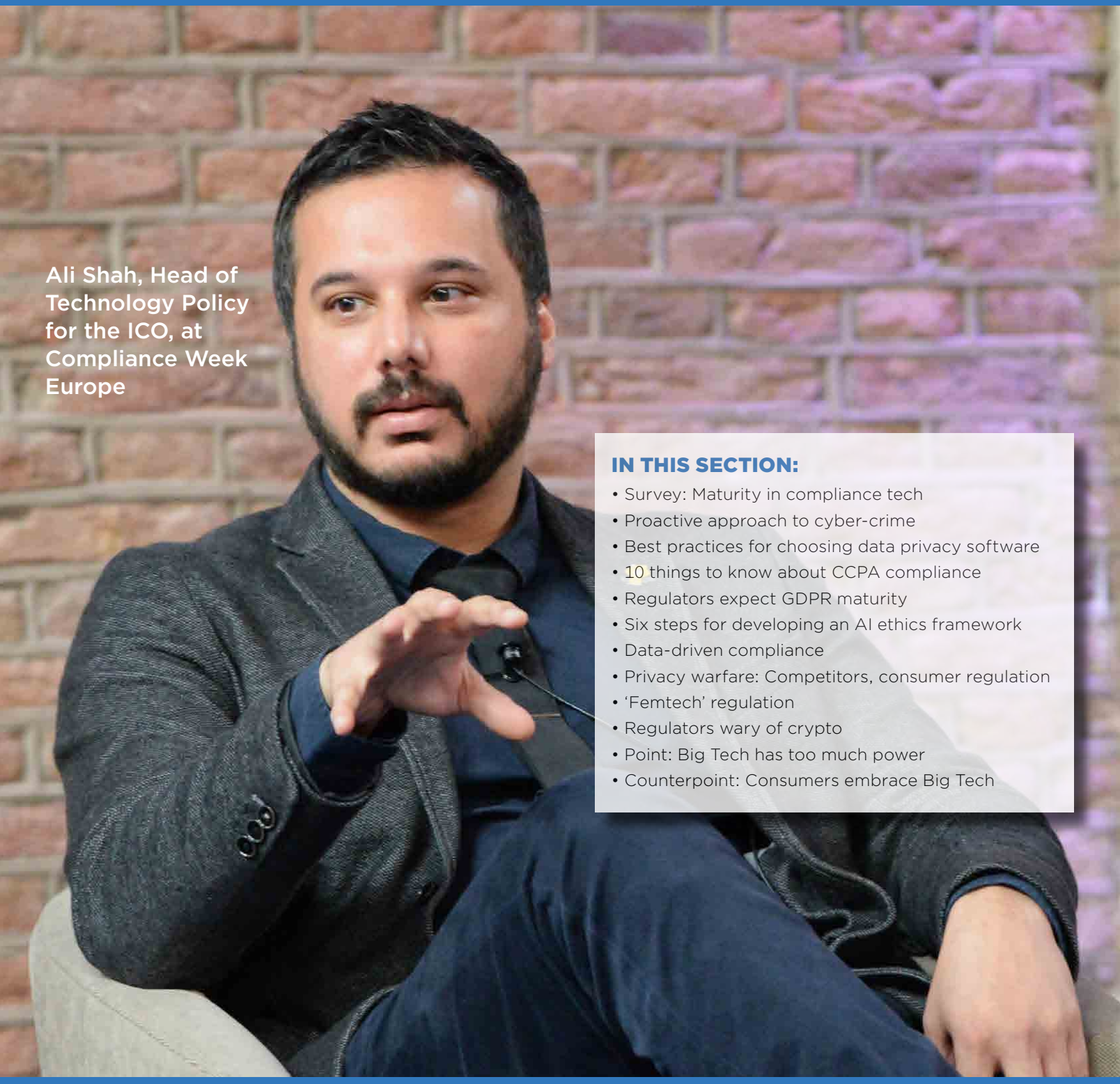
Brought to you by the publishers of COMPLIANCE WEEK

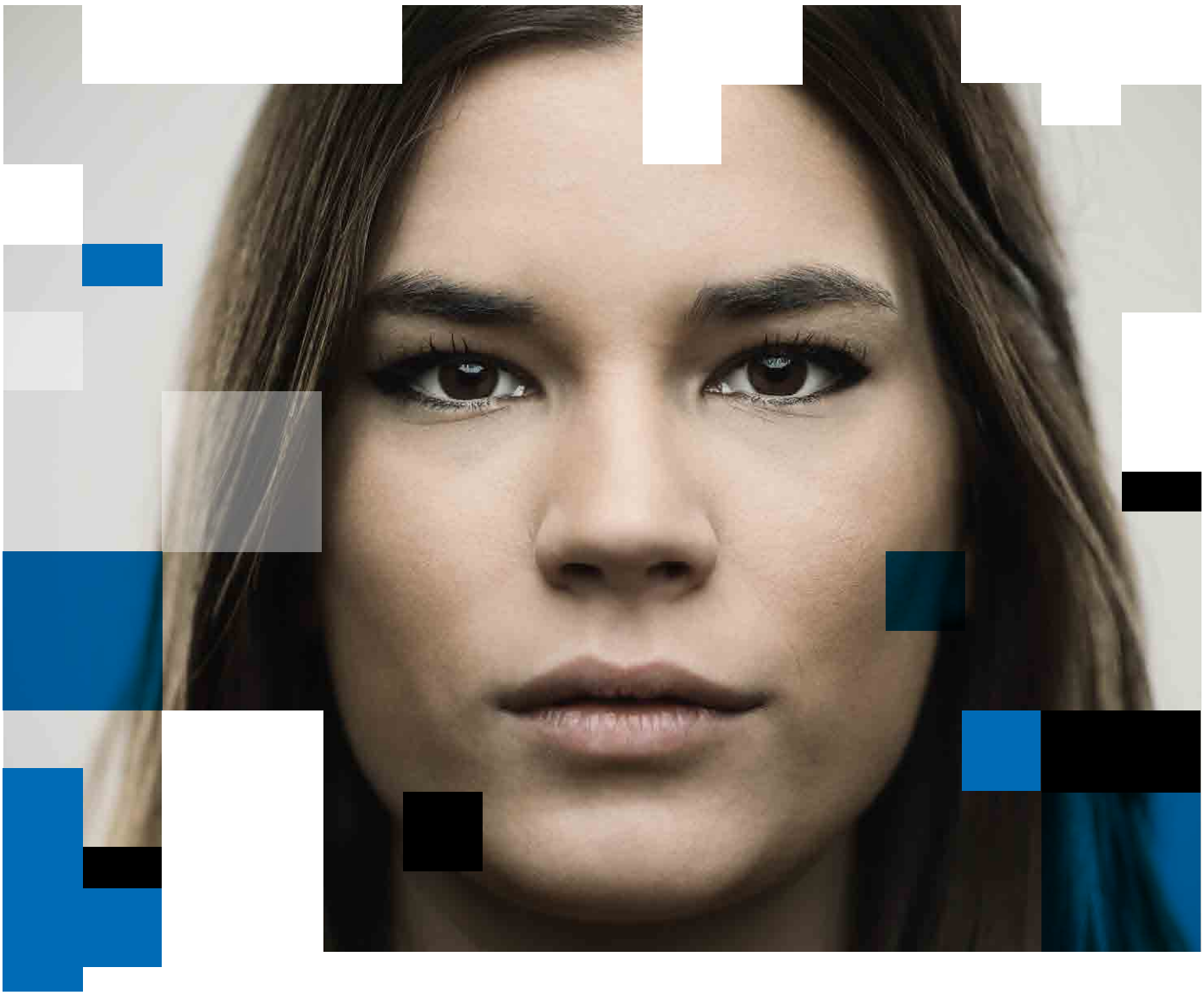


Ali Shah, Head of Technology Policy for the ICO, at Compliance Week Europe

IN THIS SECTION:

SPECIAL REPORT:

Maturing in your technology journey



REFINITIV QUAL-ID
POWERED BY TRULIOO

HOW DO YOU KNOW YOUR CUSTOMER IF YOU DON'T KNOW YOUR CUSTOMER?

A powerful combination of digital identity verification, document proofing and risk screening all via API technology

- Secure digital identity verification and screening
- Seamless delivery via API
- Delivers a frictionless customer experience
- Reduces customer abandonment rates
- Decreases fraud and enhances compliance

refinitiv.com/qual-id

REFINITIV™
DATA IS JUST THE BEGINNING™

Maturing in your technology journey

Our second annual special report on compliance and technology addresses the challenges and opportunities posed by the continuing evolution of the compliance function and the advanced tools that both power it and make it infinitely more complex.

Technology is creating efficiencies, automating formerly manual processes, and allowing practitioners to better demonstrate the bottom-line value of a robust compliance program. But it's also introducing new ethical dilemmas, creating vulnerabilities around the collection and storage of data, and muddying the regulatory waters.

This special report aims to help you figure out where you fall along the compliance technology maturity curve and to introduce new tools available to help protect your data and ensure you're using it in accordance with new standards in place in both the European Union and (soon) California. It also explores the Pandora's Box of questions and ethical conundrums presented by advanced technologies like machine learning and cryptocurrencies that both businesses and regulators are trying to wrap their arms around.

exterro®

The **ONLY** Legal Governance, Risk and Compliance (GRC) Software Platform designed for Corporate Counsel

PRIVACY

- Complete DSAR solution (including collection, review, redaction)
- Data Inventory
- Data Minimization/ Defensible Disposition
- 3rd Party Risk Profiling

E-DISCOVERY

- Legal Hold
- Collection, Processing, Review, Production
- Legal Project Management
- Identification/File Analysis

LEARN MORE AT
EXTERRO.COM

Survey: Growing evidence of maturity in compliance tech

Data from CW's second annual survey shows logical progression along the technology curve. **Aly McDevitt** reports.

Results of Compliance Week's second annual technology survey suggest that companies are moving along the technological maturity curve in ways that are both quantitative (bigger budgets) and qualitative (more interested in practical applications than conceptual) compared to last year.

A smaller percentage of respondents to CW's "How are you choosing and using new GRC technology?" survey—conducted in partnership with Refinitiv—indicated they were shopping around for new tools, and a larger segment was in the process of implementing those tools compared to the results of the 2018 survey.

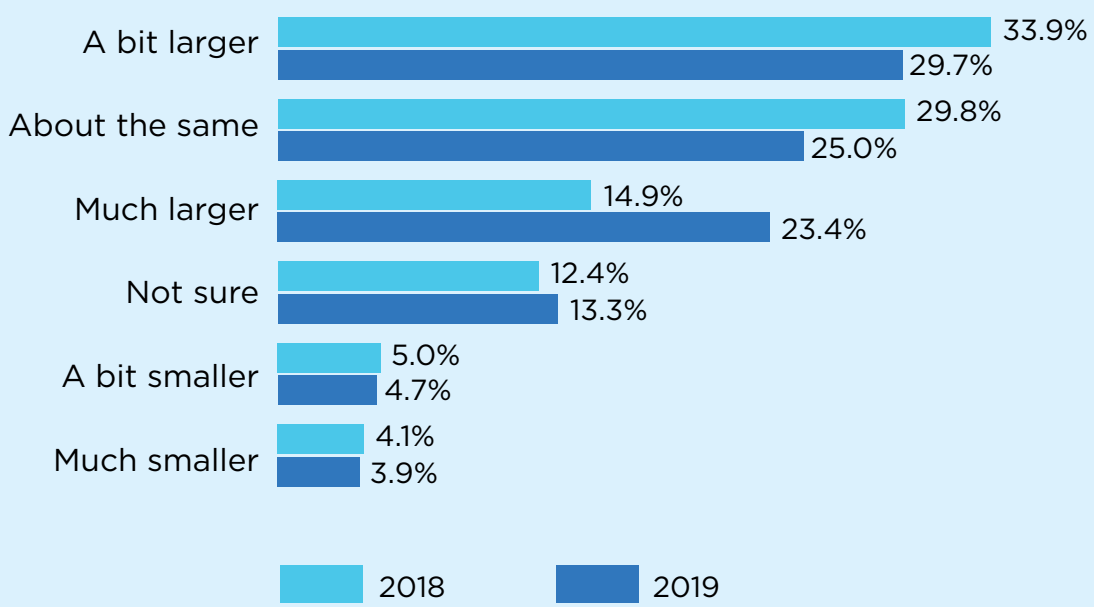
Specifically, 46 percent of 128 compliance practitioners polled who play a role in their organization's technology decisions said they're currently choosing a new or upgraded product, a 4 percent decrease over last year, and 21 percent said they were implementing technology that had been greenlighted, a 3 percent year-over-year increase.

