Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Detecting Misconduct in Real-Time

Assessing Your Digital Marketing Risk

Balancing Social Media and Compliance Risks

SAI Global: This Compliance Violation Will Self-Destruct in 24 Hours

Managing Data Security and Privacy Risks 2.0

Is Blockchain Technology FinTech's Magic Bullet?

Mounting a Defense Against

Digital Media Risk

An e-Book publication sponsored by SAI GLOBAL

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives.

SAI GLOBAL

SAI Global helps organizations manage risk, protect reputation and perform better in an increasingly complex and interconnected ethical and regulatory environment. The company's solutions include risk management software, standards and regulatory content, ethics and compliance learning, risk assessments, certification, testing and audits. In Australia, SAI Global are also a leading provider of settlement related services; company, personal and property information.

Inside this e-Book:

Detecting Misconduct in Real-Time 4
Assessing Your Digital Marketing Risk 6
Balancing Social Media and Compliance Risks 8
SAI Global: This Compliance Violation Will Self-Destruct in 24 Hours 10
Managing Data Security and Privacy Risks 2.0 14
Is Blockchain Technology FinTech's Magic Bullet? 16

Detecting Misconduct in Real-Time

As the financial sector embraces the speed and efficiency of instant messaging services, compliance officers have a new challenge: how to detect misconduct in real time

by Joe Mont

Not so long ago banks and financial services firms were poised to swear off social media and instant messaging. Faced with the Sarbanes-Oxley Act's record retention demands and the risk of employees using social media communication for illicit behavior, the compliance risks outweighed the benefits.

That line in the sand blew away over time. Traders found that in-house messaging services—and even external offerings from Google, Yahoo, and AOL—offered speed and increased productivity. Executives glued to smartphones and tablets couldn't be weaned off that addiction.

"Compliance wants it all locked down and controlled, and the other side wants as much information and speed of communication as possible," says Cromwell Fraser, director of NICE Actimize's communications surveillance portfolio.

Let's be honest: The other side won.

That being said, the ubiquity of these modern communication tools, and their eventual embrace by financial firms, has validated initial concerns. If you want proof, read the chat logs of individuals caught in the recent rate-rigging scandals for LIBOR and foreign exchange. You'll find plenty of evidence all over those communications. Security of those instant messages is another concern, regardless of whether your employees are chatting about misconduct or anything else.

The latter concern explains the recent scrutiny of a new chat service aimed at banks. The programs, called Symphony, is funded by a consortium that includes Goldman Sachs, Bank of America, BNY Mellon, BlackRock, Citigroup, Deutsche Bank, JPMorgan, Morgan Stanley, Wells Fargo, and others. Symphony also boasts that its built-in security measures can prevent "government spying."

Warren

That claim caught the attention of Sen. Elizabeth Warren (D-Mass.). In August 2015, she laid out her concerns to bank regulators, the Securities and Exchange Commission, and other regulators in writing.

"The communications that Symphony will allow companies to hide from 'government spying,' such as text messages and chat room transcripts, have proven to be key evidence in many previous regulatory and compliance cases that have uncovered criminal action by Wall Street," Warren wrote. She urged the agencies to assess how the technology could affect their enforcement efforts.

Warren even pointed to the LIBOR and forex rate-fixing scandals as evidence of her point. "It was the trail of such messages that permitted regulators both to discover and prosecute these financial crimes, resulting in this case in admissions of wrongdoing and a settlement of $6 billion in fines and penalties," she added.

Also firing a shot is Anthony Albanese, acting superintendent for New York's Department of Financial Services. In a letter to banks in July, he demanded that they report back on how they intend to use Symphony products; what personnel will be using them; whether Symphony will be used in conjunction with or to the exclusion of other communications services; how messages will be retained; and whether the encryption technology can be used to prevent review by compliance personnel or regulators.

> "Compliance wants it all locked down and controlled, and the other side wants as much information and speed of communication as possible."
>
> Cromwell Fraser, Director, Communications Surveillance Portfolio, NICE Actimize

Albanese also asked how the banks intend to prevent their employees from adapting the service to circumvent compliance controls and regulatory review.

The regulatory scrutiny comes at an interesting time for vendors providing chat services. In the past year many have added new features and services, and competition is fierce. Among the big name players in the space are Bloomberg, Markit, NICE Actimize, Intercontinental Exchange (through its acquisition of a Web-based chat platform), CME Group (an investor in Wickr, a start-up offering military-grade encrypted and self-destructing messages), Thomson Reuters, and Microsoft with its Lync service.

Here Comes the Problem

The challenge for compliance programs isn't so much the need to archive and retrieve messages for e-discovery or regulatory exams any longer (although those are still headaches). The real problem is how to monitor chats in real time and keep pace with innovative ways employees are communicating. Even something as simple as a winking emoji could be a covert signal.

"Not only is compliance paying more attention to it; the regulators are requesting an evolution of how they approach it," Fraser says. "Instead of employing a small team of people in the back to just listen or read random chat messages, you want to utilize those people to be far more effective and actually try to monitor for risk on all forms of communication."

"Compliance teams are informing some of the technol-

ogy decisions and seeking consolidation of the number of messaging systems to reduce risk and exposure, increase control, and reduce their firm's total cost of ownership," says Lesli Fairchild, head of compliance and administration for collaboration services at Thomson Reuters. "While needs may vary … the main themes to emerge have been around heightened controls, automation, alerting, and insight delivered through enhanced reporting capabilities."

Those demands partly drive the fierce competition among vendors. In December 2014, Bloomberg launched its "Compliance Center," a dashboard for compliance officers that provides the ability to block unauthorized employee communications before they are sent. Recently, Thomson Reuters added a feature to its flagship chat service, Eikon Messenger, which allows compliance officers to restrict who specific employees or departments are allowed to communicate with via chat. It also provides keyword controls that can block and flag terminology that might indicate a problem.

"In the wake of the LIBOR and FX fixing scandals, banks no longer allow multidealer communication between traders from more than two firms," Fairchild said. "Unauthorized multilateral chat rooms are rarely sanctioned by compliance officials unless they are for legitimate business use and pre-approved by them." A "managed chat room" allows a compliance officer to restrict or allow multilateral communications.

Digging through old chat logs to uncover evidence is one thing; finding misconduct as it happens is quite another, especially when participants speak in code words. This sort of monitoring requires smarter technology, Fraser says.

"The only way you are going to spot something is to notice that the words being used in the sentence are out of context," he says. Technology is getting better at seeking out odd syntax, random words, and sentence structures that do not make sense.

In Fraser's view, the solution is to combine technology with human intuition. "I would question any compliance officer who lets technology do all the work," he says. "You need to be using the technology to try to focus what you want humans to look at. The technology is there to help you break down the noise. You can do a lot with the technology, but you are always going to need a sanity check from a human once the technology has made a decision."

Valentine

Denise Valentine, a senior analyst with Aite Group, suggests a risk management approach to chat monitoring. Before relying on technology, segment and prioritize who you are tracking and how deeply you plan to dig into e-mails, texts, or messages. For example, trader profiles can assist with surveillance. A change in that trader's behavior can escalate matters to a compliance officer for further review.

