Information Management

SOCIAL MEDIA

FINRA Compliance Is a Challenge With Social Media

Financial organizations must be especially cautious about the information they share on social media, in light of the U.S. Securities and Exchange Commission's (SEC) recordkeeping rules. *Forbes.com* reports that a poll conducted by Financial Industry Regulatory Authority (FINRA) shows that financial organizations are especially concerned about two compliance issues stemming from such activity: the use of unauthorized social media accounts and the inability to capture and retain social media content.

Among the additional concerns are cyberattacks, inadvertent sharing of personal information, embarrassment through inappropriate sharing, and false or misleading content.

At the 2018 FINRA annual conference, a panel of financial services compliance professionals discussed ways to leverage social media while remaining compliant. Among the suggestions were a few basic governance practices, such as putting processes and controls in place to monitor and supervise social media

communications, deploying technology to capture and retain approved business communications wherever they occur, and developing reasonable supervisory practices that are reinforced through training.

"We train our employees that any type of communication that relates to business, and needs to be captured, should be redirected to the appropriate device or firm system that is able to capture those communications," said panelist Nubiaa Shabaka of Morgan Stanley.

According to FINRA, organizations have recordkeeping, content, and supervisory responsibilities when they "adopt" or "become entangled" in third-party content, which includes the original digital communication and its link. The panel advised organizations to develop a library of pre-approved third-party content for its associates to share. More conservative organizations will tend to avoid such content altogether, due to copyright and branding issues, according to the article.

DATA SECURITY

New Scrutiny May Show More Breaches, Despite Security Boost

The CEO of security firm Varonis foresees continued troubling trends in cybercrime, despite steep spending on data security – $100 billion in 2018 alone, according to Gartner Inc.

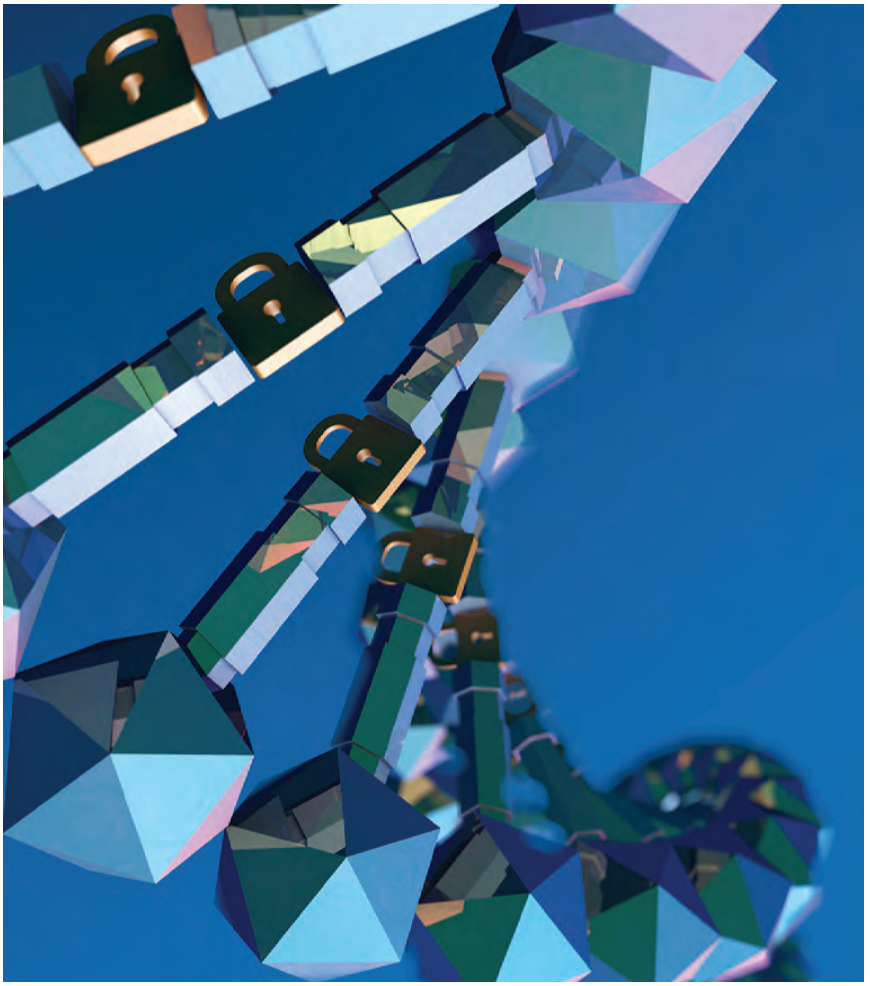
Yaki Faitelson, on *Forbes.com*, writes that the General Data Protection Regulation (GDPR) alone will require more organizations to monitor for and report on data breaches. "When we shine a light on our dark data, it exposes things we may not want to see – but sometimes things have to get worse before they can get better," the Varonis CEO