"The pace at which technology is changing has almost forced [companies] to move through that maturity curve," said Holly Sais Phillippi, Rifinitiv's head of risk market development for the Americas. "Companies are starting to see their peers moving quickly and adopting technology faster."

While these year-over-year statistical changes seem small in isolation, other survey results echo the theme that compliance functions are maturing technologically. A year ago, nearly a third of polled practitioners (31 percent) said their organizations were "late to the party" in terms of technology investments. That proportion dwindled to 22 percent in 2019.

This finding may be partially explained by the fact that companies are able to evaluate and make decisions about in-

How does your technology budget compare to what it was 3 years ago?



vesting in new technologies faster and more efficiently than they were previously.

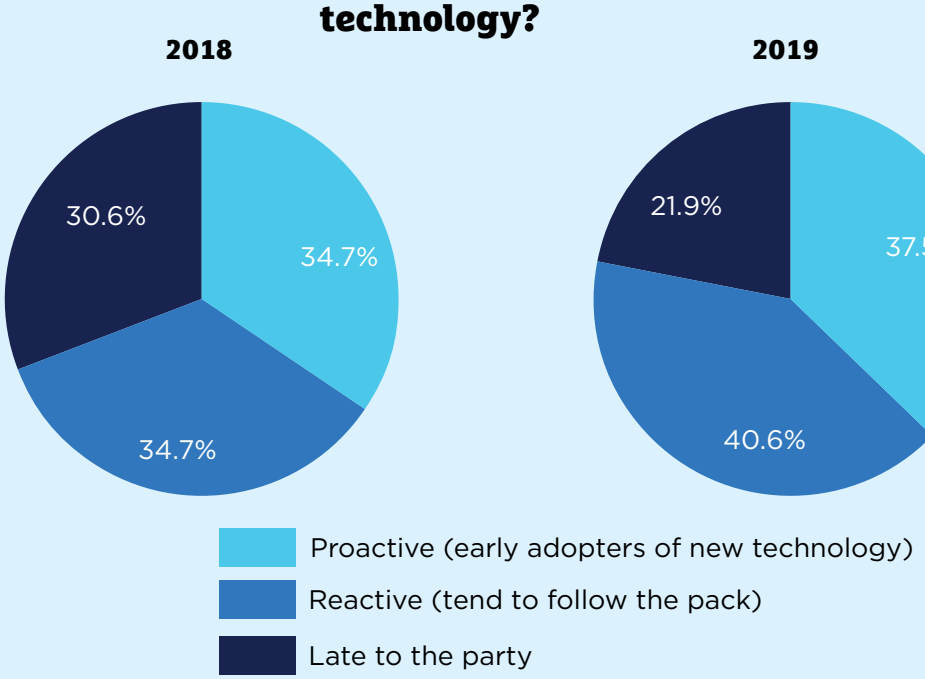
"In the past, companies were seeing big, heavy-lift systems that required many months—sometimes years—to get adopted and configured; if you were going to go through an evaluation period, it would take quite a bit of time. You'd have to do some testing, go through a proof of concept, and look at project plans that could take 24 months," Phillippi said. "Now, companies can take four different technology providers and evaluate them at the same time and at a fairly significant pace."

And it's not that proponents of compliance technology are just paying lip service—they are also putting their organization's money to work. Companies are willing to spend more in 2019 than they were even a few years ago to build a more robust technology-enabled compliance function, according to survey results. Nearly a quarter (23 percent) of compliance practitioners said their technology budget is much larger today than it was three years ago, an increase of 8 percent over last year's survey. While this budgetary shift may not be seismic, it is corroborated by corresponding declines in other responses to the same question. For instance, 5 percent fewer respondents to this year's survey said their technology budgets are about the same as they were three years ago (25 percent in 2019 versus 30 percent in 2018); in addition, 4 percent fewer respondents said their budgets were only a bit larger (30 percent in 2019 versus 34 percent in 2018).

Quantifiable metrics like bigger budget size is tangible evidence the winds of change are blowing. But there are also subtler indicators of change, derived from respondents' answers to other, more subjective questions. One survey question asked compliance practitioners, for instance, "When making a case for investing in technology, what's the most effective argument?" The more popular answers of 2018 were conceptual or general in nature: Process efficiency (31 percent) and compliance with a regulatory requirement (21 percent). In 2019, practitioners' responses to the same question showed more of an applied reasoning than theoretical: Improved results and better data/analytics rose 5 percent and 6 percent respectively, year over year, while process efficiency dropped 6 percentage points and compliance with a regulatory requirement declined 11 percent. While cost/staff savings was a common answer choice both years, its popularity increased by 5 percentage points in 2019. This growth could be an indicator that companies' cost-benefit analyses for making a technology investment are panning out favorably.

"Absolutely yes," Phillippi agrees. "The fact that you can see an immediate ROI by investing in these technologies and have an immediate reduction in cost internally is a big driver.

How would you describe your organization's approach to compliance technology?



I only see that trend continuing to rise."

Indeed, a year ago, demonstrating return on investment rated 4 percentage points higher in 2018 (31 percent) than it did in the 2019 survey as an answer to a question about the most difficult thing about implementing a new software solution. This year, challenges with the implementation process was the top answer to that question (37 percent), rising 11 percentage points year over year.

This year's greater emphasis placed on implementation suggests more organizations are already putting a technology investment into effect. Instead of combing through issues that arise during the planning process, they are grappling with those that emerge during the execution phase.

"A lot of organizations struggle because they have been on certain systems for a long period of time. There's a lot of compliance risk to moving systems because companies have to make sure they're not going to miss anything from an audit perspective. So, it's not that [new technologies pose] a harder implementation—it's just taking a little more time to get a level of comfort that the changes being made are not missing anything," Phillippi explained.

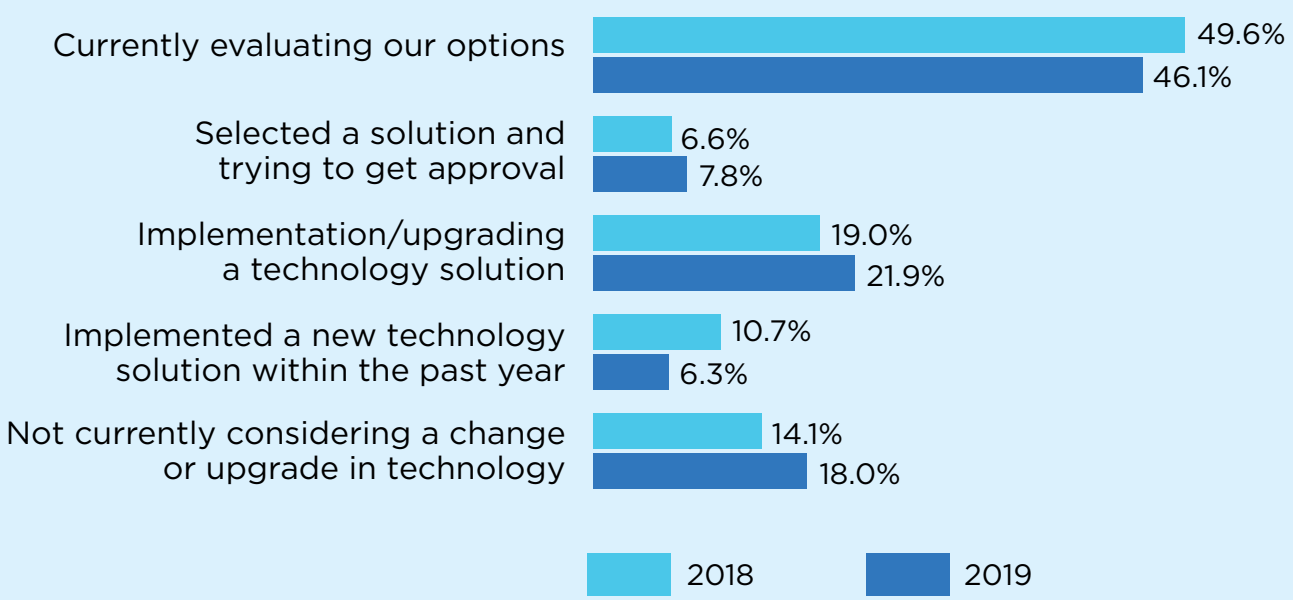
Advanced technologies like artificial intelligence (AI) also got more attention in the 2019 survey, not only in reported usage but also in confidence. Thirty percent of practitioners polled said they are evaluating AI at their organizations, up 3 percent from 2018. More convincingly, 17 percent of respondents said their companies are currently using AI-powered tools, a 7-point gain, year over year.

"Everybody is interested in AI," Phillippi said. "There's no question AI is going to have significant impact within the compliance space. … It will, however, take some time for full AI solutions to be implemented. Companies that are currently able to say 'yes, I use AI,' can do so not because they've incorporated AI into all of their programs or directly into their own systems, but because they've adopted a piece of technology that has an AI component."

Indisputably, there is still some resistance to the sea change. Forty-two percent of 2019 respondents remain resistant to cutting-edge technologies like AI, with 20 percent saying they are unsure about harnessing AI and another 22 percent stating they have no plans to implement it. By comparison exactly half of last year's respondents expressed unease or opposition to AI, an overall 8 percentage-point decline in skeptics year over year.

"I think you're seeing people back off because there has been a reset of what AI is exactly. What is the definition of AI within the compliance world? How do you start to train it? How do you gain a level of comfort [with the prospect of removing] that visual human touch associated with the things

Where is your company at in the process of adding or upgrading compliance technology?

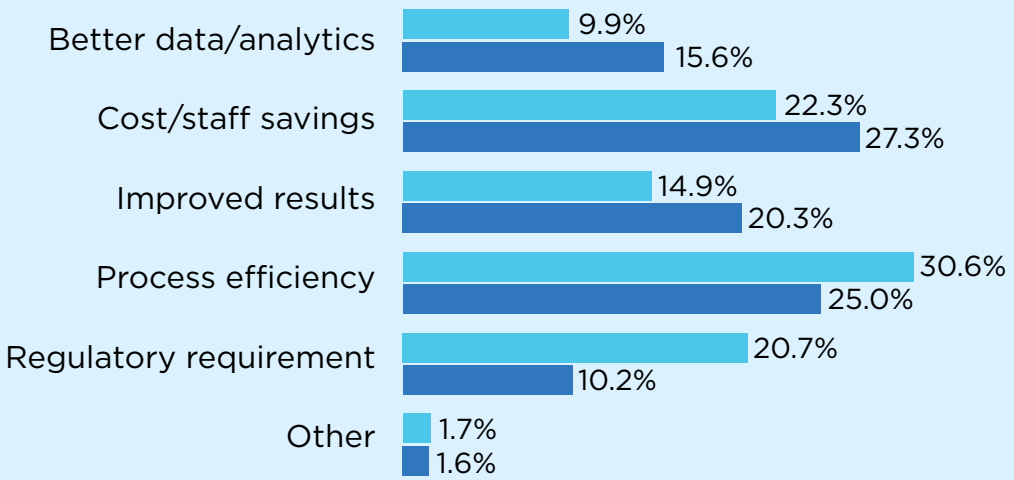


AI is being incorporated for, and how do you get the regulatory bodies comfortable with the AI output?" Phillippi asked.

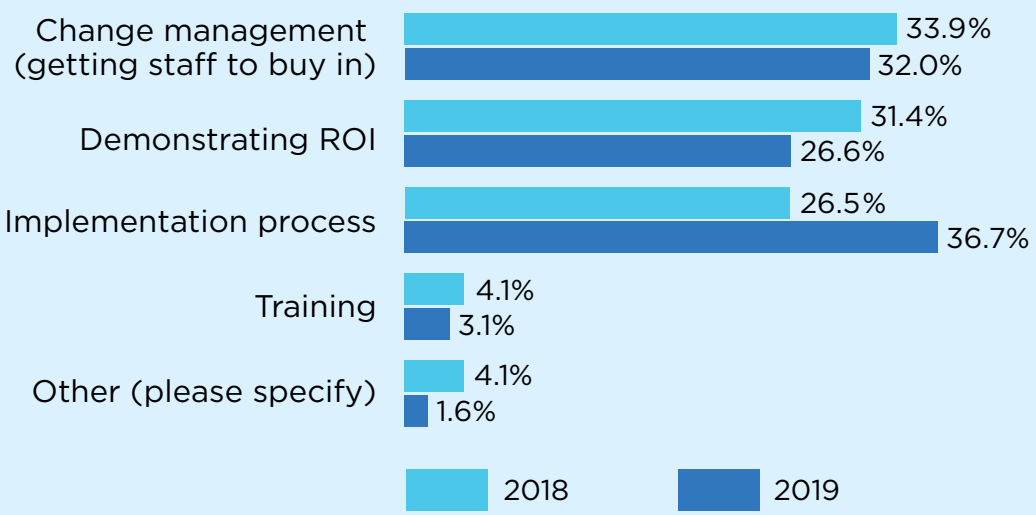
So, what is the current application of AI within the compliance world?