When adopting surveillance technology, compliance officers also need to ensure that it is configured in a way that is easy for them to use. "This is confidential information," Valentine says. "You cannot have the IT desk knowing everything." ■

WARREN'S CONCERNS

The following is a selection from Sen. Elizabeth Warren's Aug. 10, 2015, letter to the Securities and Exchange Commission regarding Symphony Bank.

… the New York State Department of Financial Services wrote to Symphony regarding concerns that the new communication system could be used to "circumvent compliance controls and regulatory review."

I have similar concerns about how the biggest banks' use of this new communications tool will impact compliance and enforcement by the Securities and Exchange Commission at the federal level. My concerns are exacerbated by Symphony's publicly available descriptions of the new communications system, which appear to put companies on notice—with a wink and a nod—that they can use Symphony to reduce compliance and enforcement concerns.

Symphony claims that "[i]n the past, communication tools designed for the financial services sector were limited in reach and effectiveness by strict regulatory compliance … We're changing the communication paradigm." The company's website boasts that it has special tools to "prevent government spying," that "there are no backdoors," and that "Symphony has designed a specific set of procedures to guarantee that data deletion is permanent."

When banks fixed interest rates (LIBOR) in direct violation of the law, they used chat rooms and text messages to coordinate their activities, and it was the trail of such messages that permitted regulators both to discover and prosecute these financial crimes, resulting in this case in admissions of wrongdoing and a settlement of $6 billion in fines and penalties.

The communications that Symphony will allow companies to hide from 'government spying—such as text messages and chat room transcripts—have proven to be "key evidence: n previous regulatory and compliance cases that have uncovered criminal action by Wall Street. If banks are now making this information more difficult for regulators to obtain and interpret, it could prevent regulators from identifying and preventing future illegal behavior.

[Warren also asked each regulator to respond to the following information requests …]

» Your agency's existing rules for communications retention and encryption and whether Symphony may make it easier for financial firms to evade these rules.

» The impact of symphony's 'end to end encryption' with 'no back doors' on your agency's ability to obtain and interpret relevant compliance-related communications by financial firms.

» The impact of Symphony's approach to permanent data deletion on your agency's ability to obtain and interpret relevant compliance-related communications by financial firms.

Source: Securities and Exchange Commission.

Assessing Your Digital Marketing Risk

Internal auditors with not enough to do, cheer up: Digital marketing risk is emerging as a new headache to keep you busy. Data theft and fraud are rampant, and ways to find and seal up those weaknesses aren't entirely clear

by Tammy Whitehouse

Cyber-security has taken a new twist as companies begin to assess risks posed by sales and marketing activities that rely on digital channels and social media.

Long gone is the deliberate pace of marketing from the "Mad Men" era, where teams took days or more to mock up proposed print advertising that went through multiple layers of review. Digital marketing moves more quickly, involves more people, can trigger more regulatory oversight, and is far more prone to fraud or data theft than anything Don Draper worried about.

Little surprise, then, that Corporate Executive Board lists digital marketing as a "hot spot" in internal audit planning that deserves greater corporate attention. The rise in digital marketing gives companies the ability as never before to target their sales and marketing activities to specific customers. But it also produces reputational and data privacy risks playing out in news headlines with greater frequency, CEB says.

"This is something many internal auditors are not familiar with," says Ruth Shaikh, associate director at CEB who performed the research that led to CEB's conclusions. "When we talk about digital marketing, we mean use by companies of digital channels—like social media, e-mail, Web applications—to connect with their customers and stakeholders." The idea that digital marketing channels can create risk is perhaps not news to internal auditors, she says. Knowing how those risks are created, and what controls should be in place to mitigate them, is a work in progress.

The potential risks are every bit as numerous and complex as the modern digital supply chain and its long list of characters, says Danielle Ritter, assurance director for PwC who works primarily in technology and media sectors. "If you're sharing data, what are you sharing?" she asks. "Who are the partners you're working with? Who is helping you deliver or build your digital marketing campaign? Internal auditors may want to evaluate the risks of those parties." That's a key part of protecting the data the company is sharing with its service providers, she says.

Digital marketing fraud is rampant, says Linda Wooley, president and CEO of Trustworthy Accountability Group, a grassroots organization trying to combat the problem and give companies standards and tools to protect themselves. "The entire supply chain is very complicated, with a lot of parties in the chain to deliver a digital ad," she says.

The supply chain even for something as simple as an online advertisement has advertisers, ad agencies, ad buyers, advertising networks, ad exchanges, publishers, and auctions to bid for ad dollars and placements. Along the way, nefarious players sneak into the system and siphon off ad dollars that never deliver the advertising impressions intended, she says.

> "You don't always see marketing and advertising as a high focus in the internal audit plan, but companies should start by inventorying what their digital marketing touch is."
>
> Danielle Ritter, Assurance Director, PwC

Another risk, Wooley says, is piracy: rogue players picking off legitimate ads and creating spoofs re-directed to fraudulent URLs. "It looks as if those ads appeared somewhere, so the criminals are paid, but the ad was not seen by a human," she says. "And there are many, many more types of fraud in the system."

The Association of National Advertisers released a study showing that advertisers will lose $6.3 billion of their advertising spend globally in 2015 to non-human bot traffic. The scam is that "clicks" on online advertisements are made by machines with no actual spending power, rather than humans that the advertisers were paying to get. For U.S. companies, that amounts to as much as 30 to 50 percent of a company's digital advertising budget, Wooley says.

"So you have chief marketing officers looking at their budget and saying 30 to 50 percent of what I spend on digital advertising is wasted," she says. "That's not sustainable."

Getting Ahead of the Problem

TAG is in the early stages of creating standards for participants in the digital advertising supply chain, intended to reduce the ability of illegitimate players to weasel their way in. Such standards will be helpful not only to advertising and sales executives, but to internal auditors as well, she says. "There will be business rules for everybody who operates in the ecosystem. These will be things you need to do to vet your vendors."

The role of internal auditors is to become much more educated on digital marketing risks and to help manage

those risks across the enterprises, Ritter says. "Digital marketing is a relatively new area of risk, and it's constantly changing," she says. "You don't always see marketing and advertising as a high focus in the internal audit plan, but companies should start by inventorying what their digital marketing touch is."

> "Now we're seeing more instances of social hijacking, more cases where parties outside are coming in and doing damage. Companies haven't viewed it that way very much."
>
> Bill Michalisin, Chief Marketing Officer, Institute of Internal Auditors

Bill Michalisin, chief marketing officer for the Institute of Internal Auditors, says internal audit's focus so far for digital marketing risks has been centered on the employee side, or what orgainzations are doing internally. "Now we're seeing more instances of social hijacking, more cases where parties outside are coming in and doing damage," Michalisin says. "Companies haven't viewed it that way very much."

Interest in more education and information on digital marketing risks is growing in internal audit circles, Michalisin says. "It's a newer area, so I don't know if we can say there are even best practices yet per se," Michalisin says. "There is a need for peers to share ideas and strategies they can start to put into place to address this. There is demand for that."

Michalisin suggests internal auditors start the dialogue within their own organizations to assess the company's exposure as a result of its digital marketing activities. "Once internal audit has a full view, they can bring to the conversation their expertise and their perspective around mitigating risks and evaluating controls."