writes. "Not only should we expect to continue to hear about breaches, we should expect many of these breaches to be very damaging – far more damaging than they need to be."

Faitelson says U.S. data breach incidents surpassed 1,500 in 2017, according to the Identity Theft Resource Center (ITRC). The Varonis Global Data Risk Report, a study conducted by his organization, reveals that, on average, 21% of an organization's folders were accessible to every employee and 41% of organizations had at least 1,000 sensitive files open to all employees.

The report, he asserts, "puts front and center why data-related regulations are being enacted and why boards need to be very concerned: It's just too easy for insiders and outside attackers that get inside to steal valuable data."

Opinion: DNA Donors Should Demand Better Privacy Protections



A medical doctor and a lawyer from Yale Law School's Information Society Project are advocating for stronger privacy protections for DNA donors, especially in reference to All of Us, a project administered by the National Institutes of Health.

According to Mason Marks, M.D., and Tiffany Li, J.D., whose op-ed appears on *StatNews.com*, the goal of All of Us – to uncover paths toward delivering precision medicine – is a good one. But the authors warn prospective donors to "decline the invitation to join unless you fully understand and accept the risks."

The authors say a genetic profile is far more complex than a fingerprint and is the single most identifiable characteristic an individual has. "Such profiles contain a treasure trove of information about individuals and their health, such as predispositions for cancer, neurodegenerative disease, and mental illness," they assert.

Reportedly, the All of Us project also seeks to collect biospecimens and data about donors' medical histories, lifestyles, families, and psychological health. In addition to the DNA, it gathers data from wearables like Fitbits and Apple Watches.

According to Marks and Li, U.S. health privacy laws were written before genetic privacy was an issue. The Health Insurance Portability and Accountability Act (HIPAA), for example, does not apply to companies like GEDmatch, 23andMe, or Ancestry.com, all of which work with DNA samples in some capacity. And it does not apply to All of Us, to its corporate partners, or to new forms of medical data gathered from websites, apps, and wearables.

Marks and Li assert that HIPAA applies only to "covered entities" — individuals and organizations traditionally associated with health care, such as doctors, hospitals, insurance companies, and their business associates. "In many cases, the All of Us program may have more sensitive information about you than your doctor [has]. But the program is not your physician and is not subject to the duties imposed on health care providers by HIPAA and other regulations such as state medical licensing laws."

Further, few laws prohibit law enforcement from accessing genetic data that's stored in public or private databases. For example, if a relative's DNA is found at a crime scene, a donor could be dragged into an investigation due to kinship alone. "Even a distant relative's data could provide probable cause for law enforcement to conduct a search or interrogation," the op-ed says.

Marks and Li also say that commercialization and theft of the samples are additional risks that potential donors should consider. "Once it [DNA] has been disseminated, it would be impossible to retrieve and conceal again. Hackers could hold the data for ransom or sell it to third parties such as data brokers or unscrupulous employers."

The editorial encourages legislators to expand HIPAA's definition of covered entities to include app developers, websites, and other organizations that collect and analyze health data, including genetic information.

RETENTION

Professor Urges Second Look at Push for Expanded Metadata Laws

Granting law enforcement more powers in accessing metadata is an Australian trend that troubles at least one law professor. Rick Sarre, of the University of South Australia, writes on *TheConversation.com* that the push to allow authorities to access encrypted digital data has consequences that must be considered.