"From a compliance outlook, AI can help identify some of that low-risk work that an analyst does and take it off of their plates … I don't think anyone is worried about AI taking over their jobs; the value is providing analysts the opportunity to focus on the higher-value items versus false positive volumes, as an example," Phillippi said. ■

When making a case for investing in technology, what's the most effective argument?



What's the most difficult thing about implementing a new software solution?



MEANINGFUL COMPLIANCE INSIGHTS TODAY, TOMORROW & NEXT YEAR

Onspring gives you a big-picture view of your control environment and the fine detail you need to manage performance and efficiency. With Onspring's no-code, cloud-based compliance software, you can capture your control library, map to regulations, perform design and operating tests, and manage issues. Discover more at onspring.com.

Your Process.
Our Platform.
A PERFECT MATCH.

Onspring

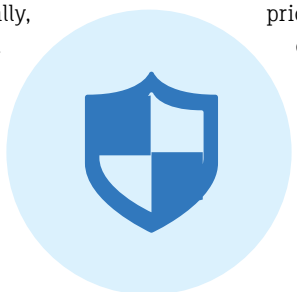
Proactive approach needed in today's cyber-crime environment

An expert sheds light on behavioral science-driven solutions that help businesses prepare for a breach before it happens. **Aly McDevitt** has more.

Over a third of 128 compliance practitioners who participated in the "How are you choosing and using compliance technology?" survey indicated they are considering upgrading or implementing a cyber-security solution, more than any other type of compliance-related software.

Companies are right to be on high alert, says Jamie Miller, president and CEO of cyber-security solutions company Mission Multiplier. "The appetite or the allure to get information is only growing, and the ability for those adversaries to actually penetrate your networks is becoming easier and easier through advanced technologies," Miller said.

The first half of 2019 witnessed more than 3,800 publicly disclosed breaches exposing 4.1 billion records globally, according to a research report by Risk Based Security. The number of reported breaches increased by 54 percent compared to the first half of 2018, and the number of exposed records went up 52 percent, indicating breaches are continuing at a "breakneck pace," the report states.



CYBER-SECURITY

"I can guarantee somebody has been somewhere on your network they shouldn't have been," Miller warned. "It's a matter of figuring out how to protect that key information you have and make sure it doesn't get in the wrong hands."

Firms should get a third-party risk assessment done at least annually or even every quarter, depending on the industry. This will help them gain a better appreciation for what their existing security function is doing now, what it needs to be doing, and how to align it with industry-specific best practices.

A third-party risk assessment would entail "a governance aspect, where [the assessor] would review a company's existing set of policies against whatever the compliance drivers are for their industry relevant to cyber-security," Miller said. "In addition, there would be a technical review of the company's architecture to assess security controls from a technical perspective."

A technical review normally includes some type of penetration test. In the end though, a company's weakest link is its people. "It's not because they're uneducated, incapable, or using the wrong tools. It actually is because we're all irrational actors," Miller explains. Consequently, phishing attacks are currently the biggest issue facing organizations around the globe.

Supply-chain breaches are also massive, as hackers zone in on the paths of least resistance. "They look for pivot points—the supply-chain companies that are working with those organizations—because those [supply-chain partners] are smaller organizations. They're probably less well-funded, and they probably don't have security controls as mature as the bigger, target organizations," Miller said.

Technological cyber-solutions intended to drive behavior change through the nexus of data analytics and behavioral science are available now. Miller's firm is rolling out a solution called MARS Suite that aggregates disparate data from a company's tools and technologies and uses a custom algorithm to prioritize and present that dataset in a risk economy. The economy scores people in different component groups, creating transparency around employees' risk management profiles.

"It's a dynamic system where you're incentivizing the right behavior with risk scoring and prioritization of the data through data analytics," Miller said. "Now, [employees] are not beholden to their irrational behavior." Thus, the cyber-security game is changing as the focus shifts more heavily onto the individual and their decision making. Training employees remains a critical component of a security program too.

Taking a purely defensive stance on cyber-security isn't going to cut it anymore, explains Miller. "The enormity … and dynamic nature of threats is going to be the issue," he said. "The solution will be leveraging AI to take that volume and all those different patterns to come up with a way to predict what's coming and protect ourselves instead of just react."

Miller also has advice on what to do when you realize you've been hacked … or that a breach is in progress. "Call somebody in that will take that terminal to an offline environment, a sandbox environment," he said. "They will go on your network and see if there's any activity or indicators for what happened."

And don't touch any files: "If you start closing and deleting stuff, the ability for [solution providers] to go back in and do forensic analysis around what happened, who came in, and what they did becomes more and more difficult," Miller said. "Leave it as is, and make the call immediately." ■

Cyber-security glossary

For those unfamiliar with the vernacular involved with cyber-security and the methods by which bad actors attempt to access restricted data, we present this glossary of common terms:

Backdoor: A malware type that allows unauthorized users to discreetly bypass normal authentication procedures to gain access to a computer system. By design, the perpetrator can issue system commands, steal personal and financial data, and update malware, all remotely.

Cloud-data leakage: A breach that occurs when an employee deliberately or inadvertently uploads sensitive company information to cloud services; data leaks can occur through hacks via connections on unsecured networks, through human error, or both.

Emotet: A banking Trojan malware strain that steals financial information by injecting computer code into the networking stack of an infected host computer, allowing sensitive data to be stolen via transmission. Emotet is typically distributed as a URL within the body of an email or as a PDF attachment.

Malware: A portmanteau of "malicious software," it is any piece of software designed to intentionally damage or disable devices, steal data, and/or cause disruption on computer systems, networks, tablets and mobile devices, often by remotely usurping control of the device's operations.

Mobile malware: Malicious software that specifically targets the operating system on mobile devices, allowing hackers to steal data on the device.

Phishing: A cyber-attack that uses social engineering to steal user data. It occurs when an attacker, impersonating a trusted entity or individual, deceives a victim into opening an email, instant message, or text message and often induces the victim to reveal personal information.

Ransomware: A strain of malware that, once loaded onto a computer system, blocks access to it and/or threatens to publish a victim's data in perpetuity until a ransom is paid.

Skimming: the theft of payment card data through the use of malware, which is injected onto the payment page of an e-commerce website to steal payment information. Skimming also occurs directly from compromised payment card machines.

Spyware: Malware that enables an attacker to gather private information and assert control over a device without the consumer or entity's knowledge or consent.

SQL injection: An attack method that executes malicious code on a database server, allowing a hacker to bypass normal security measures in order to steal, modify or delete data stored there.

Supply-chain hack: An attack that targets less-secure elements in a supply network with the goal of damaging or stealing data from the larger organization.

Targeted attack: A class of malware that uses a variety of hacking methods to methodically attack a predetermined user or organization to capture sensitive information.

Trojan: A type of malware that looks legitimate but is designed to take control of your computer. It seeks to dupe the victim into loading and executing the malware on a device. Once installed, it can steal data and damage or disable the network.

Virus: A type of malware that replicates itself and becomes part of another program, allowing it to propagate and spread infection. Unlike a worm, a virus requires a user to execute it, as it is not active or able to be spread until a user opens a malicious host file or program.

Worm: A type of stand-alone malware that replicates itself and becomes part of another program, allowing it to propagate and spread infection. Unlike a virus, a worm does not require a host program or human to execute it.

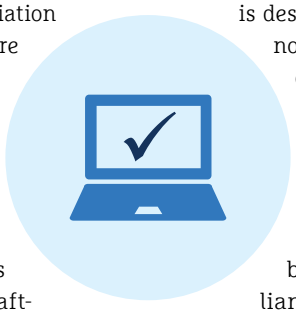
Zero-day attack: An attack that targets software vulnerabilities, or security holes, in a program or operating system, which a software vendor may or may not be aware of, and which has yet to be patched.

Best practices for choosing the right data privacy software

Don't expect a plug-and-play technology solution to this complex new problem. **Lori Tripoli** reports.

Burgeoning regulatory requirements protecting personal information and increased consumer interest in privacy rights have fostered a growth industry over the past few years. The number of privacy technology companies leaped from 51 vendors just two years ago to 224 in 2019, according to a report issued by the International Association of Privacy Professionals. Apparently, these vendors are very much responding to a market need. Almost 33 percent of respondents to Compliance Week's second annual technology survey, sponsored by Refinitiv, reported they are considering upgrading or implementing technology solutions around data privacy.

Finding all of an individual's personal data can be a daunting challenge for companies, a fact that is perhaps surprising in an age when even a poorly crafted search term on Google can pull up all sorts of pertinent information instantaneously. The fact is, though, that large enterprises don't necessarily have robust search power in their internal systems.



SOFTWARE

> "One of the most important aspects of any data protection program is having an in-depth and documented knowledge of the what, the why, the where, the who, and the how."
>
> Aoife Harney, Senior Regulatory Consultant, Fenergo

Privacy software "can help to answer one of the most challenging questions: Where is the data?," says Safi Raza, director of cyber-security at Fusion Risk Management. In addition to locating data that falls under various privacy regulations, software can alert data administrators if unauthorized access or transfer is detected, Raza explains. Technology can also help with privacy assessment and data pseudonymization. There is one caveat, though: "There isn't one solution" that offers all of these characteristics, Raza says. That's a caution that a number of experts in the field mention. "Privacy technology is designed to make your privacy program more efficient, not replace it entirely," notes Nicholas Merker, co-chair of the data security and privacy practice at the law firm Ice Miller.

Why is personal data so hard to find in the first place?

"When data flows into a large business, it could be used for any number of purposes," explains Cilian Kieran, CEO of privacy software company Ethyca. That data might be used for marketing, for business intelligence, for product development, or for all sorts of other reasons. "Data is flowing throughout an organization in a myriad of ways the business doesn't often fully see," Kieran says.

To some degree, the current demand for privacy technology solutions may reflect the fact that laws requiring protection of data were passed just a bit before the regulated community had the know-how to comply with these new requirements.

Different software, of course, does different things. Some just focuses on incident response to privacy, explains Michael Rasmussen, a pundit on governance, risk management, and compliance technology and founder/principal analyst for the research firm GRC 20/20 Research. Other software focuses on management of cookies, notices, and disclosures, he continues. Still other software provides a broader privacy platform, while some enterprise governance, risk, and compliance platforms "have modules that people leverage and use for privacy," Rasmussen explains. Yes, it's complicated.

Three types of privacy software

Generally, there are three categories of privacy software tech-

"When data flows into a large business, it could be used for any number of purposes. Data is flowing throughout an organization in a myriad of ways the business doesn't often fully see."

Cillian Kieran, CEO, Ethyca

nology that serve varied functions, Kieran explains. The first involves more traditional program and workflow management tools. These products ostensibly are "privacy technology systems," he says, "but their real function is to provide readiness assessments and workflow management frameworks, the kind of things that allow you to understand the current status of the organization and then provide you with workflows that various stakeholders and businesses can go through to achieve compliance."

The second is "data discovery systems," Kieran says. These products "make the identification of where personal information is in the organization faster" than a manual process involving various stakeholders in a firm. These speed up the process but are not foolproof. Some manual review is still necessary because data discovery systems "rely on machine learning and machine learning is an imperfect science," Kieran maintains.

The third category focuses on "obligation management," like data subject requests, Kieran says. "Retrieving and managing subject data requests is pretty labor intensive, so these systems effectively aggregate the process of ingesting the subject's request, and then returning that data," he explains.

Data privacy compliance isn't easy given different jurisdictional definitions of personal data and varied requirements depending on how sensitive certain data happens to be (if, for instance, it involves a medical condition). "Legacy compliance solutions" are not "well equipped to deal with this new generation of compliance issues which are a function of how very complex systems handle data," Kieran says.