Stippich

Warren Stippich, a partner and national GRC leader for Big 4 audit firm Grant Thornton, says larger organizations that are brand-driven and consumer-oriented generally are much further along the learning curve in assessing and responding to digital marketing risks, but virtually any company could potentially benefit from reviewing their policies and procedures. Before digital, sales, and marketing activities generally were subject to layers of internal approval before anything would be released to the public, Stippich says.

"Now, anyone can upload and hit 'post,' and it happens in seconds, read by tens of thousands of constituents," he says. "That's a big risk." ■

THE LOWDOWN ON TRAFFIC BOTS

Below the IAB offers information on why traffic bots are dangerous and guidance on what to do to protect your company.

Some of the ways bot code generates false traffic:

- Generating ad views while consumers browse unaware.
- Hijacking user controls to generate fake clicks when the computer is dormant.
- Running invisible processes behind the scenes to simulate consumer activity.
- Compromising cookie data to simulate high-value consumers.

Why you should care

Allowing the bad actors in our industry to profit from traffic fraud affects the entire online community. In addition to diluting inventory value and diverting funds from legitimate businesses, traffic fraud undermines the integrity of digital media.

Some of the negative impacts of traffic fraud:

- Brands waste money on ad campaigns that are served to invisible inventory.
- Digital media is degraded, and brands look elsewhere for their marketing solutions.
- Ad performance and website visit data are contaminated, undermining analysis.
- Artificial fraudulent inventory floods the market and decreases the value of legitimate (real human) inventory.
- Criminal activity is enabled.
- The industry may be subjected to government oversight, negative press and potentially business-dampening enforcement.

What You Can Do

The solutions to traffic fraud are not always intuitive. For example, the outright blocking of fraudulent traffic gives information to the fraudsters that helps them blend in better and become more difficult to identify.

In addition to the following general guidelines, steps specific to buyers, publishers and networks are outlined in subsequent sections.

The following general guidelines can help any online business get started:

- Educate yourself about traffic fraud and the risks that it poses to your business.
- Adopt policies and strategies to identify fraud and mitigate its impact.
- If you are an advertiser, set clear objectives for your media campaigns that focus on the measurement of real ROI, which is difficult for fraudsters to falsify. Measures such as click-through rate, completion rate, and last-touch attribution are easy to game.
- Practice safe sourcing and trust only business partners who have earned trust.
- Implement technology to detect and prevent fraud.
- Filter traffic through vendors who prioritize fraud detection.

Source: IAB.

Balancing Social Media and Compliance Risks

Companies must craft policies that don't overly restrict the business from leveraging social media, while addressing both regulatory and reputational risk

by Karen Kroll

Companies still face huge risks when they communicate via social media Websites.

Some industries, such as financial services and healthcare, must still navigate lots of regulations when communicating over social media sites. And even if a message doesn't spark action by regulators, the possibility that a thoughtless or offensive Tweet or Facebook post will generate negative publicity, alienating customers or business partners is real.

There are also risks for companies in how they deal with employees' use of social media or if they ignore social media completely. "If you don't participate in social media, you run the risk of not knowing what others are saying, unfiltered, about your brand," says Lizzie Roscoe, social media manager of global digital communications at McDonalds. "You miss the opportunity to engage with consumers online."

Rather than ignore or avoid social media, companies can benefit by identifying ways to use it to promote their interests that don't violate regulations or incite a backlash. The key is identifying "what you are trying to accomplish and how you can do it in a way that makes sense without being burdensome but still protecting what you need to protect," says Kathryn Ossian, founder of law firm Ossian Law and editor of the book, *Social Media and the Law*.

Compliance officers must balance the opportunity for the company to leverage social media as a powerful communications tool with the risks it presents. For starters, companies need to train employees and create policies that can reduce the risk of improper or illegal use of social media, yet they can't implement policies so broad that they violate labor laws. A policy that requires employees to gain approval, for example, before posting any work-related comments on any social media—including their own accounts—essentially restricts employees from talking about their working conditions, which would violate the National L In many cases, companies' ability to censor employees' personal social media messages may be limited to requiring them to keep any confidential corporate information confidential, and to refrain from intentionally harming the company's reputation or legitimate business interests, says Lothar Determann, partner with the law firm of Baker & McKenzie and author of *Determann's Field Guide to International Data Privacy Law Compliance*.

Companies also need to protect their data, along with any client data they retain, from threats or malware that arrive via social media, says Joanna Belbey, social media and compliance specialist with Actiance, a provider of communication, collaboration, and social media governance solutions. Labor Relations Act, Ossian says.

It's worth pointing out to employees, adds Belbey, that the laws and policies that apply offline also apply in the virtual world. For instance, any advertising messages disseminated via social media—just like those on television or in print—can't mislead and claims must be substantiated in certain cases, Belbey says.

Social media messages also can be subject to record retention requirements. "If you type it, it's a record," Belbey says. That's of particular concern in highly regulated industries, such as financial services.

Similarly, social media comments or posts may be subject to litigation holds and used in court proceedings, Determann says. In these cases, an employer involved in litigation may struggle to ensure that the holder of the account can't delete or manipulate the data related to the proceedings, even if it resides within a personal account.

Mitigating the Risks

While the risks of engaging customers and others via social media are real, trying to avoid social media means losing valuable opportunities to promote your brand. "Consumers are already talking about the brand, so it's imperative that they're also talking with the brand," Roscoe says.

REGULATORY GUIDANCE

Many regulatory agencies have been developing guidance on the appropriate use of social media for the industries under their purview.

Among the information issued so far:

- The FDA's Guidance for Industry Fulfilling Regulatory Requirements for Postmarketing Submissions of Interactive Promotional Media for Prescription Human and Animal Drugs and Biologics

  (Draft guidelines, issued January 2014)
  http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM381352.pdf

- The FFEIC: Social Media: Consumer Compliance Risk Management Guidance

  (Final guidance, issued December 2013)
  http://www.ffiec.gov/press/pr121113.htm

- The SEC: Guidance Update on Social Media Filings by Investment Companies

  (Guidance update, issued March 2013)
  http://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171513280#.UyHkjChsI1c

Moreover, prohibiting the use of social media among employees can tempt them to engage in it surreptitiously, Determann notes. When that occurs, the company's ability to track the conversations is reduced. Such a policy can even lead to a loss of talent, as some employees may balk at what they see as corporate over-reach, or take technology and communications preferences into account when searching for employment.

> "If you don't participate in social media, you run the risk of not knowing what others are saying—unfiltered—about your brand. You miss the opportunity to engage with consumers online."
>
> Lizzie Roscoe, Social Media Manager, McDonalds Corp.

The goal is to develop an approach and policies that allow for the use of social media within parameters that enable the company to meet its compliance obligations and minimize the risk of offensive or tasteless messages.

Selecting the right platform for a particular objective is essential, Determann says. Open, public platforms like Twitter and Facebook can be great for disseminating information to a large group of people. Companies that want employees to collaborate and share confidential information with a select group of co-workers or business partners, however, probably will find a secure intranet more effective.

It's also important to bring together top stakeholders to outline the social media risks most relevant to the organization, as well as tactics to mitigate them, Belbey says.

At McDonalds, for instance, the communications, marketing, legal, IT, and technology audit groups are among the teams providing input to the company's social media initiatives, says Guy Pieroni, director of technology audit. "Everyone comes with a different perspective," which helps ensure that all angles are covered, he adds.