Angus Taylor, minister for Law Enforcement and Cybersecurity, said the government will continue to pursue new powers that permit authorities access to encrypted metadata in the fight against terrorism, organized crime, and online crime.

Sarre, in response, encourages a review of the record in this trend of granting increased access to metadata. He writes that 21 law enforcement agencies have been granted access to track and retain metadata. "Given the ubiquity of smartphones and other portable devices, these agencies can find an enormously rich trail of information on users' locations, calls, and networks."

In 2015, new laws required telecoms to retain and store their metadata for two years so that it would be available for analysis. At the time, the government sought to ease concerns about "overreach" by granting more power to the Commonwealth Ombudsman to monitor compliance.

Sarre writes that a primary concern was that the new laws would "erode the very democratic freedoms that governments are duty bound to protect, such as freedom of political association." He cites an April 2017 incident in which an Australian Federal Police operative sought and acquired the call records of a journalist without a warrant.

Lost, perhaps, in the traditional privacy concerns was the likelihood that this strategy was not future-proof. Technologies that conceal metadata from collection are already rampant, he asserts. "Any encrypted messaging app — such as Wickr, Phantom Secure, Blackberry, WhatsApp, Tango, Threema and Viber — can circumvent data retention. Moreover, any secure drop system based on Tor is capable of evading metadata scrutiny too."

Minister Taylor, aware of this reality, therefore seeks to continue pursuing new powers. Sarre asks, "Will this be through some form of commercial arrangement? Will it be via a threat to block services of non-compliant telcos? Will it involve embedding surveillance codes in devices? Will warrants be required in all cases? How much will it cost?"

The professor goes on to question whether the current metadata laws are having any effect. He says there is anecdotal evidence now and again, but no actual confirmed evidence that access to metadata has disrupted any threats to national security. In turn, he offers this caveat: "It is worth remembering that governments must ensure that no policy sacrifices our hard-fought liberties in the pursuit of an expensive goal that is not readily attainable."

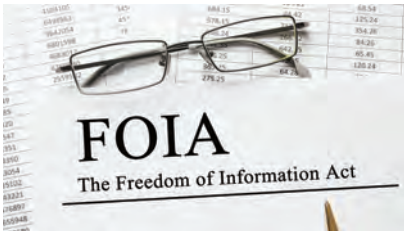
FOIA

FOIA Backlog Is Trimmed Even as Requests Set Record

As reported on *FedWeek.com,* U.S. federal agencies received a record 818,271 requests under the Freedom of Information Act in fiscal 2017, according to the Justice Department, but agencies still managed to reduce the backlog to just more than 111,300 by processing 823,222.

The total number of requests has risen steadily from roughly 600,000 in fiscal 2010. Currently, the Department of Homeland Security continues to account for the largest share, at 45%. The departments of Justice and Defense and the National Archives and Records Administration accounted for 10%, 7%, and 7%, respectively.

According to the article, about 22% of the requests were fully granted, 37% partially granted, 22% had no relevant records found, 5% were denied based on exceptions under law, and the rest were withdrawn, duplicative, or had other outcomes.



Critical Efficiency Improvements

EXL improved mail- and document-handling operations for a key client using OPEX Corporation's Universal Document Scanning Workstations.

When it comes to document management, productivity and accuracy are critical and require enterprise-class technology to ensure efficiency and traceability. EXL was able to improve efficiency by several hours per day and reduce resource requirements significantly using OPEX® FalconRED® and Falcon® document scanners for a high-volume customer.

EXL is a global operations management and analytics company based in New York. As part of its service offerings, the company provides mailroom and document services to companies primarily in the finance, accounting, and insurance markets.

The company operates customer mail centers both on-site and in its own facilities where document imaging and document management are key activities. "Our imaging center really feeds the process for the folks doing the work at these companies," says Glen Baker, Vice President of Life and Annuities at EXL. "Images are our lifeblood."

At one particular customer site, however, the quality and reliability of those images were in question. The company operated a mailroom for the customer where staff received, prepped, and scanned documents on a conventional production class scanner. The facility processes between 6,000 and 6,500 documents per day, with each document containing 3.5 to 4 pages. "The preparation process caused some problems in terms of quality and productivity," Baker says. "We went back and revisited that entire environment with an eye toward swapping out the software and hardware."