What to look for

In contemplating privacy technology, look for "a solution that is highly engaging and intuitive to use," Rasmussen suggests. It should, of course, also "cover the spectrum" of what an organization needs, he notes. As a practical matter, the first step of compliance where the EU's General Data Protection Regulation or the soon-to-be-enacted California Consumer Privacy Act happen to apply "is to be able to document your data flows," Rasmussen explains, referring to how European Union citizens' or California citizens' data comes into an organization, flows through it, and (possibly) is disposed.

"A lot of the older technology solutions have you diagram those data flows," Rasmussen acknowledges. Newer privacy technology "has business process modeling type capabilities built in," he notes. That means a company "can document those data flows and manage them and even turn them into dashboards" that show risk issues and how privacy is built into the system, Rasmussen says.

"One of the most important aspects of any data protection program is having an in-depth and documented knowledge of the what, the why, the where, the who, and the how," says Aoife Harney, a senior regulatory consultant at Fenergo.

In sum, an organization should know what data is collected, why it is required, where it is stored, who has access to it, and how it is collected and secured. "Being able to clearly see when a client's personal data was collected, what legal basis is relied upon for that activity, who accesses that information, and when it's appropriate to erase is incredibly useful to any organization," Harney says.

"Don't expect a 'plug-and-play' compliance solution," cautions Conor Hogan, a senior manager of information governance at BSI Cybersecurity and Information Resilience. When choosing a privacy technology software vendor, consider whether the solution addresses the actual compliance challenge that you happen to have, he suggests. If it does, "consider licensing costs (one off, per user, per annum, etc.), scalability, and transferability for the global landscape of evolving privacy legislation," Hogan says.

Should you go with a startup?

Some organizations that need help in this area might be reticent to sign with a startup privacy technology vendor for fear it may not exist in five years. But a startup may be achieving success because it has figured out how to do something well that more established operations haven't. "Startups will usually have identified a reason to be a startup" such as a niche in the market or a problem that only they can fix, explains Hogan.

Going with a more established company "means you might have to make process changes or be forced to accept a rigid mechanism to achieve something," Hogan says. Startups, on the other hand, "will likely offer more flexibility and customization and would usually be more open to suggestions from their early adopters." ■

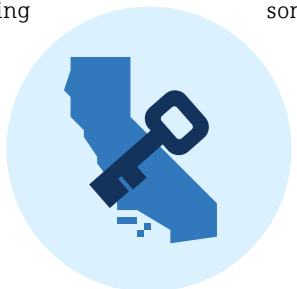
10 things you need to know about CCPA compliance

It's go-time for compliance as the clock ticks toward the Jan. 1 effective date of the California Consumer Privacy Act. **Lori Tripoli** explores.

Companies that have customers in the Golden State need to start prepping to comply with the California Consumer Privacy Act (CCPA).

To some degree, California's statute "represents a shift in perspective" for data, observes Heather Buchta, a partner at the law firm Quarles & Brady. Courtesy of California's state legislature, we as a society are evolving from looking at data as a company asset and moving toward "a consumer rights mentality," Buchta says. Still, businesses cannot afford to dither about compliance.

What follows are 10 pieces of expert advice compliance practitioners should heed if their companies are going to be in compliance with the CCPA:



REGULATION

1 Determine whether you are subject to the law

Not every organization is subject to the CCPA. The law applies to businesses that have gross annual revenues greater than $25 million; those that buy, receive, or sell the personal information of 50,000 or more consumers, households, or devices; or businesses that derive 50 percent or more of their annual revenue from selling consumers' personal information. For-profit enterprises do not necessarily have to be based in California to be subject to the statute.

2 Don't just hand off CCPA compliance to the IT team

"There are IT aspects to compliance with the CCPA," says Jason Schwent, data privacy specialist at the law firm Lathrop Gage. While data tracking information, deletion, and security do tend to be tech-oriented tasks, adherence to the CCPA "is a legal compliance issue," he maintains.

Businesses should put together a team "comprising legal, compliance, business, and technology expertise," suggests Richard Harris, chair of the technology, telecommunications, and outsourcing practice at the law firm Day Pitney. The team can "assess the compliance strategy to address the implications of the CCPA on their business and an impending onslaught of similar legislation expected in 2020," Harris says.

3 Set up a schedule

Behavior modification will not happen overnight. "Agreeing upon a realistic timeframe for achieving compliance is essential," Harris says. Keep it real. "Most likely, a two-week sprint to compliance will fail miserably and frustrate all involved," Harris says.

Take an organized, steady approach toward adherence with the California law. "Inventory your collection, use, storage, and transfer of personal information," Schwent suggests. Developing processes for evaluating and responding to data access requests and training employees will also take some time.

4 Decide whether to extend CCPA protections to your entire customer base

A key issue companies will face is whether your entire client base will be given CCPA protections. Touchy customer relations issues can ensue if a company offers a slate of new rights to customers in California and not to everyone else, observes W. Reece Hirsch, a partner at the law firm Morgan Lewis.

"A business that is very consumer-facing and heavily depends on direct relationships with consumers for its reputation and business growth may want to extend CCPA rights and protections to all consumers as a promotional, consumer-friendly gesture," suggests Nancy Perkins, counsel at the law firm Arnold & Porter.

> "Personnel need to understand their privacy program so they can help reduce risk for the business, both from a process perspective and a customer communications perspective."
>
> Heather Buchta, Partner, Quarles & Brady

"Agreeing upon a realistic timeframe for achieving compliance is essential. Most likely, a two-week sprint to compliance will fail miserably and frustrate all involved."

Richard Harris, Chair, Technology, Telecommunications, and Outsourcing Practice, Day Pitney.

5 Revise your online privacy notice

"Update Website and employee privacy policies to include descriptions of the categories of information collected, third parties with whom data is shared, and rights available to individuals under CCPA," suggests Laura Jehl, leader of the global privacy and cyber-security practice at the law firm McDermott Will & Emery.

Take a look at your internal (non-customer-facing) privacy policies and procedures as well. "Businesses should have such an internal privacy policy," Lathrop Gage's Schwent says, noting that too many do not. "The policy should be drafted with the specific needs and uses of the organization in mind to ensure that it is implementable, useful, and enforceable," he says.

6 Document "reasonable security" practices

The CCPA "also contains data protection and security provisions and provides a private right of action for consumers affected by a data breach caused by a business' failure to provide 'reasonable security,'" Jehl notes. Although the entire law takes effect on Jan. 1, 2020, "only the security provisions will be immediately enforceable, either by the California Attorney General or via a private right of action," she explains.

Covered businesses should review information security processes "against established data security standards such as National Institute of Standards and Technology, International Organization for Standardization, or CIS Critical Security Controls," Jehl suggests. Companies should "ensure sufficient documentation of those controls is in place to demonstrate 'reasonable security' in the event of a data breach," she says.

7 Establish a subject data request process

Remember that verification obligations under the California law "are significant," Schwent says. "And businesses that fail to comply with those requirements and release personal information to the harm of the consumer may face litigation for those mistakes (as well as regulatory enforcement actions)," he notes.

"Companies should be prepared to intake and effectuate consumer access and deletion requests," says Kandi Parsons, an attorney at the law firm ZwillGen.

8 Figure out where your data is

Map personal information that your business maintains or that service providers maintain on your behalf, suggests Perkins of Arnold & Porter. "You'll need to know the types of personal information that you have collected in the past 12 months, the purposes for which you collected it, and the types of entities to whom you disclosed it in the past 12 months, and continue to track that on an ongoing basis," she says.

Don't forget "offline" data—the sort that's in the real world. The CCPA regulations "clearly push data privacy disclosures into the offline realm, including onsite consumer interactions," Buchta cautions.

9 Review vendor contracts

"Figure out which vendors have access to any personal information, pull the contracts, and double check the data use language," Buchta adds. Put amendments in place "to give you the contractual protections you need for data restrictions," she says.

10 Train employees

The "CCPA places a strong emphasis on training of personnel who will be responsible for receiving and acting on consumer requests," Harris notes. "Personnel need to understand their privacy program so they can help reduce risk for the business, both from a process perspective and a customer communications perspective," Buchta says.

After all, "the process of fielding access requests, deletion requests," and requests to opt-out of the sales of one's data "is not a typical customer service exercise," Schwent notes. Addressing these requests "can impact a number of operations," he continues. Ultimately, "employees must be trained on the policy to make sure that everyone (not just IT) knows how to handle personal information within the organization and what each employee's responsibility is with respect to the same." he says. ■

RED OAK
Compliance Solutions

The Industry's Leading Advertising Review Software.

Where compliance, expertise, and superior technology meet.

35%
Faster Approvals

70%
Fewer Touches

100%
Books and Records

LET OUR TEAM OF EXPERTS HELP YOUR FIRM

www.redoakcompliance.com (888) 302-4594

Regulators sympathetic to GDPR growing pains but expect maturity

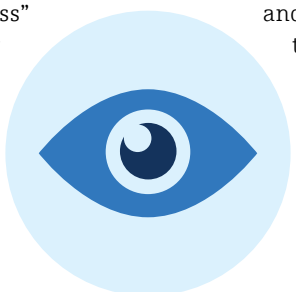
Officials from EU data privacy sanctioning bodies stress importance of good-faith efforts and DPOs. **Dave Lefort** has more.

If you are still trying to fully understand and implement the European Union's General Data Protection Regulation (GDPR) nearly a year and a half after it went into force, you're not alone.

Regulators who spoke at the recently concluded Compliance Week Europe conference in Amsterdam acknowledged businesses were still very much in the "awareness" phase of implementation of the EU's complex new set of data privacy rules, but that doesn't necessarily mean they're shielded from sanctions.

In fact, data protection authorities (DPAs) from at least 23 of the 28 EU member states have issued fines under the GDPR, three of which have topped $50 million. The exact number of enforcement actions is not known, but it's more than 100.

The question you might be asking, then, is if you're among the many organizations still trying to fully grasp the rules and wrap your head around all of the data your organization collects, should you expect the "carrot" of guidance from regulators or the "stick" of enforcement if you've been found to be in violation?



VIEW FROM EUROPE

"If there is a complaint, we're going to investigate," insisted Ventsislav Karadjov, deputy chair of the European Data Protection Board and chairman for the Bulgarian DPA. "We cannot say there is a grace period and we're not going to sanction you. If the infringement is very severe, and it concerns a lot of people, the remedy for these people would be a sanction.

"But if we identify that the [data] controller is responsible and has done his (or her) utmost to be compliant, then there is a good opportunity that the controller is not sanctioned, but with some of the instruments of the regulation will be advised what to do, how to do it, and be prescribed a period of time to take actions. After that time, if he doesn't undertake the actions, he'll be sanctioned."

In other words, if you can prove you've demonstrated a good faith effort at implementing the rules and understanding which data is collected across your organization and for what purpose, you're much more likely to get the carrot than the stick.

Ali Shah, the head of technology policy for the U.K.'s DPA, the Information Commissioner's Office (ICO), took issue with the carrot versus stick characterization, saying it's "more nuanced" than one or the other, but agreed with the idea that the more you can show efforts to protect data across your

organization, the better you'll be viewed in the eyes of regulators.

"If a complaint comes in or we determine there's an issue, we need to investigate and to understand," said Shah. "Sometimes the answer is talking to the organization and advising them on how to resolve the issue. Or, depending on the nature of the issue, it could lead to a compulsory audit, stop notices, fines—all of the range of enforcement powers."

Specifically, regulators will look at whether you're taking a mature approach to how you manage data.

"We understand it's a journey, but what we won't accept is that the work is not being done in all parts of the organization to try and become more mature," Shah said. "You have to be on that journey and demonstrate that."

Empower your DPO

An engineer by trade with a specialty in machine learning, Shah has been with the ICO for just over nine months and brings a valuable outsider's perspective. He said a company's data protection officer (DPO)—a role required for every company impacted by the GDPR—is critical, and that whoever fills those shoes needs to be empowered by their organization's leadership in order to be truly effective.

"It's a tough environment," Shah said. "Not only do you have to wrestle with what the law says, but you also have to go and convince your leadership about why this matters, alongside all of the employees who are dealing with your customers and the different ways that your customers might be interacting with you. That can feel like a tall order."