It's also important to develop policies to guide employees' and the company's use of social media. While the purpose of social media technology differs significantly from, for instance, a payroll or accounting system, some of the same control mechanisms come into play, Pieroni points out. That may mean formally provisioning access to the company's social media profiles and requiring those allowed access to follow an established sign-in procedure. "We can take our existing set of policies and frameworks and apply them in a slightly different way," he says.

Just as important as the policies in place is a commitment to ensuring that they're followed. Belbey notes that SEC examiners working with a company not only review the policies, but also interview its employees to assess how completely they're being followed. Firms need to develop reasonably enforceable policies, and then follow them.

While critical, policies and supervision are not enough. Employees also need to be trained in the prudent, legal use of social media, Determann says. Given how rapidly electronic communication can travel, and how fast technology changes, it's almost impossible to cover every situation with a law. "You have to trust employees to do the right thing at short notice and when they're under pressure," he says.

Technology can also play a role in ensuring that a company's social media initiatives comply with applicable regulations and remain within the company's guidelines. Among other capabilities, technology solutions can maintain social media records, provide a repository of pre-approved content, and flag words in social media messages that might be problematic, Belbey says. "You come up with policies and then use technology to do what the policies say." ■

DON'T IGNORE INVESTORS

Below is an excerpt from the Securities and Exchange Commission announcement regarding use of social media for corporate announcemounts.

The Securities and Exchange Commission [in 2013] issued a report that makes clear that companies can use social media outlets like Facebook and Twitter to announce key information in compliance with Regulation Fair Disclosure (Regulation FD) so long as investors have been alerted about which social media will be used to disseminate such information.

The SEC's report of investigation confirms that Regulation FD applies to social media and other emerging means of communication used by public companies the same way it applies to company websites.

The SEC issued guidance in 2008 clarifying that websites can serve as an effective means for disseminating information to investors if they've been made aware that's where to look for it. Today's report clarifies that company communications made through social media channels could constitute selective disclosures and, therefore, require careful Regulation FD analysis.

"One set of shareholders should not be able to get a jump on other shareholders just because the company is selectively disclosing important information," said George Canellos, acting director of the SEC's Division of Enforcement. "Most social media are perfectly suitable methods for communicating with investors, but not if the access is restricted or if investors don't know that's where they need to turn to get the latest news."

Regulation FD requires companies to distribute material information in a manner reasonably designed to get that information out to the general public broadly and non-exclusively. It is intended to ensure that all investors have the ability to gain access to material information at the same time.

Source: Securities and Exchange Commission.

This compliance violation will self-destruct in 24 hours

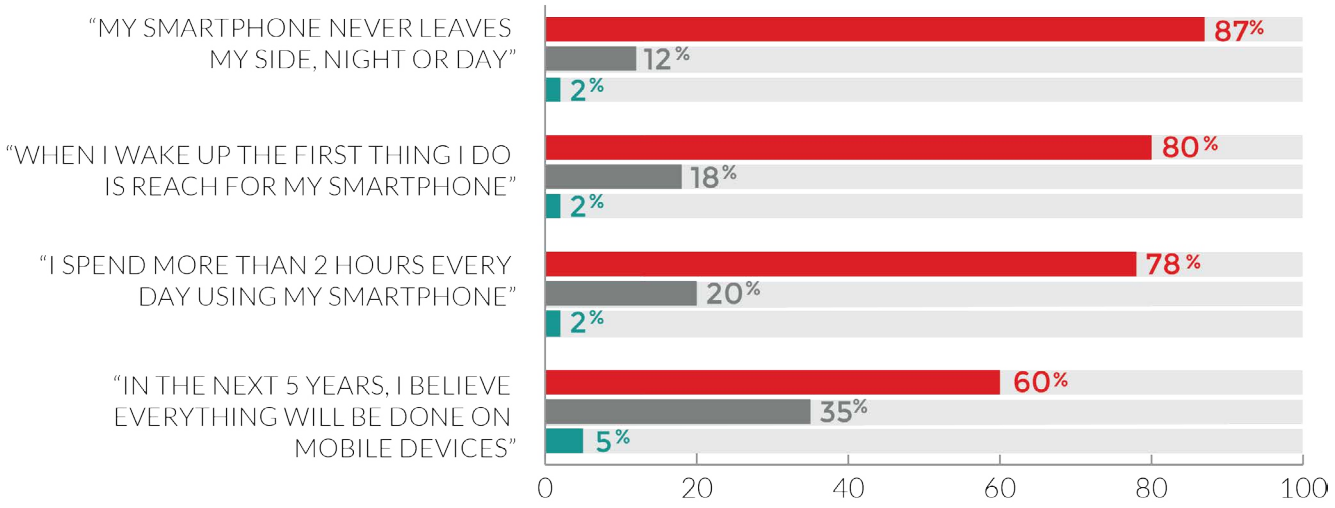
by Sean Freidlin, SAI Global

Over the past decade, innovations in digital media and social networks have transformed the frequency and nature of how we interact with our friends, family, colleagues, and the world. It's hard to believe that Facebook was released over 10 years ago, and how much has happened since as a result. While technology continues to change our daily behavior and habits, an underlying concern exists for employees whose ability to digest and distribute information is more powerful than ever. Even more concerned are the regulators, compliance officers, and corporate stakeholders who find themselves racing to control the risks associated with innovations they have little control over.

From a regulatory perspective, the speed at which organizations can understand and react to new risks presented by digital and social media is inherently slower than the speed at which these digital properties can release a product update or new feature that creates a new series of regulatory questions. That doesn't even scratch the surface of the time and effort it takes to implement an actual regulation, bill, law, or rule that governs how we use these new digital innovations and social platforms. Meanwhile, chief compliance officers and their colleagues, who are responsible for prevention, awareness, and countless other tasks, are stuck with the expectation of stopping bad things from happening without even knowing they are a possibility. This is not an insult to their market savvy as much as it is a testament to the speed at which technology trends evolve.

Kleiner Perkins Caufield & Byers (KPCB) is a renowned venture capital firm in Silicon Valley that publishes and presents an annual "Internet Trends" report, detailing important digital trends and insights on how they are changing the world. When it comes to the future of digital media, KPCB are experts. In considering the relationship between these trends, the future of compliance, and the risks that may arise as a result, there are some particularly important findings from their 2014 and 2015 reports. These findings are especially important when consid-

MILLENNIAL SMARTPHONE BEHAVIOR, USA, 2014



Source: KPCB Internet Trends 2015

ering the growing roles of millennials in the multigenerational workforce and the omnipresence of digital channels inside and out of office, across all industries and regions. Consider the following:

In the United States, rapidly evolving smartphone technology, combined with more affordable prices for these devices, has led to a massive shift in how we spend our time. According to research conducted by eMarketer shared in the 2015 KPCB Internet Trends report, the amount of time we spend watching television and looking at our laptops and desktops has remained static between 2010 and 2015, however, the amount of time spent looking at our mobile screens is now seven times higher than it was in 2010.

That statistic may not be very surprising to you. All you need to do is look around your office, or really anywhere you spend time, to notice that people are staring down more than they're looking up. But it's how people are spending time on their smartphones that should begin to make compliance professionals a bit more concerned about digital media risks.