Working closely with the client, EXL created a scorecard and wrote a detailed requirements document that was used to evaluate the new scanning hardware. "We wanted something that was production-quality and could help take us from receipt through archiving," Baker says.

Eventually, EXL narrowed their choices down to the OPEX Falcon and FalconRED series of document scanning workstations and another scanner manufacturer. OPEX ultimately won out, in part because of the way the scanners handled the archiving process. "We would have the ability to tag information when it comes through and follow those documents throughout the entire process for traceability," Baker says. "It also required less customization out of the box." The second important feature of the Falcon series was OPEX's one-touch prep and scan environment.

EXL also replaced the existing software implementation with Hyland Software's OnBase® product. "We had used OnBase for many years at our own New Jersey scan center," Baker says. "When we re-evaluated the client facility, we found we could get almost 95 percent of the features we needed out of the box with OnBase as opposed to the previous software."

Minimize Labor, Maximize Quality

EXL has deployed five FalconRED scanners and one Falcon scanner at the site. FalconRED combines the Falcon scanner with the OPEX Model 72 Rapid Extraction desk. This unrivaled combination of envelope opening, content extraction, and document imaging makes FalconRED the most efficient, secure, and cost effective way to scan directly from sealed envelopes with no added prep operators needed.

Because the customer had multiple lines of business operating out of the same mailroom, EXL was able to install the new solution in phases. Initially, they brought in a demo Falcon unit for evaluation. "After that, we took the big leap," Baker says. "We were convinced this was the answer we would need going forward. We went through the process of getting the software up and running while the machines were being built and had a parallel document processing operation in place [using both new and old equipment] as we went through each phase."

Read the entire article here.

For more information visit www.opex.com

OPEX® CORPORATION

BREACH LEGISLATION

Oregon Tightens Data Breach Notification Law

In June, amendments to Oregon's data breach notification law went into effect. As reported on *HuntonPrivacyBlog.com*, the amended law redefines "personal information" to now include the consumer's first name or initial and last name combined with "any other information or combination of information that a person reasonably knows or should know would permit access to the consumer's financial account."

Additionally, the law now applies not just to those who own or license personal information, but to anyone who "otherwise possesses" such data and uses it in the course of their business.

The amendments call for a new notice deadline; notice must be given in "the most expeditious manner possible, without unreasonable delay," and no later than 45 days after discovering or being notified of the breach.

If organizations offer consumers credit monitoring services or identity theft prevention in connection with their notice of a breach, the amended law says they cannot make those services contingent on the consumer providing a credit or debit card number, or accepting another service that the person offers to provide for a fee.

PRESERVATION

Pittsburgh Archivist Seeks to Remedy Longtime Recordkeeping Mess

A recent article on *TheIncline.com* describes how poor records management for thousands of inactive municipal records has left them piling up in basements and warehouses around the city.

According to City Archivist Nick Hartley, there are about 10,000 boxes of old municipal records stashed here and there with no rhyme or reason. They include maps, genealogical-type documents, and clerical copy. Most, if not all, are inactive.

The Pittsburgh City Council has begun the process of fixing the problem. Under consideration are bills that would expand archives duties and staff and establish a records management division within the city clerk's office to standardize recordkeeping practices citywide.

Archivist Hartley is promoting the passage of both bills. He says the city needs to take a more corporate approach to managing its records. "We create them, we use them, but we've never really had someone on board to think about what happens to them," Hartley told *The Incline*.

He says there are few written policies on the administration of records, which results in "ad hoc and uneven practices in the storage, retrieval, use and destruction of records."

In a June meeting with the city council, the archivist emphasized the value of retention schedules as well: "Without retention schedules, we can't maintain an accurate inventory of city records, nor can we ensure that important records are preserved indefinitely."

He also stressed the cultural and historical value of the documents that are scattered about town – records the public and genealogists would be interested in.

iStock photo.

"We don't know what's in these basements, and if we're asked about a particular document, we can't just go down to the basement and find it. That would take forever," he said at the meeting.

