CONCISE?

Most information management (IM) professionals would agree that well-written policies are clear and concise.

Too often, though, the policies are “dumbed down” because someone is afraid that maybe, somewhere, some individual in the organization might not be familiar with one of the technical words used in the policy. The logic is that if one person doesn’t understand the policy as worded, that lack of understanding would be a terrible thing.

The result of such caution is either (1) a policy that's written in such general terms as to be meaningless to the professional, or (2) a policy that's so bloated with explanatory text that it's the opposite of "concise."

On the surface, we have a contradiction. Making text "clear" often entails using more words, whereas making it "concise" is about using fewer words. This apparent contradiction is the result of a fundamental misunderstanding: the failure to differentiate a policy document from the guidance document that explains it.

Let's start with some examples outside the world of IM, to make the distinction easier to see.

POLICY VS. GUIDANCE DOCUMENT: INCOME TAX

So far, you've likely managed to file your annual income tax return each year without having to read the Income Tax Act.

The Income Tax Act is the operative authority. It's written in technical language, meant to be understood by experts in the tax field. There is no expectation that you and I ever read that document, despite the fact that it does apply to us.

To help us file our annual returns, a separate piece of guidance has been written, called something like How to Fill Out Your Income Tax Form. The guidance explains everything we need to know about the Act to get the job done, along with other helpful advice.

It is that guidance document that “dumbs down” the technical jargon of the Act and explains concepts that might be confusing. It is that guidance document that uses plain language, that gives us examples, and that fills in any gaps in our knowledge.

As a taxpayer, I do my job properly when I follow the instructions contained in the guidance document. Even when I need clarification, I don't reach for the Income Tax Act to get it. Instead, I look for an expert who can help me understand the situation.

POLICY VS. GUIDANCE DOCUMENT: DISEASE CONTROL

A local hospital has a policy that reads as follows:

All incoming cases presenting sub-dermal or subcutaneous lesions are treated as epidemiological risks.

I have no clue what that policy means. I’m not trained in medicine, and it uses words that I don’t understand.

But so what. If I’m supposed to take some action as a result of this policy, the hospital will post a sign somewhere in plain language telling me to wash my hands or wear little cloth booties or whatever it is I'm supposed to do.

Whether I understand the wording of a hospital policy is of no importance. What's important is that the medical specialists in that institution can all agree on what the policy means.

If they do all agree, then they can explain it to the rest of us. If they don't agree, then we have a problem that's worth paying attention to.

POLICY DOCUMENTS ARE FOR EXPERTS

While everyone in your organization may be governed by the IM policies, few people actually need to read them.

All authorities — that is, statutes, regulations, policies, and standards — are not written to be used by the layperson. What is important is that the language in the authorities is clear and meaningful to experts in the field. Once that condition is fulfilled, the experts can give the non-experts some plain language guidance to tell them what to do.

In my experience, the more serious problem with IM policy documents has been that the IM professionals at the organization weren't all on the same page about how various statements were to be interpreted. As a policy writer, if you can achieve a single, common understanding of a given wording among the experts, you have done your job. Making the policy understandable to the masses is a separate task, handled by the guidance you produce.

CONFUSION ALSO STEMS FROM MISUSE OF ‘POLICY’ IN TITLES

It’s no wonder that people confuse policy documents with the supporting guidance documents. Many web sites direct you to a page erroneously called “Privacy Policy.” When you get there, the document you find is not an actual policy, but rather guidance explaining the policy to you. The policy itself is a separate document, sitting somewhere in their corporate records repository.[1]

WHEN THE ACTUAL POLICY DOCUMENT IS NEEDED

A policy is more like a wall stud than wallpaper. It supports the wall, but it’s not what people should see when they walk in the room.

The guidance documents are the wallpaper. The policies provide a framework on which the wallpaper is hung. The vast majority of people never have to see the studs holding up the wall behind the wallpaper.

If your guidance is written properly, the only time you will need to produce the original policy document is when you’re challenged on it. It’s when someone storms into your office, shouting, “Show me! Show me the policy that says that I’m not allowed to chew bubble gum in the office!”

On those occasions, you will be prepared. You calmly reach into your back pocket and pull out the authoritative instrument. You point to the relevant statement and say, “Look, right here. It says ‘no synthetic masticating substances.’”’ And then you can add, “That means ‘bubble gum.’”

HOW TO GET TO ‘CLEAR AND CONCISE’

When you accept that your IM policy documents are not written for a general audience, you have the freedom to use whatever technical terms are required for clarity. You can omit all the simplifications, explanations, teaching points, and examples, and instead focus directly on technical accuracy.

When you limit your policies to only what is necessary to express the policy decisions made, and put all the “in-case-someone-doesn’t-understand” information into your guidance, you will be able to produce policies that are both clear and concise.