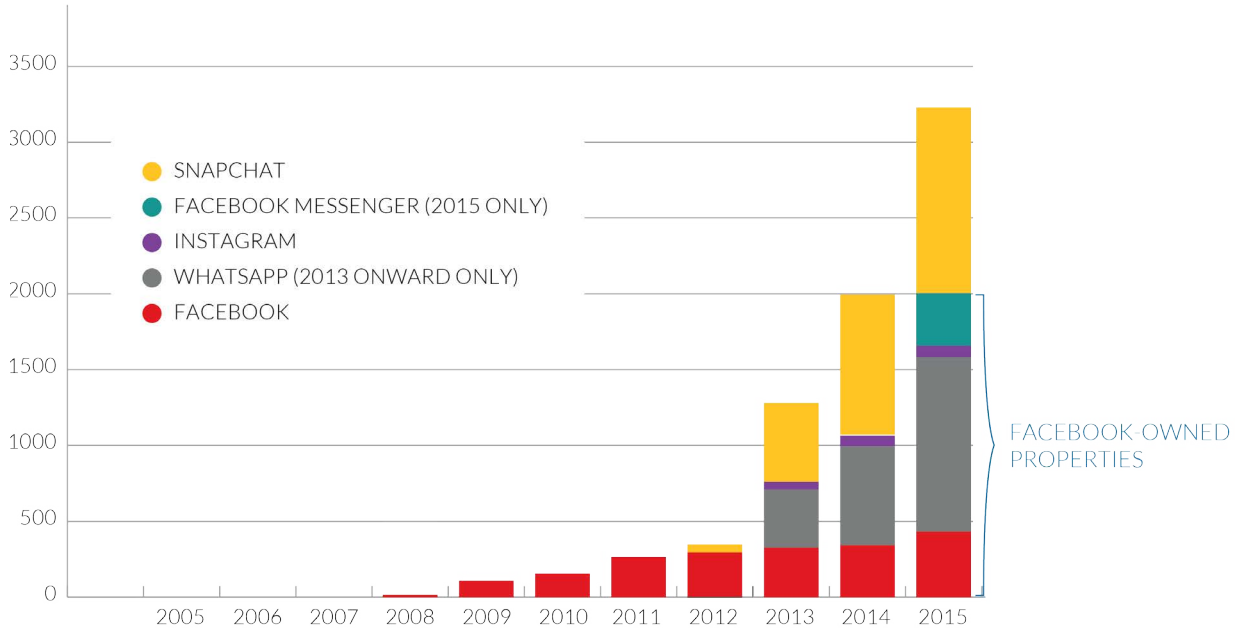
In 2010, most of that time was spent texting, writing, and typing, but in 2015 and beyond, the evolution of mobile usage has gone from text to image to video, and now, as you read this, streaming and disappearing video. Nine of the ten most used apps around the world are social media platforms or messaging programs. That includes ones you're probably familiar with and already cover in your compliance programs, like Facebook and Twitter, and ones you may be less familiar with and prepared for: Facebook Messenger, Line, Viber, KakaoTalk, WeChat, Instagram, and WhatsApp. Not included on that list, but gaining rapidly is Snapchat, which has seen a steady rise in popularity over the past year as Millennials and other mobile users grow tired of the original social media networks they may have joined years ago.

The 2014 KPCB report shows a staggering 1.8 billion photos uploaded and shared from smartphones every single day, a massive increase compared to the 250 million in 2010.

The report also includes a piece of data from Zogby Analytics from a survey of over 1,000 millennials (adults between 18 and 34 years old) asking them, "how often do you use your device's camera/video function?" 44% of millennials use their smartphone camera to take pictures or video at least once a day. On a weekly basis, 87% of millennials will use their smartphone to take a picture or video. When asked what they do with those pictures, 76% responded that they post them on social media, more than any other response.

The driver behind that jump isn't just the improved quality of smartphone cameras, but the presence of new apps that people simply love to use. In 2010, almost all photos being uploaded and shared were on Facebook. In 2015, WhatsApp accounts for over 600 million photos a day, trailing the industry leader Snapchat, which is responsible for over 800 million new photo uploads every day. Over 700 million "snaps" are sent every day on Snapchat, and the millions of photos sent on WhatsApp each day are only a small fraction of the 30 billion total messages sent on the app every day. According to an article published in *Bloomberg* on April 28th, Snapchat users

DAILY NUMBER OF PHOTOS SHARED ON SELECT PLATFORMS, GLOBAL, 2005 - 2015



Source: KPCB Internet Trends 2016

are now watching a combined 10 billion videos a day on the app. The number was 8 billion two months prior. What will it look like by 2017?

While the sheer popularity of these apps is impressive, the reason compliance officers need to be concerned about employees using WhatsApp and Snapchat is that the pictures and messages sent on these apps are not searchable or publicly available, making them more or less impossible to find. This is in stark contrast to when an employee posts something dangerous, incriminating, illegal, or downright foolish on Facebook or Twitter, which is usually easy to find and pretty quick to surface. The new breed of digital media harbors latent risk.

For WhatsApp, this is accomplished with End-to-End Encryption, an appealing aspect of guaranteed privacy to its users. To quote the FAQ on their website:

"Privacy and security is in our DNA, which is why we have end-to-end encryption in the latest versions of our app. When end-to-end encrypted, your messages, photos, videos, voice messages, documents, and calls are secured from falling into the wrong hands. End-to-end encryption is available when you and the people you message are on the latest versions of WhatsApp. WhatsApp's end-to-end encryption ensures only you and the person you're communicating with can read what is sent, and nobody in between, not even WhatsApp."

In a recent article, *WIRED* says End-to-End Encryption in apps like WhatsApp and Viber is "designed to make it technically impossible for anyone to read the services' messages other than the people in conversation: not eavesdropping hackers, not law enforcement, and not even the companies themselves."

Self-destructing messages that contain highly confidential information, company secrets, incriminating evidence, blackmail, and bribes used to be reserved for James Bond and other fictitious characters entertaining us on the silver screen. Today, anyone with a smartphone can channel their inner secret agent or evil villain, but unlike the movies we love, the risks and repercussions of these behaviors are very real.

For Snapchat, where "delete is our default" and 63% of the monthly users in the U.S. are between the ages of 18-34, the unique selling proposition of the app is the short-lived, fleeting, and temporary nature of the content shared on it. To quote their privacy policy:

"Snapchat lets you capture what it's like to live in the moment. On our end, that means that we automatically delete the content of your Snaps (the photo and video messages that you send your friends) from our servers after we detect that a Snap has been opened or has expired.

Self-destructing messages that contain highly confidential information, company secrets, incriminating evidence, blackmail, and bribes used to be reserved for James Bond and other fictitious characters entertaining us on the silver screen. Today, anyone with a smartphone can channel their inner secret agent or evil villain, but unlike the movies we love, the risks and repercussions of these behaviors are very real.

Not content to fall behind the times and lose their audience to new alternatives, Twitter and Facebook are also innovating the way people use their apps by focusing on video, and more specifically, live streaming video. These changes don't just reinforce trends that are happening today, but seem to signal a sign of things to come in the ways we share and digest information on our phones. In 2015, Twitter acquired Periscope, an app that lets anyone stream video in real time to a global audience. In the year that has followed, unprecedented levels of transparency and real-time video access have enabled triumphant new experiences, but also, extreme tragedy and moral ambiguity. Perform a Google search for "Periscope Controversy," and you will discover stories so chilling and unfortunate that I don't want to rewrite them here. Behind every one of these stories is a person holding a phone, consciously choosing to share with anyone willing to watch.