It's an especially tall order without headline-grabbing enforcement actions that can scare senior management into empowering the compliance function. The ICO has issued the two biggest fines under the GDPR so far—£183 million (U.S. $230 million) for British Airways and £99 million (U.S. $124 million) for Marriott—both in the wake of massive data breaches. Aside from those two, there haven't been the kind of big fines many predicted for 2019. Thus, DPOs in some organizations face an uphill battle in their quest both to take stock of all the data the company holds on customers (and whether they need to hold it) and to implement the data protection measures required by the GDPR.

Shah's advice for DPOs: "Start to make the rest of the organization understand it's no longer possible to tick compliance and have it rest just on the data protection officer. This has to go upwards and downwards and across the board. Raising awareness within the organization about why it's necessary for everything from product and engineering, through to the InfoSec security teams through to the leadership. Being aware of the intrinsic nature of personal data in your business and what risks that might carry if there is noncompliance, that's important."

Find your data privacy champions

That perspective was backed up by Angela Bardenhewer, the DPO at Fusion for Energy, an EU institution that is governed by a slightly different set of rules from the GDPR but that is generally very similar.

She pointed out most of the principles of the GDPR are not new, "but what has really been changed is this shift of culture" that is required.

Her strategy is to delegate across her organization, to essentially create data privacy coordinators across all silos of the business—HR, finance, procurement, product management, etc.—and hold them accountable. It's a strategy endorsed by Shah and Karadjov wholeheartedly.

"If you identify like-minded people in product and engineering and elsewhere, they will act as your champions because they will feel motivated," Shah said. "Fundamentally, most people just want to do the right thing, but they're not necessarily going to get energized by conversations about compliance. But they will get energized if you say, 'Let's work on your product idea and try and [figure out] how you can achieve what you want to achieve with your innovation but make sure it fits on what we all have agreed as a society about the laws that represent us.' "

During the panel discussion, Karadjov briefly took off his regulator hat and put himself in the shoes of a DPO, offering examples of the questions he'd ask his company and how he would approach one of the most difficult jobs in compliance.

"First thing is, you need to have a clear understanding of all of the activities of the business," he said. "You have to understand that clients are data subjects as well. What is the minimum data you need to provide the service you're providing? DPOs should talk to departments to see if [the personal data] they are collecting is reasonable. Is it excessive? Keep in mind, every data subject may request this data to be deleted.

"Second, you have to know what every department is doing, what data they are collecting, for what purposes, to whom they are delivering the data outside the organization, and why they are doing it. And you have to document all of this."

It's a daunting task, but one Karadjov explains will benefit the company in a number of ways. Not only will the DPO be able to create a comprehensive data blueprint and perform a risk assessment for each department, but he or she will also be able to respond promptly to data subject requests: "You'll immediately know on what legal grounds you are processing this data and can immediately respond instead of doing the analysis on each request." ■

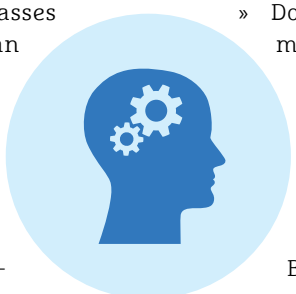
Six steps for developing an AI ethics framework

Artificial intelligence can undoubtedly improve processes and create efficiencies, but it can also be an enormous risk if it's not designed with ethics in mind. **Jaclyn Jaeger** has more.

The more that companies rely upon artificial intelligence in their business operations, the more vital a role chief ethics and compliance officers play in ensuring that the use of such technologies aligns with their organization's mission, core values, and regulatory requirements.

Managed the right way, the opportunities for application of artificial intelligence (AI) are endless—but managed the wrong way, so are the legal, regulatory, reputational, and financial risks. "A myriad of opportunities to leverage AI highlight why an ethical mindset is critical to protect an organization from unintended, unethical consequences," Maureen Mohlenkamp, a principal in Deloitte's risk and financial advisory practice, said during a recent Deloitte Webcast on AI ethics.

In broad terms, artificial intelligence encompasses technologies that are designed to mimic human intelligence. Because AI's application is still in its early stages, companies across all industries have only just begun to scratch the surface of its full potential in the business world.



ARTIFICIAL INTELLIGENCE

In the financial services industry, for example, banks are using machine-learning algorithms to sift through vast oceans of data to uncover anomalies and possible fraud scenarios in payment transactions in real-time. In healthcare, hospitals are using AI to more accurately diagnose and treat patients. In the transportation industry, AI is being used to create self-driving vehicles intended to reduce accidents and—eventually—replace human drivers for some businesses (think trucking, shipping, ride-sharing, etc.).

Enter AI ethics

"AI ethics is about integrating ethical constructs into how organizations develop new technologies," Mohlenkamp said. Chief ethics and compliance officers (CECOs) play a very important supporting role in this process. Consider the six key steps below as you think about developing your company's AI ethical framework.

1. **Develop an AI Code of Ethics.** Many companies as a matter of practice include in their Code of Business Conduct reflection questions to support individual decision making in a wide variety of risk areas. This same idea could be applied in a similar manner to questions around the ethical use of AI. Examples of reflection questions to include might be:

- How is artificial intelligence used in my specific job function, and how does AI help me achieve that?
- What consent do I need (from customers, employees, etc.) around that data?
- What third parties will be handling sensitive data, and for what purpose?
  - Does that purpose align with the organization's core mission and values?

"The challenge is to ensure that the guidance provided on this topic does not become so specific that it is silo-bound and simply reflects the nature of the department that has introduced it," Guendalina Dondé, head of research at the Institute of Business Ethics, told Compliance Week. "Issues can and should extend across different departments and activities."

What's also important is for the company to recognize what expertise it needs and be willing to seek it out—data scientists, software engineers, analytics experts. Tae Wan Kim, associate professor of business ethics at the Tepper School of Business, Carnegie Mellon University, put it this way: "There are computer scientists who are interested in ethics, and there are ethicists who are interested in computer science … but it's not easy to find one single person who can address these two aspects at the same time."

It's also important that a speak-up culture be in place that complements an AI ethics policy, Dondé said. And those responsible for fielding employee concerns and complaints should be aware of any potential ethical lapses created by AI, not unlike any other risk.

Regulators need experts in AI, too

Machine learning isn't something that's going to happen—it's already happened.

"If you've got a smartphone in your pocket, you've interacted with machine learning and AI. ... It's already part of our everyday lives, yet we don't necessarily recognize that," said Ali Shah, head of technology policy for the U.K.'s Information Commissioner's Office (ICO). Shah spoke at the Compliance Week Europe conference in November.

Shah spent 15 years working in various roles as an engineer and leader of emerging technology at the British Broadcasting Company before joining the ICO just over nine months ago. His professional interests lie in artificial intelligence, data, and the rights of citizens, among other things.

AI and machine learning are a transformational development with the potential to alter the nature of how we operate in society, Shah said. Yet, he cautioned there are still challenges to address (like the gap in people's understanding of what AI is) along with significant business, regulatory, and ethical considerations that often conflict with one another.

Compliance leaders are in the hot seat to determine how to balance the corporate incentives of using machine learning with their organization's responsibility to protect the rights of individual citizens—not to mention complying with the European Union's General Data Protection Regulation (GDPR).

"There are tensions between what the GDPR says and the current approach taken in the development of machine learning," explained Shah. For instance, GDPR says data minimization is really important, but the development of machine learning depends upon ample data collection.

Plus, business leaders "have to balance the needs of their organization—generating a profit and being successful—with the sorts of provisions that are in the law," said Shah.

Data protection authorities like the ICO and the Federal Trade Commission in the United States will need individuals who can make sense of the way these emerging technologies are being used in real-world applications.

Shah

Shah's team is developing a framework that will allow the ICO's investigations and regulatory assurance functions to make sense of how emerging technologies are being used by companies and evaluate whether those businesses have put the risk and control measures into place to avoid a problem.

"If your corporate incentives don't include an acknowledgment, by action, of the rights of individuals as part of the equation, you will have issues," warned Shah.

The ICO expects to issue guidance on this topic in the spring of 2020.

—Aly McDevitt

2. **Embed an ethical framework into AI.** "Given the rapid adoption of AI in business, there is the risk that the governance systems required to mitigate the potential risks of its deployment are overlooked," Dondé said. This would be a mistake. The ethics team needs assurance that the AI systems align with the company's core values, while legal and compliance needs assurance that the company complies with relevant rules and regulations, especially concerning data privacy and cyber-security.

"This is going to require a team approach, with different lenses of expertise and different areas of focus both inside and outside the organization," said Christopher Adkins, executive director of the Notre Dame Deloitte Center of Ethical Leadership, who spoke on the Deloitte Webcast. "We really need to think from the beginning about, what is our design mindset? Not just what can be built, but what should be built."

"This is going to require a team approach, with different lenses of expertise and different areas of focus both inside and outside the organization. We really need to think from the beginning about, what is our design mindset? Not just what can be built, but what should be built."

Christopher Adkins, Executive Director, Notre Dame Deloitte Center of Ethical Leadership

Consider creating internal workshops or working groups that bring together different departments and functions—led by IT, data-security, and privacy, in collaboration with ethics and compliance, HR, risk, legal, procurement, and senior management—to share AI-related issues from various perspectives. In conducting an AI impact assessment, questions to explore may include:

- How is the company using AI?
- Where does this happen within the organization?
- What job functions should be thinking about AI ethics?
- What data is being fed into the algorithms?
- Does the AI solution's intended purpose align with the organization's mission and values?
- How do you get consent around the data? Do customers need to be informed, for example, that you're capturing their data?
- Is there a reporting process in place to escalate issues concerning ethical lapses in AI?

Think of it as an AI ethics-by-design framework. Much like privacy-by-design, which is thinking about data protection and privacy controls from the outset, AI ethics-by-design is thinking about the ethical use of AI data and technology at the outset.

3. **Conduct an AI ethics gap analysis.** The next step should be to test and monitor the data to ensure that it's of sound quality and to reduce the risk of inherent biases and inaccuracies. "The objective of zero bias is unlikely to be realized. That is true with humans, with machines, or a combination of both," said Nicolas Economou, chair of the law committee of the IEEE's Global Initiative on Ethics of Autonomous and Intelligent Systems. But companies can develop ways to determine the impact that algorithms will have and the extent to which the processes they have in place produce desirable effects, he says.

For example, many large companies today are using AI in their hiring practices to sift through résumés and narrow them down to the top job candidates. Here, an analysis could be performed to ensure that the résumés received through the AI process align with the decisions that HR would have made, Economou said.

Real-world scenarios provide cautionary tales about what can happen when proper testing and monitoring is not done. Amazon, for example, once tried using an algorithm in its hiring practices by training computer models to vet the best job candidates, but because the algorithm was based on historical job data in the technology industry, it inherently favored men over women.

"AI ethics is as much about understanding the risks as it is about establishing a process for avoiding them," Mohlenkamp said. "Review existing organizational policies, procedures, and standards to address existing gaps, then expand existing policies or build new ones accordingly."

4. **Conduct due diligence on third parties.** It is also prudent to monitor any third parties that handle sensitive data to ensure that they commit to similar ethical AI standards. "The design of these systems might be outsourced, and it is important to conduct ethical due diligence on business partners," Dondé says.

"AI ethics is as much about understanding the risks as it is about establishing a process for avoiding them. Review existing organizational policies, procedures, and standards to address existing gaps, then expand existing policies or build new ones accordingly."