[1] To add semantic insult to lexical injury, a website might ask you to “consent” to the policy. Any law student can tell you that you can consent to “terms” of an agreement, but as an outsider to the organization you have no standing to consent or not to consent to the policy!

SPONSORED CONTENT

MICROFILM IN THE DIGITAL WORLD

by James Westoby, president of e-ImageData

Bringing the best technology to the full life cycle of microfilm, e-ImageData's ScanPro® line of microfilm scanners moves you into the digital world with speed and economy.

Today, in this digital age, users expect information to be easily and quickly accessible. Information on microfilm is no exception. So, it is no surprise that the focus today is to convert those trillions of stored microfilm records to a digital format to make it possible to quickly locate the information and immediately provide access to its content.

Microfilm conversion scanning is not new. In fact, conversion scanning equipment has been around for many years. However, recent advances in technology have eclipsed the older technologies which are excessively expensive to purchase, expensive to maintain, time-consuming to use, complicated to operate, and don't provide the totally reliable and affordable conversion solution that the industry demands.

ScanPro Background

The e-ImageData ScanPro line of microfilm scanners has been and continues to be the micrographics equipment of choice in the world's most prestigious libraries, universities, government agencies, medical facilities, financial institutions, and corporations. And, for good reason. Included are features like ABBYY® FineReader OCR, PowerScan Productivity Suite comprised of WORD Search™, INFO-Link™, Copy-to-Clipboard, and searchable PDF multi-page. Additionally, the handy SPOT-Edit™ tool selectively adjusts brightness and contrast within a document and the AUTO-Adjust™

tool which, with a single click, automatically adjusts brightness and contrast as well as straightens and crops the document.

This reputation is well-earned and based on innovative engineering that has won multiple awards worldwide. The ScanPro equipment is built to last, employing a heavy gauge steel framework and steel ball bearings throughout, resulting in the highest reliability rating in the industry, and is backed by the industry's leading three-year factory warranty. The ScanPro scanners are truly universal, supporting all film types, including 16mm, 35mm, and cartridge roll film, fiche, jacketed fiche, aperture cards, micro opaques, and ultrafiche. The ScanPro scanners are rugged, compact, intuitive, and easy to operate.

ScanPro All-In-One | Your Conversion Project Solution

Expanding on the unprecedented success of the standard ScanPro platform, e-ImageData recently introduced the ScanPro All-In-One™ scanner which provides all of the features of the standard ScanPro scanners but with the added capability of doing high-speed conversion scanning, making it the most versatile piece of microfilm equipment ever made.

Ribbon or Strip Scanning vs. Multi-Mode Smart Scanning

Both ribbon or strip scanning and multi-mode smart scanning ensure the capture of every image on the film. However, the decades old conversion technologies of ribbon or strip scanning methods use a line sensor whereas the ScanPro All-In-One multi-mode smart scanning technology uses an area sensor. Ribbon or strip scanning methods use a fixed brightness and contrast setting throughout the entire roll of film. If the film images are all of the same density and contrast, ribbon or strip scanning works well. Unfortunately, this is rarely the case. Consequently, in the best case, manual post scanning editing is required, and in the worst case, the film will need to be retrieved again and re-scanned. Multi-mode smart scanning is able to adjust brightness and contrast for each individual image, ensuring that it is captured correctly the first time.

Ribbon or strip scanning methods output a proprietary file type and the images are not straightened or cropped. To convert this proprietary file type to a PDF or TIFF and to straighten and crop the individual image requires considerable additional time and effort and the purchase of additional expensive software. The multi-mode smart scanning method of the ScanPro All-In-One outputs a standard file type such as PDF or TIFF and the images are already straightened and cropped. And, no additional software is required.

Ribbon or strip scanning hardware is very expensive to purchase and to maintain. This is reflected in the limited one-year warranty provided. The ScanPro All-In-One is a small fraction of the cost to purchase and to maintain. This is reflected in the standard three-year warranty.

Ribbon or strip scanning hardware is not useful as an on-demand scanner whereas the ScanPro All-In-On is both an on-demand scanner and a production conversion scanner.

The ribbon or strip scanning hardware requires special expensive accessories to support film types other than roll film. The ScanPro All-In-One comes fully equipped to handle all film types.

ScanPro All-In-One

Summary

The ScanPro All-In-One is your microfilm scanner for today, tomorrow, and well into the future. With a ScanPro All-In-One, conversion scanning in the digital age has never looked so good.For more information, please visit www.e-imagedata.com.

e-ImageData
microfilm scanners

essentials OF INFORMATION GOVERNANCE

ARMA's new 'blended learning' course brings together the best practices for establishing information governance in your organization.

http://bit.ly/IGessentials