Not that Twitter needs to add live streaming video into their product offering to cause controversy and stir the regulatory pot, since their traditional 140-character messages have proven quite effective at accomplishing that. When Elon Musk, CEO of Tesla, wrote a tweet teasing the release of a "major new Tesla product line," it was retweeted over six thousand times and resulted in a sudden rise in the company's stock price equivalent to one billion dollars in market capitalization, leading some to accuse Musk of market manipulation. Over the past few months, Facebook has rolled out its own live video product, "Facebook Live", which lets anyone stream video to the Facebook community for up to 30 minutes. An early test case of the product's reach and appeal—a live video from Buzzfeed's office in which two employees methodically added rubber bands to a watermelon one by one until it exploded—attracted over 4 million viewers in one hour. A video posted by a woman in her car wearing a Chewbacca mask? 100 million viewers in 24 hours. Harmless for now to everyone but the watermelon, but who knows how the platform can be used in the future and what problems may stem as a result.

SAI GLOBAL

While these videos don't magically disappear, the risk lies in the live nature of the content itself. You can't regulate what you cannot see first or prepare for in advance. If an employee streams something live from the office or shares sensitive information in real time without advanced notice or prior screening, the only thing to do is prepare to deal with the repercussions. If your employee uses this technology outside of the office to break the law, how will that reflect on you, the employer?

In some industries, these digital risks can be even more dangerous to a business. How do finance companies and Wall Street firms prevent insider trading or market manipulation if their employees are sharing sensitive, private data over Snapchat, WhatsApp, and other channels that can't be easily tracked? What happens when a Facebook Live session from the office, intended to connect with an online community and reinforce corporate transparency, ends up a bit too transparent by accidentally sharing information on someone's desk or computer screen that wasn't meant for the whole world? What happens when these firms develop their own technology to send confidential messages?

Dubbed as "the WhatsApp for the financial world" by *Reuters*, Symphony is 75,000 users strong, heavily funded by venture capital, and growing fast. It's designed as a flexible, secure messaging service that allows financial firms, corporate customers, and individuals to host texts, chats, and e-mails on one centralized platform. If it sounds a bit like a Bloomberg terminal, it's because that's the very device they're hoping to replace. While many spectators are sceptical that the service will simply enable finance companies to act illicitly and avoid regulators, Symphony's creators sell their vision as "the next wave in organizational productivity" without "compromising on organizational compliance." Whether regulators and the public buy that or not, it's simply another instance of new technology coming into the fold to disrupt the way things used to work and create new problems for compliance departments to try and solve.

So what can compliance professionals do to help prevent these digital risks? For starters, they can use smartphones to their own advantage as a resource and education tool. According to the 2015 KPCB report, 52% of smartphone owners use their phone to get help in an emergency situation. It is one thing to train and reinforce lessons over time in advance of a situation or circumstance where things can go wrong, but it is another thing entirely to provide ethical guidance and compliance resources to someone in an on-demand, "just in time" capacity at the moment of truth. I can't speak for everyone reading this, but when I don't know something, my first instinct is to pull out my phone and Google it. Creating a similar resource for your Code of Conduct and compliance program may be the best way of helping prevent an emergency situation from becoming a potential violation.

The way people use the internet and digital media in their personal lives drives expectations and behavior in the workplace; in this context, traditional compliance training and other resources look stale and outdated. We can't expect to push, essentially static, information at employees in a world where expectations are for a dynamic, two-way dialogue. We need to embrace social and collaborative tools for compliance and learning.

The "just in case" model for the management of compliance risk is redundant; as an industry, we can't continue to do two-hour training once a year "just in case" someone experiences a compliance risk several months later (and hope that they remember what we told them)—we need to provide meaningful "just in time" performance support at the point in time when risk occurs and useful support is needed. Smartphones are the perfect tool to aid this evolutionary method of learning.

We need to get personal. For millenials especially, the barriers between professional life and personal values are blurring—the fear factor of "comply or suffer the consequences" is not a compelling argument for this audience. We need to appeal to common human values by highlighting the human (and global) consequences of compliance risk to win hearts and minds and drive compliant, ethical behaviors.

We need to get personal. For millennials especially, the barriers between professional life and personal values are blurring—the fear factor of "comply or suffer the consequences" is not a compelling argument for this audience. We need to appeal to common human values by highlighting the human (and global) consequences of compliance risk to win hearts and minds and drive compliant, ethical behaviors.

As digital media continues to change our lives, our only choice is to change with it. To reduce risk in the future, we're going to have to take a few risks of our own.

To talk to the team at SAI Global about your compliance and ethics program requirements in the age of digital media risk, contact them at marketing.americas@saiglobal.com or visit www.saiglobal.com/complianceweek. ■

SAI GLOBAL

Managing Data Security and Privacy Risks 2.0

Modern technology allows robust employee monitoring ability to sharpen business performance, but also spawns a new set of data security risks to keep CCOs busy

by Jaclyn Jaeger

It's a compliance conundrum for the modern age: The proliferation of digital data generated while using employee monitoring technologies—often to ensure that workers stay on the right side of compliance—is creating a whole new set of data security and privacy risks that compliance officers need to worry about.

Companies today can monitor the work-related activities of employees in many ways, from GPS tracking on company-issued vehicles and iPhones to fingerprint or retina scanning for authentication purposes. Do they work? You bet. But using those technologies is forcing companies to strike a careful balance between legitimate business purposes and employees' expectation of privacy and security.

"Employers need to make sure they have a really compelling business reason for requiring employees to use biometrics in the workplace," says Mariam Wugmeister, a partner with law firm Morrison Foerster.

One easy example of legal risk is discrimination claims, such as for disability or religion. If employers want to use monitoring technologies, they should be prepared to respond to any reasonable accommodations employees might request. For example, earlier in March the Equal Employment Opportunity Commission urged a federal judge in West Virginia to grant an injunction to stop coal mining company Consol Energy from forcing its employees to use biometric hand scanning devices, because they could violate anti-discrimination laws under Title VII of the Civil Rights Act. "The likelihood of future violations may be inferred from past unlawful conduct," the EEOC said.

In January 2015, a jury awarded $150,000 in compensatory damages to a former employee of Consol, Beverly Butcher, who argued that he was forced to leave his job after refusing to comply with the company's hand scanning policy for timekeeping purposes. As an evangelical Christian, he believed that submitting a hand scan had a connection to the "Mark of the Beast," as referenced in the Book of Revelations. Consol refused Butcher's request to allow him to track his time through a manual time recording system instead. The EEOC has since filed a motion seeking an additional $413,000 in lost wages.

> "Employers need to make sure they have a really compelling business reason for requiring employees to use biometrics in the workplace."
>
> Mariam Wugmeister, Partner, Morrison Foerster

C.R. Wright, a partner with law firm Fisher & Phillips, says the case serves as a valuable lesson to compliance and risk officers that they must carefully evaluate an employee's reasoning for not using biometric technology. By listening to employees' concerns, and finding other ways to accommodate them, the company may be able to avoid a discrimination claim, he says.