Maureen Mohlenkamp, Principal, Risk and Financial Advisory Practice, Deloitte

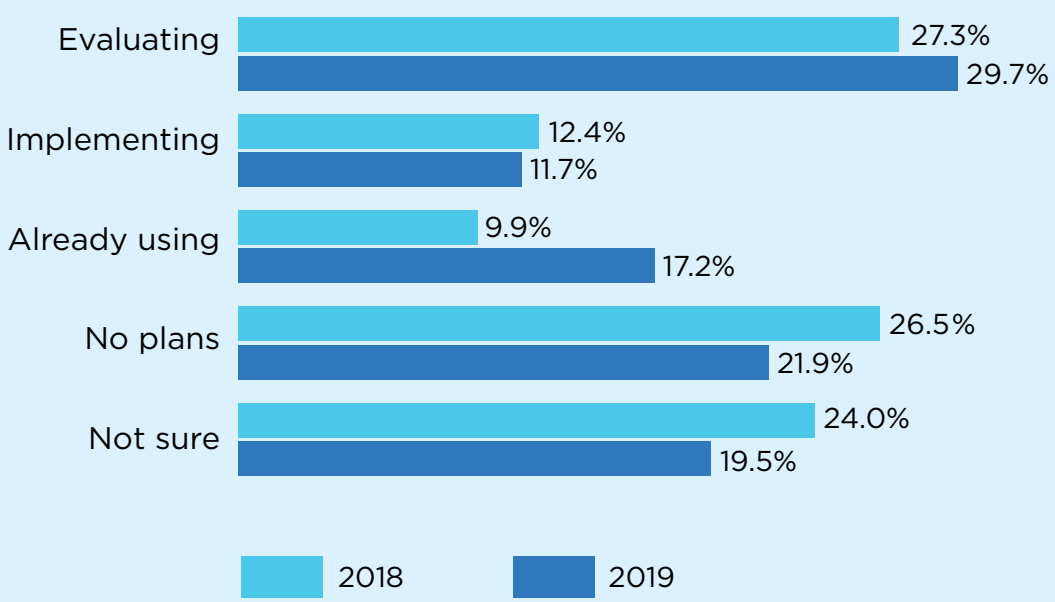
"A similar principle applies to clients and customers to whom AI technologies are sold," Dondé said. "Testing a third-party algorithm in a specific situation is also important to ensure accuracy."

5. **Educate and train.** "It is not realistic to expect that every company can train every employee to become experts at AI," Economou said. Instead, focus on training and educating those who make extensive use of AI in their job functions. Make sure they know which fundamental questions to ask and whom to ask, and what answers reasonably make sense. Also, those developing algorithms and managing data will need to be specially trained to identify and mitigate bias within AI applications.

AI competence builds confidence. Users of AI should be competent enough to understand its limitations, understand where weaknesses or biases in the data may be located and how to correct for them, ensuring that the decisions being made by AI technologies are consistent with those that an expertly trained, qualified employee would have made. "That's a nascent challenge, that there is more AI than competent people to utilize it across the board," Economou said.

"Employees and other stakeholders need to be empowered to take personal responsibility for the consequences of their use of AI," Dondé said. They need to be provided

What best describes your company's approach to artificial intelligence?



with not only the technical skills to build or use AI, but also understand the potential implications that it can have, she said.

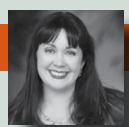
6. **Establish accountability.** Accountability is another important consideration in the AI ethics process. Companies simply do not have the prerogative to blame ethical lapses on AI systems. Business leaders, regulators, enforcement authorities, customers, and other stakeholders will demand full transparency and accountability, and accept nothing less. "You can't hold a system accountable," Economou said. "You have to hold humans accountable."

The difficult question, however, is who should be held accountable when an AI system produces an unethical outcome, whether that outcome is intentional or not? "You need to be able to map out the accountability," he said. "Who is accountable and responsible for what decision?" It's a complex question with no easy answer.

Accountability should also extend to third-party service providers and vendors. The IBE recommends including in contracts with third parties a clause defining each party's responsibilities and limitations. "Although it is not always practicable or comprehensive and it can't substitute for individual empowerment, this can help to prevent a situation where all parties have shared responsibility and, therefore, it becomes difficult to attribute accountability appropriately," Dondé said.

Finally, it's important for CECOs to stay on top of the latest developments in AI ethics. The National Institute for Standards and Technology, for example, recently announced that it is developing standards for the use of AI. The Council of Europe, too, is currently working to develop a certification program and legal framework for use of AI application. Such guidance will serve as real-world, practical instruments that CECOs can turn to in their important quest to help advance the ethics of AI. ■

Ask Amii mailbag



Compliance and the advance of automation

In your opinion, in which industry will compliance be most important five years from now? I am of the opinion that automation is going to change EVERYTHING (self-driving cars, delivery drones, etc.) and that the compliance function in the industries where automation is most predominant is going to be more important perhaps than the innovation that drives this change. Do you agree? And do you think Big Business will see it the same way? - Anonymous

Amii: Advances in automation, artificial intelligence, machine learning, and the use of blockchain will certainly impact the entire economy, including manufacturing, healthcare, transportation, retail, and education. Compliance systems will need to keep pace with the volume and velocity of data and the complexity of automation. In parallel, we can expect automation to change compliance.

Will advances in technology help us do our jobs better? Will these new tools help us in our mission to scale, do more with less, and reduce risk in our organizations?

I'm hopeful. Automation holds promise by providing compliance with comprehensive data and early warning signs of potential issues. For example, one cutting-edge training company is using AI in its sexual harassment training to anonymously collect "orange flag" behaviors before they escalate, enabling organizations to reduce hot spots with skill-building, increased awareness, and behavior change. In a recent survey by Dun & Bradstreet, the top areas to benefit from AI were enhancing fraud and risk detection, data gathering and validation, risk screening, and account reconciliation. A substantial number of compliance professionals believe, however, they do not have the talent in place to use AI in the next year.

Regarding Big Business: As powerful as technology is in shaping our environment, it won't change human nature. Businesses will still be scattered across today's risk appetite continuum, many appreciating the alignment of compliance as a strategic asset critical to the achievement of profit goals. Then again, many will stand in blind or willful denial in the absence of an active crisis that compels them to act.

To ask Amii Barnard-Bahn a question of your own, go to complianceweek.com/ask-amii-mailbag.

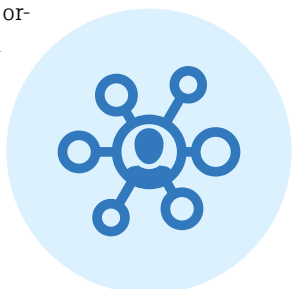
Data-driven compliance can create business success

Smart uses of data analytics show that companies can not only improve their compliance programs with technology, but actually create bottom-line results for their companies as well. **Tom Fox** has more.

The Ethical Edge—it's the idea that proactive, data-driven compliance programs can not only ensure an ethics-by-design culture, but also create business process efficiencies that can lead to greater profitability.

We are now at a place where there is sufficient data, academic research, and actual use cases from businesses that demonstrate proactive ethics and compliance programs are not simply good for businesses but, properly used, also lead to greater profitability.

One of the more interesting stories is from an organization that performed a standard fraud risk analysis of business-development personnel spending in a high-risk FCPA country. Because the country was high-risk, there was a relatively low gifts-and-entertainment limit below which the business folks could spend without pre-approval—$75. The fraud risk analysis looked at traditional metrics, such as split receipts and invoices right at, but not over, the limit. The company also looked at the aggregate amount of gifts-and-entertainment spending on individual government officials to see if multiple salespersons were directing their money at one official.



DATA ANALYTICS

The findings of this analysis were not what was expected, or even what the organization was looking for. The gifts and entertainment spending segregated into two buckets: low spend (Data Point A) and high spend (Data Point Z). The sales team had to spend a minimum of "Data Point A" to make a sale but, if they spent above "Data Point Z," the data demonstrated that the government official was not going to enter into a contract and conclude a sale.

As a result of its analysis, the company decreed that the sales team had to spend up to "Data Point A," but could not spend above "Data Point Z." It turned out the sales team appreciated the information, as they now had a metric by which they would know when they were not in the running to make a sale. When they got to "Data Point Z" in gifts-and-entertainment spend, they moved on to the next customer.

The effect was twofold: First, the company had an immediate cost savings—business development personnel were not throwing good money after bad (above "Data Point Z"). More interestingly, the company found that by moving on from a sales prospect with which there was virtually zero chance of success in making a sale, it reduced its sales cycle time and increased performance and profitability in the business unit.

What started out as a compliance-focused data analysis ended up not only ensuring a more ethical business culture. And it also—unexpectedly—created a business process efficiency that directly impacted the organization's bottom line.

Academic research lends credence to this theory as well. A pair of Harvard professors—George Serafeim and Paul Healy—demonstrated in their paper, "An Analysis of Firm's Self-Reported Anti-Corruption Efforts," that companies with robust compliance programs do better financially in countries prone to corruption than companies with less effective programs. Without a robust compliance program, even with high sales in a high-risk country, the sales will drop off and lead to a negative return on equity (ROE) of between 24 to 30 percent.

George Washington University Professor Kyle Welch, in a paper entitled "Evidence on the Use and Efficacy of Internal Whistleblower System" reviewed 15 years of anonymized whistleblower data from NAVEX Global. His key findings were that more robust whistleblower reporting systems led to a material reduction in litigation costs, fines, and penalties. He found there was higher quality corporate governance in companies with more robust reporting cultures and that higher earnings were reported. Overall litigation settlements of non-material litigation matters also dropped 20 percent over 3 years.

If we are to learn from the abundance of research, businesses would surely benefit from the Ethical Edge. ■

Three Technology Must-Haves for Your Compliance Training

ADAPTIVE LEARNING

The most effective training uses adaptive technology to adjust the difficulty of training as each course unfolds. Adaptive training goes far beyond "personalization" and "branching", because it allows for individualized coaching and feedback. Training platforms like Scholar by True Office Learning guarantee 100% mastery of each topic, and save learners up to 50% in seat time.

BEHAVIORAL DATA CAPTURE

Compliance training can become your greatest source of behavioral intelligence. Look for solutions that capture true behavioral data behind trainings that help you predict where incidents are most likely to happen, and address those weak spots before it's too late. Platforms like I.Q. Analytics help you put data to use; retarget segments that need support, identify knowledge trends, and avoid training fatigue.

TRAINING ECOSYSTEM

For a year-round successful program, choose a solution that picks up where training leaves off. Operationalization tools like job aids inject compliance into employees' day to day work. Diagnostic tools give you a "pulse check" on risk areas throughout the year. Training videos help engage employees in a relatable, effective way. Using behavioral data and a suite of full-lifecycle training tools, you can turn your program into a training ecosystem that makes compliance a part of your company culture (and even uses A.I. to automate it).

Get a Demo Today

Privacy warfare: Competitors, consumers pose new risks

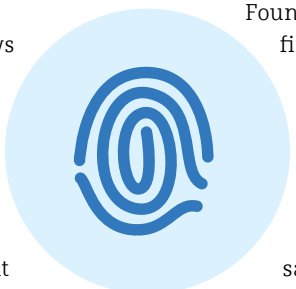
With a new wave of privacy laws empowering consumers to police their own data, companies are facing increased risk in areas they might not have considered. **Kyle Brasseur** has more.

It started with a billboard. High above the Las Vegas Convention Center, just off the Vegas strip, a message from Apple overlooked the annual Consumer Electronics Show convention, where key competitor Google was getting ready to announce its latest and greatest technological developments.

"What happens on your iPhone, stays on your iPhone," the billboard read. A riff on the popular Vegas saying, the quote garnered attention for Apple at a convention it wasn't even attending and stands as the opening salvo in a war of words tech giants have waged in 2019 around the burgeoning world of data privacy legislation.

"I'm starting to see that, and it's pretty new," says Dominic Sartorio, SVP of products and development at software provider Protegrity. "It used to be: keep quiet, because you don't want to be out there publicly gloating and then the very next day you're the one that gets breached as well. It used to be like that."

He adds: "What's starting to change is now that companies are putting in place more sophisticated and more mature data protection mechanisms, they may feel more confident."



PRIVACY

Since data privacy laws became in vogue with the European Union's General Data Protection Regulation (GDPR) in May 2018, Apple certainly has not lacked for confidence. CEO Tim Cook spoke in Brussels on the topic in October 2018, calling on the United States to enact its own version of the law and bashing those who "put profits over privacy."

Things went quiet until Apple again made headlines with its billboard in January universally seen as a shot at the privacy shortcomings of Google, which would be fined €50 million (U.S. $57 million) later that month by France's data protection watchdog, CNIL, for violations of the GDPR regarding its ad practices. Though Google continued to find itself in the muddy waters of the GDPR, with Ireland launching a new probe into the search engine giant in May, that same month CEO Sundar Pichai couldn't help but take a veiled shot back at Apple in an opinion piece defending Google's dedication to privacy penned for the *New York Times*.

"Our mission compels us to take the same approach to privacy," Pichai wrote. "For us, that means privacy cannot be a luxury good offered only to people who can afford to buy premium products and services. Privacy must be equally available to everyone in the world."

The "premium products" jab didn't seem to faze Apple. It wasn't until August that Google was able to really ruffle the feathers of its competitor, courtesy of a blog post from its Project Zero team.