If passed, the bills before the council should ease these problems. The records would be taken to a central location and indexed there.

The bills are expected to pass and be signed into law. Councilmember Darlene Harris is firmly behind the push: "We have in the basement many, many records just tossed that are turning black with mold, and we have to do something," she said.

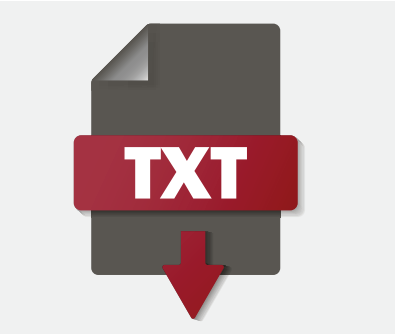
DATA CAPTURE

U.S. Agencies May Have to Deal With Text Message Archiving

A poll conducted by Smarsh, a company that provides archiving and retention solutions, suggests that most U.S. public agencies (70%) allow staff to conduct official business via texting, but only 46% of those agencies have controls in place to capture and retain the content.

As noted on *Law.com,* the report polled 236 respondents from city, county, and state government agencies.

"So many public agencies are flying without a net. We're seeing more and more examples of agencies running into very public legal challenges—putting taxpayer resources



at risk—as a result of ungoverned mobile communications," said Bonnie Page, Smarsh general counsel.

The article indicates that Freedom of Information Act (FOIA) requests are rising at the same time. Data collected by The FOIA Project, a nonprofit entity, finds that FOIA lawsuits jumped 26% between 2016 and 2017.

Smarsh's Page believes the trend will increase as courts continue to define what constitutes a public record.

"Every state court that has decided the issue has declared text messages to be public records which are producible unless exempt," she said.

Meanwhile, the sense of urgency for capturing such data may be lacking. Only 32% of respondents said they expected their organizations to capture text communications by 2020, and one-fifth said their agencies would "likely not ever" archive texts.

COPPA

FTC Urges Knowledge of COPPA Mandates for Data Destruction

FTC.gov encourages organizations to take a closer look at their retention policies to ensure they are fully complying with the Children's Online Privacy Protection Act (COPPA). Most companies are aware of the law's mandate for getting parental consent before collecting personal data about children, but many are not aware of a separate COPPA requirement for destruction.

COPPA requires companies to give parents the right to review and delete their children's information, but the law in some cases requires them to delete the personal data, even if the parents don't ask them to.

The article gives the example of a subscription-based app that offers children under 13 various games and learning tools. If the parent decides not to renew the service, can the company keep the child's personal information?

According to *FTC.gov*, no it cannot. Under Section 312.10 of COPPA, a company can retain children's personal information "for only as long as is reasonably necessary to fulfill the purpose for which the information was collected." After that, the company must delete it using reasonable measures to ensure secure destruction.

The FTC site offers these questions to help organizations navigate COPPA's data retention and deletion requirements:

- What types of personal information are you collecting from children?
- What is your stated purpose for collecting the information?
- How long do you need to hold on to the information to fulfill the purpose for which it was initially collected? For example, do you still need information you collected a year ago?
- Does the purpose for using the information end with an account deletion, subscription cancellation, or account inactivity?
- When it's time to delete information, are you doing it securely?

The FTC asserts that it has resources to help companies streamline COPPA compliance.

PRIVACY LAW

New California Privacy Law to Affect 500,000 U.S. Organizations

On June 28, California passed the California Consumer Privacy Act of 2018, a compromise measure that staved off an even tougher ballot initiative. The new law will apply to more than half a million U.S. companies, most of them small or medium-sized organizations, according to analysis done by the International Association of Privacy Professionals (IAPP).

The new act provides Californians with a right to transparency about data collection, a right to be forgotten, a right to data portability, and a right to opt out of having their data sold (opt in, for minors). It applies to organizations that collect consumers' personal information and those that sell such information or disclose it for a business purpose.

The law defines "business" as a for-profit legal entity that collects consumers' personal information and does business in the state of California. IAPP, in a news item, says "we assume that this law does not apply to nonprofit entities, although that is not entirely clear from the definition." IAPP further presumes that "doing business" in California applies to organizations that sell goods or services to California residents even if the organization is not physically located in the state.