Privacy Risks

A common concern for GPS-tracking devices is privacy risk. The privacy risks posed by GPS tracking, while not a new concept, are especially relevant today in an age of wearable devices, and when an increasing number of companies allow employees to bring their own devices to work—many of which are equipped with GPS tracking capabilities. "Compliance officers have a greater problem with respect to employees bringing this new technology to the workplace," says Tracy Moon, a partner with law firm Fisher & Phillips.

The benefits of GPS tracking are many: companies can confirm that vehicles they own are being used for proper work purposes, or they can track delivery and pickup times to customers more accurately. The risk, however, is that companies also end up collecting data concerning employees' private and personal non-work-related activities (sometimes inadvertently). The risk of privacy-related claims is especially heightened when the company seeks to put such tracking capabilities on a device the employee owns rather than the company—say, installing a tracking app on a worker's own phone.

The policy management challenges to navigate that situation are not easy. First, your policy should notify employees that their whereabouts and activities are being tracked

FINGERPRINTING LAW

New York Labor Law §201-a states, in full:

Fingerprinting of employees prohibited. Except as otherwise provided by law, no person, as a condition of securing employment or of continuing employment, shall be required to be fingerprinted. This provision shall not apply to employees of the state or any municipal subdivisions or departments thereof, or to the employees of legally incorporated hospitals, supported in whole or in part by public funds or private endowment, or to the employees of medical colleges affiliated with such hospitals or to employees of private proprietary hospitals.

Source: New York Labor Standards.

or monitored. "Employees need to be put on notice that the employer is conducting tracking and surveillance, so that they waive potential claims for violations of privacy rights," Tracey Moon says. "An important factor is for employers just to be honest with their employees about what their uses are and what protections are in place."

To develop such a policy, companies must first identify the legitimate business interests they want to protect by collecting that data. "The key is trying to strike a balance between the employee's personal privacy interests versus the company's legitimate reasons or interests and trying to use the least intrusive method possible to achieve the company's goals," says Lilly Moon, a shareholder of law firm Jackson Lewis. One solution, for example, would be to track mobile devices only during business hours.

Most devices with tracking capabilities have a feature that allows users to turn them off. "Often, the company will tell the employee, 'Turn it on when you come to work, turn it off when you leave work'," Tracy Moon says.

"Only collect that information that you really need," Wugmeister says. "If you don't need it, don't collect it."

Security Measures

As with the use of any technology, employee monitoring devices create security risks as well. "Companies need to stay abreast of the latest, greatest security measures to keep the biometric data—just like any other data—from being inappropriately accessed," Wright says.

The same data security and privacy measures companies already put in place for other forms of personally identifiable information (PII) apply to employee tracking data. "Make sure that only the people who really need to have access to the information to do their jobs have access," Wugmeister says. "Make sure whenever you have sensitive data that you can articulate a business rationale as to why each different employee really needs access to that data."

Another important security measure: data destruction. "Get rid of data when you don't need it anymore," Wugmeister says. "Don't just keep everything because maybe someday it might be useful."

In some respects, biometric data is even more invasive and sensitive than other PII. It's also permanent, which makes the loss of such data all the worse if you get hacked. "You can change your password, but you cannot change your iris, or your thumbprint, or other biometric indicators," Wugmeister says. Given how difficult it is to keep basic information like user names and passwords secure, companies need to assess whether the risk of using the biometric data outweighs whatever benefit you expect, she says. ■

EEOC RELIGIOUS DISCRIMINATION COMPLAINT

Below is an excerpt from the EEOC announcement of its suit against Consolidation Coal Company for religious discimination.

Canonsburg, Pa.-based CONSOL Energy and Consolidation Coal Company violated federal law when they forced a long-time employee to retire because they refused to accommodate his religious beliefs, the U.S. Equal Employment Opportunity Commission (EEOC) charged in a lawsuit it announced today.

According to the EEOC's lawsuit, Beverly R. Butcher, Jr. had worked as a general inside laborer at the companies' mine in Mannington, W.V., for over 35 years when the mining companies required employees to use a newly installed biometric hand scanner to track employee time and attendance. Butcher repeatedly told mining officials that submitting to a biometric hand scanner violated his sincerely held religious beliefs as an Evangelical Christian. He also wrote the mining superintendent and human resources manager a letter explaining the relationship between hand-scanning technology and the Mark of the Beast and antichrist discussed in the Book of Revelation of the New Testament and requesting an exemption from the hand scanning based on his religious beliefs.

The mining companies refused to consider alternate means of tracking Butcher's time and attendance, such as allowing him to submit manual time records as he had done previously or reporting to his supervisor, even though the mining company had made similar exceptions to the hand scanning for two employees with missing fingers. The EEOC charges that Butcher was forced to retire because the companies refused to provide an accommodation to his religious beliefs.

Religious discrimination violates Title VII of the Civil Rights Act of 1964. The EEOC filed suit (EEOC v. CONSOL Energy, Inc. and Consolidation Coal Company, Civil Action No. 1:13-cv-00215-IMK) in U.S. District Court for the Northern District of West Virginia after first attempting to reach a pre-litigation settlement through its conciliation process.

"In religious accommodation cases, the standard is not whether company officials agree with or share the employee's religious beliefs," said Philadelphia regional attorney Debra M. Lawrence. "Instead, the focus is on whether the employer can provide an accommodation without incurring an undue hardship."

EEOC District Director Spencer H. Lewis, Jr. added, "In this case, the mining companies not only lost the services of a long-tenured employee, they also violated federal law when they obstinately refused to consider easy alternatives to their new hand-scanning time and attendance system to accommodate Mr. Butcher's religious beliefs."

Source: Equal Employment Opportunity Commission.
*The EEOC enforces federal laws prohibiting employment discrimination. Further information about the agency is available at its website, www.eeoc.gov.

Is Blockchain Technology FinTech's Magic Bullet?

Bitcoin is dead; long live blockchain. Blockchain is poised to become the hottest technology to hit the financial world in years, albeit not without significant business and regulatory challenges

by Joe Mont

Bitcoin is dead; long live blockchain.

To be fair, bitcoin, the much-hyped virtual currency, is hardly ready to fade into oblivion. The technology underlying those online exchanges, however, is poised to, on its own, become the hottest technology to hit the financial world in years, albeit not without significant business and regulatory challenges.

Blockchain technology is basically a peer-to-peer, distributed "open ledger." Rather than a traditional, centralized server or clearing process, blockchain relies upon decentralized, consensus-based authentication protocols. Any item that can be securitized or represented as an item of value can be transferred with an immediate settlement process.

Among those heralding the potential of the technology is J. Christopher Giancarlo, a member of the Commodity Futures Trading Commission. "The 20th century underpinnings of the current 'closed ledger' financial system are inefficient and unstable," he said during a December 2015 speech, describing a process where third parties authenticate financial information in three-day settlement timeframes that "add undue risk, cost, and volatility to the marketplace. The 2008 financial crisis revealed that "a portion of the recordkeeping infrastructure of the multitrillion dollar swaps market was recorded on handwritten tickets faxed nightly to the back offices of market counterparties."