In the blog, titled "A Very Deep Dive into iOS Exploit Chains Found in the Wild," the Project Zero team, tasked with finding zero-day vulnerabilities in software across the world, carefully explained the flaws in Apple's syste=ms that allowed hackers to target China's Uyghur Muslim community. Perhaps it was too carefully explained though as all the technical jargon masked the Uyghur target portion of the story and caused many iPhone owners unnecessary concern they might have been hacked.

"The sophisticated attack was narrowly focused, not a broad-based exploit of iPhones 'en masse' as described," Apple responded in a statement. "The attack affected fewer than a dozen Websites that focus on content related to the Uyghur community. Regardless of the scale of the attack, we take the safety and security of all users extremely seriously.

"Google's post, issued six months after iOS patches were released, creates the false impression of 'mass exploitation' to 'monitor the private activities of entire populations in real time,' stoking fear among all iPhone users that their devices had been compromised. This was never the case."

Facebook has also had its say in the back-and-forth with veiled shots from CEO Mark Zuckerberg at Apple's practices in China, where Apple has notably made concessions on user privacy to appease the government. Other companies have been much less subtle, like the Mozilla Foundation publicly calling out payment service provider Venmo twice in the last two years over its privacy practices.

Herein lies the risk that affects all companies. On top of

getting in line with new privacy regulations that tout stiff penalties for violations of requirements not easy to achieve, the idea that another firm could put a target on your back regarding your privacy practices poses significant reputational risk.

"To me, the companies that have distinguished themselves the greatest and are far long in the maturity curve are the companies that have really viewed privacy and good data protection/data governance as a competitive differentiator for them," says Hilary Wandall, senior vice president, general counsel, and chief data governance officer at TrustArc. "They see it as embedded into goodness in practice—their reputation as a whole—with customers as well as the broader public, and that has really been the primary driver."

With great power …

Privacy laws are undoubtedly designed to empower consumers to protect themselves and their data from being misused by companies. But what happens when the consumer utilizes that power for reasons other than what is intended?

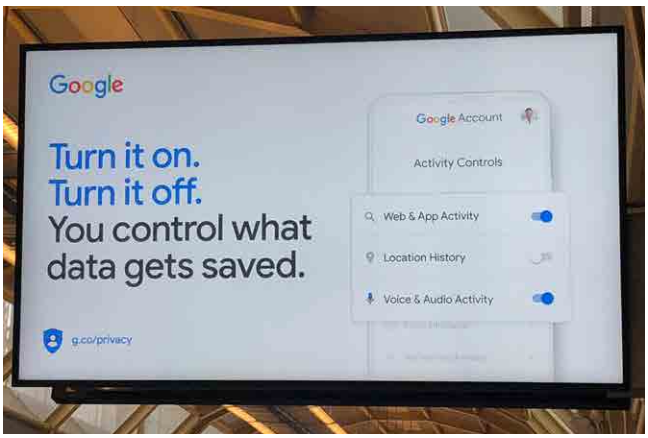
An example of such conduct arose in October, when a post on the aggregate site Reddit went viral after suggesting readers overload the gaming company Blizzard with GDPR requests regarding right of access. The post, shared the same day Blizzard made the controversial decision to ban a top player of its virtual card game Hearthstone for his comments supporting the Hong Kong protests in China, received more than 8,000 positive responses.

Included by the poster was a letter other users could simply copy/paste in order to submit their own GDPR requests. One comment from an individual claiming to be a data protection officer (DPO) said "reading this post made me break out in cold sweat," before lauding the original poster as a "miserable bastard genius." Requests for comment from Activision Blizzard were not returned.

"It totally does not surprise me," Sartorio says of the Reddit movement. "The idea of, 'OK, I'm going to inundate these guys with right-to-be-forgotten requests as a social statement.' It's cool, it's innovative, it's fun, and not surprising."

Mounting a defense

Under the GDPR, the onus is on the company to produce the requested data. So even if 10,000 consumers flood a company with requests for the sole purpose of disruption, that's the company's problem. In such a case, a company abiding by the GDPR can refuse to comply with a request or charge the requestor a fee if it can prove it is "manifestly unfounded," which would cover requests malicious in intent. A prudent program would want to consider each request on a case-by-case basis, however, meaning a level of disruption is still required.



Google launched a worldwide ad campaign this year touting its data privacy tools.

The same language is built into the upcoming California Consumer Privacy Act (CCPA).

So how can a firm protect itself? Sartorio's first suggestion is simple: Don't put a target on your back."If you put yourself out there with a very public statement around privacy or rights in the digital sphere, generally you should be prepared to deal with that kind of social activism," he said.

Preparedness is key, and automated technology solutions can go a long way toward helping address such a problem when it arises. Perhaps the best solution, however, is putting someone in place to identify the issue before it even becomes one.

"I think that is one of the most important things companies can do to protect themselves—put somebody who is thinking about these things strategically and has a voice with the business leaders of the company to make sure everybody is mindful of the problems," Wandall says.

Change needed?

The GDPR is just the beginning for data privacy legislation. The CCPA is around the corner in the United States (Jan. 1, 2020), and with that could come a new wave of additional state privacy laws that expose more companies to the same risks.

Could the targeted attacks of competitors and consumers lead the way to change?

"I think laws will have to take account for it," says Wandall. "I don't think the laws will be able to keep up with the issues companies are facing.

"The law will have to evolve to address these risks that weren't necessarily anticipated at the time but were written strictly to address individual rights. Because there are competing risks at play, it will have to be balanced in terms of the underlying legislation itself or the regulations." ■

‘Femtech’ wanders into uncharted regulatory territory

Applications that serve women’s health needs could soon be held to a higher standard of accountability for protecting users’ data if they become classified as “covered entities” under HIPAA. **Aly McDevitt** reports.

The burgeoning industry of “Femtech”—technology designed to serve women’s health needs—dwells in nebulous territory from a compliance standpoint. On one hand, these applications and/or wearables are developed by technology companies without the regulatory burdens associated with, say, healthcare organizations. On the other, these companies collect, analyze, and store data related to women’s health, which sounds a lot like a healthcare company to some.

So, where does the line exist between a technology company and healthcare, and how are compliance practitioners supposed to know when their organization wanders from one industry into another? That’s the question regulators and executives are grappling with, and one we’ll attempt to untangle.

HEALTHCARE

First things first: What is Femtech?

The range of women’s health needs addressed by Femtech is far-reaching. It includes fertility and menstruation tracking; pelvic floor strengthening; contraceptives; and “smart” biosensing technologies like tampons, vibrators, and breast pumps—body-invasive devices that provide analytics to companion applications with which they’re synced.

Femtech—a term coined by the CEO of one of the first women’s health apps—first emerged in 2013 with the advent of Clue and Glow, two distinct menstrual cycle-tracking apps. The industry has since exploded as venture capital markets opened to startups. Investors have poured over $1 billion into Femtech, and market research firm Frost & Sullivan predicts the industry could be worth $50 billion by 2025.

Once considered a “niche” industry, Femtech has uncovered a lucrative sweet spot in the tech world. Eighty percent of household healthcare spending is done by women; working age females spend 29 percent more per capita on healthcare than males in the same age group; and women are 75 percent more likely to use digital tools for healthcare than men, according to Frost & Sullivan’s research.

While Femtech is subject to the Federal Trade Commission Act (FTC Act), the industry is unregulated on a federal level as it pertains to privacy and data security regs regarding protected health data. To date, Femtech firms that collect and store personal health data mainly fall outside the purview of the Health Insurance Portability and Accountability Act (HIPAA). Simply put, consumers’ digital health information collected by many of these apps could be rented and sold for profit by developers.

How HIPAA could apply to Femtech

Motion for change is underway. If recent proposals for HIPAA reform are granted, Femtech developers and companies will be held to a higher standard of accountability for protecting users’ privacy and data. To that end, these companies will need to expend resources to implement technical safeguards like data encryption.

HIPAA applies to specific “covered entities” encompassing three distinct categorizations: healthcare providers or healthcare plans, clearinghouses, and business associates.

Femtech applications do not fall under the first two categorizations. Most Femtech apps are not operated by physicians or healthcare providers; nor are they payment systems or technology infrastructures that serve as conduits of protected health information. Instead, they are private companies with specialized technologies that collect and store sensitive data concerning women’s health needs.

“HIPAA’s ‘business associate’ category is the only potential category that could sweep a Femtech mobile application under HIPAA regulation,” researcher Celia Rosas writes in “The Future is Femtech: Privacy and Data Security Issues Surrounding Femtech Applications,” published by *Hastings Business Law Journal*.

A “business associate” covers a person (or a company) who “creates, receives, maintains, or transmits protected health information” on behalf of another covered entity, according to

the regulation text of HIPAA. Examples include "a Health Information Organization, e-Prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and requires access on a routine basis to such protected health information."

Uniquely, Femtech app Glow is categorized as a "business associate" and displays its satisfactory HIPAA compliance on its company Website, Rosas points out.

Glow users can opt into the "Glow Fertility Program Patient Services Agreement." The fertility program provides access to fertility clinics and lower pricing on IVF, IUI, ICSI, egg freezing, and medication, the company states. Glow serves as a conduit between healthcare providers of fertility-related services, other persons involved in the financing of healthcare services, and end users. Thus, because Glow receives, maintains, and transmits protected health information to other covered entities, it is subject to HIPAA.

"We maintain 'protected health information' (as defined in the Health Insurance Portability and Accountability Act, 'HIPAA') in compliance with applicable healthcare privacy and security rules and our contractual obligations with our business partners and customers, including healthcare providers and their contractors (who are also subject to HIPAA)," Glow's privacy policy states. Glow might serve as a forerunner for other Femtech apps and companies that could be subject to HIPAA if the scope of regulation is expanded to include Femtech companies under "covered entities."

A covered entity under HIPAA must implement "appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information," the U.S. Department of Health and Human Services Website states.

Covered entities must encrypt electronic protected health care information in motion—during data transmission. In Glow's case, for instance, any end user's protected health data transmitted to providers of fertility-related services or to persons involved in the financing of healthcare services must be encrypted during transmission. Glow, along with all covered entities, can choose its type of encryption as long as it is "reasonable and appropriate," according to the National Institute of Standards and Technology (NIST) HIPAA Security Rule Guide. In addition, employees must be skilled in their use of the chosen data encryption.

Rosas believes a line should be drawn between two types of Femtech apps: those that provide simple tracking services and those that draw on smart biosensing products to capture data and sync it to companion apps.

Early apps like Clue offer features allowing users to answer a series of questions in the app and manually track menstruation symptoms on their fingertips; this is considered a simple, non-invasive tracking service. In contrast, apps like Next Gen Jane, Lioness, and Elvie use invasive devices that users insert or wear on their person to track their bodies on a whole new level.

NextGen Jane, for example, invented a smart tampon device that women can use to monitor their reproductive health by syncing the device with its companion app. "We're developing … a way to listen to the molecular messages from the tissues of your body," the company's Website states.

If proposals for HIPAA reform are too sweeping, it could stifle innovation in the Femtech space, Rosas argues. By holding biosensing devices and their companion apps to a higher regulatory standard, traditional health logs offering simple tracking services will still be able to enter the market.

"Traditional health logs do not store and analyze a high volume of personal data to the extent emerging biosensing products do … Due to the advanced technology inherent in biosensing devices, it is not unreasonable to require that sophisticated products implement technical safeguards like data encryption," Rosas argues.

Femtech regulation today

In May, concerns were raised about protecting data privacy, especially as it pertains to third-party apps, at the Senate Help Committee on the 21st Century Cures Act. Leaders from Congress, the Office of the National Coordinator for Health Information Technology (ONC), and the Center for Medicare and Medicaid Services (CMS) were all in attendance.

When a patient chooses to release private health information from a covered entity—such as their family medical history, for example—through an app that is not a covered entity or business associate under HIPAA, that patient data is no longer subject to HIPAA protections.

Senator Bill Cassidy (R-La.), who happens to be a medical doctor, asked ONC Chief Don Rucker whether third-party apps that collect private health data will eventually be classified as covered entities under HIPAA. Rucker said they will not. When asked whether third parties could sell the data, Rucker replied: "It's a contractual thing to be negotiated between the patient and the app subject to FTC [(Federal Trade Commission)]."

While the future regulatory landscape of Femtech remains obtuse, the status quo demands consumers hold the ultimate responsibility in protecting their own health information when it comes to third-party apps that fall outside the purview of HIPAA. Consumers must read very carefully through Femtech apps' privacy policies before offering up their highly personal information. Some companies, like period-tracking Glow, expressly state on their Websites they do not sell or rent data to third parties. Others do not.