To fall within the law's reach, an organization must meet one of these conditions:

- Have $25 million or more in annual revenue
- Possess the personal data of more than 50,000 "consumers, households, or devices"
- Earn more than half of its annual revenue selling consumers' personal data

A "consumer" is defined as every individual who is in the state for other than a temporary or transitory purpose, or every individual who is domiciled in the state who is outside it for a temporary or transitory purpose. The definition includes Californians while they travel. The IAPP suggests that 111,859 organizations would be affected in California, and 507,280 in the United States.

The law does not apply to data that is already regulated under the Health Insurance Portability and Accountability Act, the Graham-Leach Bliley Act, the Fair Credit Reporting Act, or the Drivers' Privacy Protection Act.

ELECTRONIC RECORDS

Senate Bill Proposes Electronic Reporting Only

The Senate Homeland Security and Governmental Affairs Committee has approved S-3027, which would require federal agencies to send reports and other materials to Congress only by e-mail or other electronic means, according to *FedWeek.com*.

Ranking Democrat Claire McCaskill of Missouri noted the expenses of sending paper copies, often in large multiples, as one purpose for the bill. Additionally, the measure would require that information be sent in spreadsheets or other appropriate formats for structured data.

ARMA connected *intelligence*

Job Descriptions

for Information Management and Information Governance

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

NOW AVAILABLE

Members Download **$45**

(non-member price: $65)

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

ARMA INTERNATIONAL BOOKSTORE

COMPLIANCE

NSA Deletes all Phone, Text Records Since 2015 – to 'Remain Compliant'

As reported by *The New York Times* and many other sources, the National Security Agency (NSA) is deleting all of its phone call and text records since 2015 – known as call detail records or CDRs – in an effort to remain compliant. In other words, because the NSA had collected some data it should not have, the agency will delete all CDRs acquired since 2015.

Title V of the Foreign Intelligence Surveillance Act (FISA) gives the NSA the authority to collect CDRs. A few months ago, according to reports, NSA analysts discovered irregularities in some of the telecommunications data it had collected. These irregularities led to CDRs the agency was not authorized to access.

"Because it was infeasible to identify and isolate properly produced data, NSA concluded that it should not use any of the CDRs," an agency statement said. "Consequently, NSA, in consultation with the Department of Justice and the Office of the Director of National Intelligence, decided that the appropriate course of action was to delete all CDRs."

According to the NSA statement, deletion began on May 23. A *New York Times* report indicated the data could comprise some hundreds of millions of records.

'CYBER-SOVEREIGNTY'

Vietnam's New Law Puts Facebook, Google, Other Techs into a Tricky Place

A *Bloomberg.com* article suggests that if Google and Facebook choose to comply with Vietnam's new cybersecurity law, they would be violating their own terms of service to protect the privacy of their users. At least that's the view of Tim Bajarin, president of a California-based tech research firm called Creative Strategies Inc., who spoke to Bloomberg. "Officials could also censor content at will given the way the law is written," he said.

The law goes into effect January 1. It requires foreign Internet companies to store data within Vietnam and to open local offices. Upon request, such companies would have to provide the government with data of users it suspects are threats in some way to the nation.

The new law mirrors global efforts to guard domestic users' information and open the access to data that governments claim they need to combat threats. "It also reflects a growing wariness about the influence of internet and social media giants that handle and parse information on and for billions around the world," writes John Boudreau of Bloomberg.

Vietnam's efforts to have more control over its peoples' online activities emphasize the dilemma that many tech companies now face. Apple Inc., for instance, agreed to construct a data center and blocked many apps in China in order to comply with that nation's laws. Indonesia promises to ban social media providers who don't comply with tough demands to filter content its government deems as obscene.

The Vietnamese government has increased its arrests of activists since 2016. Last year, officials reportedly deployed a 10,000-member cyber-warfare squad to fight what the government sees as a growing threat of "wrongful views." President Tran Dai Quang says the regulations are necessary to maintain social order and prevent "plots of hostile and reactionary forces," according to a post on the government's website.

Facebook and Google declined the Bloomberg requests to comment on whether they will comply with the law.