Giancarlo

Distributed open ledgers "have the potential to revolutionize the modern financial ecosystem," Giancarlo said. "Distributed ledgers will have enormous implications for financial markets in payments, banking, securities settlement, title recording, cyber-security, and the process of collateral management that is made infinitely more complex by new regulations." His bold prediction: new "smart" securities and derivatives that can value themselves in real time, automatically calculate and perform margin payments, and even terminate themselves in the event of a counterparty default.

Giancarlo is not alone in his enthusiasm. The Bank of England has called blockchain the "first attempt at an 'internet of finance.' " More than 40 global banks formed a consortium, R3CEN, to develop a framework for its use. The Securities and Exchange Commission recently approved Overstock.com's registration statement to sell securities using blockchain technology. JPMorgan Chase is experimenting with blockchain transactions for international monetary transfers. D+H, a leading provider of technology solutions to financial institutions globally, has successfully integrated blockchain-distributed ledger technology into its global payments services hub and is in active discussions with banks to implement it.

Late last year, NASDAQ announced that an issuer was able to use its in-house blockchain ledger technology to, for the first time, successfully complete a private securities transaction. It has also worked with the Republic of Estonia to facilitate a blockchain-based e-voting service for companies listed on that country's Tallinn Stock Exchange.

Quinlivan

"Banks aren't necessarily known for being early adopters of new technologies. There is a lot of risk involved in switching over a system," says Stephen Quinlivan, a partner with the law firm Stinson Leonard Street. Nevertheless, in a world of increasing regulation, cross-border transactions, and demands for a faster, more secure settlement process for payments and stock transfers alike, blockchain has intriguing potential for them. "You can use it for anything you can transfer title to," he says. "You can use it for a car; you can use it for real estate. People talk about using it for artwork and music royalties."

Blockchain could enable business models that were not previously available, according to Angus Champion de Crespigny, a financial services consultant for EY. As blockchain decouples from virtual currency, the million-dollar-question is what else it can do, do well, and do safely. The real strength of the technology is establishing trust in an untrustworthy environment. "We see huge opportunities in the ability of this technology for integrating finance directly into devices and essentially getting to the point where if you can digitize it, you can securitize it." Champion de Crespigny says. "Think about financing cars directly rather than financing the people who buy these cars. Think about digital rights for music and films and being able to securitize and sell those off, being able to fund intellectual property directly, and funding decentralized energy markets."

> "We see huge opportunities in the ability of this technology for integrating finance directly into devices and essentially getting to the point where if you can digitize it, you can securitize it."
>
> Stephen Quinlivan, Partner, Stinson Leonard Street

There are, however, unprecedented regulatory implications, Champion de Crespigny warns. How do you file a Suspicious Activity Report on a car? "The regulators will regulate, and should regulate, products," he says. "But what blockchain is, at the moment, is a technology; and for them to develop a regulatory framework around it is the same as expecting them to regulate around relational databases. It is difficult to say the least."

The technology must get certain things right in order to deliver on its transformative promise, says Moti Porath, executive vice president, global pre-sales, for D+H. "One of the things with bitcoin was anonymity, and we know in the banking world anonymity is not a very good trait. You can maintain privacy, but not anonymity," he says.

The challenge is achieving regulatory compliance, without necessarily direct regulatory oversight. "You can do Know Your Customer and sanctions screens. You can do liquidity limits monitoring," he says. "You can restrict the types of operations that you allow an entity to do. Once you add a layer of regulatory compliance without strict direct oversight, you have the best of both worlds."

Blockchain has entered the "Wall Street phase," where banks and other financial institutions form consortiums and partnerships to explore its possibilities and upsides," says Robert Henry a director for business change and technology consultant GFT's North American finance business consulting practice. "They cannot sit on the sidelines, but I would never say they are not cautious."

Henry describes some of the unique applications blockchain could enable, including the shareholder voting process. "The proxy voting process is pretty archaic," he says. "You get this big package in the mail, and you have to go through reams of paper before you can actually cast a vote. This information should be shared instantaneously and the blockchain, the distributed ledger, will allow you to do that." Blockchain can also mean instantaneous vote tallies. Financial statements could similarly benefit from a distributed, shared ledger.

Regulators, Henry hopes, will tread into this new arena carefully. "The regulators should embrace the potential opportunities and utilize the rules they currently have in place for banking and financial services, but adjust, revise, or create new rules to mitigate the risks of this new technology," he says. "This is an opportunity where the regulators will not have to be reactive because they see it as an emerging technology and can instead partner with businesses. You don't want to put a heavy hand on it and stifle innovation."

"You have to look at the natural next steps," says Alan Morley, GFT's compliance and AML practice lead for North America. "What products or businesses are a natural first step? Who is going to be the first mover and what do they expect to get out of it? That is when the regulators will really start to take notice. As soon as it moves out of its niche play of the moment, where it is still very much in an incubator, that's when the attention will be exponential and accelerate. We are not there yet. This is going to take time, but that doesn't mean it is not going to happen, nor does it mean that when it does happen adoption is going to continue being slow. Each step will accelerate the curve." ■

VIEW FROM THE CFTC

The following comments on blockchain technology were made by Commissioner J. Christopher Giancarlo of the Commodity Futures Trading Commission during remarks at Harvard Law School on Dec. 1, 2015.

The 20th century underpinnings of the current "closed ledger" financial system are inefficient and unstable. At present, centralized third parties authenticate financial information in generally three-day settlement timeframes that add undue risk, cost, and volatility to the marketplace.

The 2008 financial crisis revealed that a portion of the recordkeeping infrastructure of the multitrillion dollar swaps market was recorded on handwritten tickets faxed nightly to the back offices of market counterparties.

Distributed open ledgers have the potential to revolutionize modern financial ecosystems. Unlike current settlement processes, distributed ledgers use open, decentralized, consensus-based authentication protocols. They allow people "who have no particular confidence in each other [to] collaborate without having to go through a neutral central authority."

Distributed ledgers will have enormous implications for financial markets in payments, banking, securities settlement, title recording, cyber-security and the process of collateral management that is made infinitely more complex by new regulations. Open ledgers may make possible new "smart" securities and derivatives that can value themselves in real time, automatically calculate and perform margin payments and even terminate themselves in the event of a counterparty default.

Enormous resources are being invested in developing the distributed open ledger known as the blockchain. Over two dozen major global banks have joined together in a consortium to build a framework for using blockchain technology in markets. The London Stock Exchange, CME Group, Euroclear, Societe Generale, and UBS have set up the Post Trade Distributed Ledger Working Group to look into how blockchain technology can be used in clearing, settlement, and reporting of trades.

The Bank of England has called the blockchain the "first attempt at an 'Internet of finance'" with the potential to decentralize legal recordkeeping the same way the Internet decentralized data and information. This transformation will not come without consequences, however, including a greatly disruptive impact on the human capital that supports the recordkeeping of contemporary financial markets.

On the other hand, the blockchain will help reduce some of the enormous cost of the increased financial system infrastructure required by new laws and regulations, including Dodd-Frank.

Source: Commodity Futures Trading Commission.

CAN YOU IDENTIFY THE BIGGEST RISK IN THIS PICTURE?

AS DIGITAL MEDIA CONTINUES TO CHANGE, employees have more power than ever before in the palm of their hand. Is your compliance and ethics program ready for the evolution of risk?

Get the answers — www.saiglobal.com/complianceweek

SAI GLOBAL