It is also critical that Femtech firms ensure their terms of service and privacy policies are transparent, unequivocal, and prominent; for if the regulatory tide changes and Femtech's time under the radar runs out, problems will surface. ■

PrivacyConnect

CCPA & GDPR Community by OneTrust

NEW DATES ANNOUNCED!

125+ FREE WORKSHOPS

100+ GLOBAL CITIES

CCPA, GDPR & LGPD

Dive into regulatory requirements
and how to implement in practice

INTERACTIVE ACTIVITIES

Gain practical implementation tips
through activities and group discussions

WEBINAR SERIES

Hear from distinguished privacy innovators
on top-of-mind regulatory topics

REGISTER FOR A LOCAL WORKSHOP TODAY: PRIVACYCONNECT.COM

Regulators wary of crypto as digital assets go mainstream

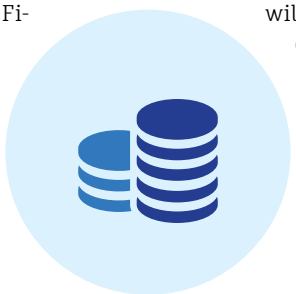
Federal agencies struggle to categorize digital coins as currency, securities, commodities, property, or something else—but even as they dither, some big companies strive forward in the digital assets arena. **Lori Tripoli** has more.

Cryptocurrency has taken a spot on the main stage again, thanks mostly to Mark Zuckerberg's plan to integrate it into a payment system Facebook is spearheading.

And while cryptocurrency generally is gaining acceptance among businesses and consumers, legislators and regulators still don't quite seem to know how to handle it.

"Facebook's plans have serious implications for investors, consumers, data privacy, cyber-security, systemic risks, monetary policy, and national security," the House Financial Services Committee Majority Staff wrote in a memo shortly before Zuckerberg testified this fall.

In some measure, regulators seem to be protecting their own turf. The U.S. Securities and Exchange Commission "has been taking the position that many digital tokens or cryptocurrencies are securities and therefore subject to securities registration requirements," explains Andrew Silver, an associate at Ifrah Law. Perhaps not surprisingly, the Commodity Futures Trading Commission "has likewise stated that both Bitcoin and Ether are commodities, potentially subject to CFTC regulation," he notes.



CRYPTOCURRENCY

Other government officials predict dire consequences with the use of cryptocurrency. Federal Reserve Board Chairman Jerome Powell has raised concerns about financial stability, money laundering, privacy, and consumer protection associated with the Facebook-backed cryptocurrency, known as Libra. Federal Reserve Board Governor Lael Brainard has said that "there are likely to be financial stability risks for a stablecoin network with global reach."

It's already here

Despite alarmist prognostications by government officials, interest in cryptocurrency isn't exactly waning. "Digital currency already has a significant degree of acceptance," says Silver. "At least among those who are tech-savvy."

There's even evidence that digital assets are gaining in popularity. "The wallet application Coinbase is currently ranked on the iTunes App Store ahead of the apps of such major banks as PNC, U.S. Bank, USAA, and Navy Federal Credit Union," Silver reports.

Perhaps even more significantly, in late October, the Bitcoin exchange Bakkt announced its intention to launch an app that would "enable consumers to make purchases with cryptocurrency in 2020," Silver notes, adding Starbucks will be the first retailer launched. Online retailers like Overstock.com and Newegg accept Bitcoin as payment, he reports. Even Microsoft allows consumers to add funds to their Microsoft accounts using Bitcoin.

Retail businesses are getting in on the crypto craze as well. "It is becoming more commonplace for U.S. retail businesses to place 'Bitcoin ATMs' in their establishments, where customers can buy Bitcoin with cash or withdraw cash using their Bitcoin wallets," Silver says.

And it's not just firms in the United States. Large companies in other parts of the world are moving into the crypto arena. "UBS announced this year that it and other major banks are developing a token that will resemble Bitcoin to settle cross-border financial transactions," Silver says.

"An internal or proprietary digital currency could help an international corporation with foreign exchange issues, particularly in jurisdictions from which it is difficult to export hard currencies," observes Philip Moustakis, counsel at the law firm Seward & Kissel and former senior counsel at the SEC.

Government reluctance to OK cryptocurrency

If consumers and businesses are so gung-ho about cryptocurrency, why does the U.S. government seem so baffled by it?

Zuckerberg maintained in his appearance before the House Financial Services Committee in October that "finan-

cial infrastructure in the United States is outdated." Indeed, U.S. legislators and regulators themselves may be as well.

"They aren't educated about it, and they can't control it," maintains David Croft, the chair of the blockchain and cryptocurrency group at the law firm Meyers Roman.

Admittedly, cryptocurrencies do pose risk to the system. "With many cryptocurrencies, including Bitcoin and Ether, trading on overseas, often unregulated platforms, regulators have expressed concern about market manipulation and other potential market abuses," explains Moustakis.

Legislators and regulators may, however, be overreacting after doing too little when digital currencies were first floated. "After being caught somewhat flat-footed with early digital currencies such as Bitcoin, the U.S. government seems to be overcompensating by scrutinizing new cryptocurrencies and digital tokens and subjecting them to securities regulation scrutiny, even when tokens do not share the characteristics of traditional investments," Silver says.

Another concern of the U.S. government could be in regard to its own tax revenue. "Government regulators likely think that a shift away from the dollar to digital currencies could present taxation challenges that ultimately lead to reduced tax collections," Silver explains. Digital currency users might also have an expanded ability "to shield profits and assets that would typically be subject to tax treatment by the IRS," he says.

Getting the go-ahead for a cryptocurrency from U.S. regulators can be a pricey endeavor. "From an SEC perspective, regulatory 'approval' can either take the form of the SEC agreeing that a proposed cryptocurrency or digital token is not a security and, therefore, not subject to securities registration requirements; or it can take the form of complying with securities registration requirements so as to comply with regulators," Silver explains.

"The problem is that it is quite costly to either comply with securities registration requirements or even to seek a 'no action' letter from the SEC," Silver notes. "A step regulators could—but have yet to—take with respect to digital currencies is to outline conditions in which cryptocurrency will definitively not be subject to their ire."

So much potential

Despite these barriers, cryptocurrency still holds a lot of promise. Even as some companies are already using digital currency, "more should," Croft maintains. For instance, "use of stable coins combined with smart contracts would be a smart move for manufacturers." Doing so, he says, "could do away with net payment terms and provide more security to a manufacturer that it will get paid."

Three positives that come with cryptocurrency are the speed associated with its use; the ease of maneuvering large transactions; and its potential for much more cross-border convenience.

Unlike credit card transactions that are subject to "multiday 'hold' periods, cryptocurrency transactions can clear instantaneously, or as soon as the blockchain network processes them," Silver explains. In addition, large transactions, such as wire transfers, normally subject to Monday-to-Friday banking hours, can be resolved more quickly, too. Cryptocurrencies "can be transferred at all hours of all days, adding significant flexibility to high-value transactions, especially when time zones come into play," according to Silver.

Lastly, cross-border deals may become less complicated. Currently, "when companies in one country do business across borders with a counterpart using another currency, one or both parties may be subject to paying exchange rates, and additional banks might need to be involved in order to complete transactions that involve the conversion from one currency to another," Silver says. That's not, however, the case with cryptocurrency since nothing needs to be converted.

What CCOs need to know

At companies contemplating using digital currencies, chief compliance officers "must consider the proper classification or classifications for each digital asset with which his or her firm deals," suggests Moustakis. "Digital assets can operate as securities, commodities, currencies, or other financial instruments," he says. It's a regulatory status that actually can shift.

"The facts and circumstances of any digital asset must be scrutinized, including its offer and sale, its economic reality, and use, to determine whether it is a security or some other kind of asset," Moustakis says. "Due to the mutable nature of digital assets, it may be incumbent upon CCOs to review periodically the possible regulatory statuses of the assets with which their firms are dealing."

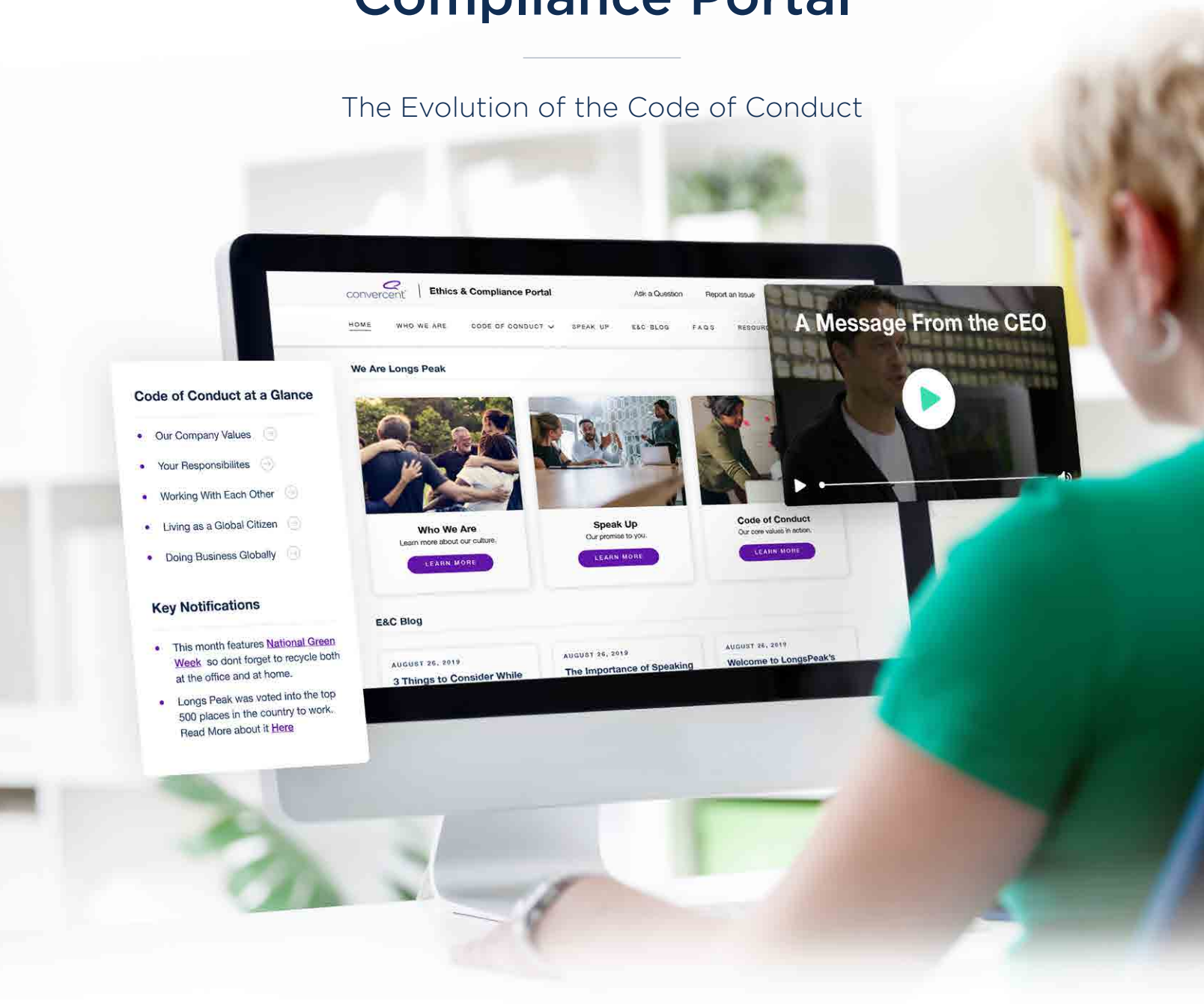
Cryptocurrency users also must beware of criminal elements. Money laundering problems or other illegal activities associated with digital currency can be thwarted with "rigorous application" of anti-money laundering and know-your-customer policies and procedures, Moustakis says.

As a former Commission enforcement counsel, Moustakis predicts "more enforcement activity from the SEC in this space." That said, he posits that "the SEC is working hard to provide sufficient guidelines to permit companies utilizing blockchain across the spectrum to move forward with their projects." ■

convercent

Convercent's Ethics and Compliance Portal

The Evolution of the Code of Conduct



Engage your Employees in a New Way

Convercent's Ethics & Compliance Portal provides a unique digital experience for employees that guides them to the most helpful and engaging information right when they need it. It enables E&C professionals to display their code of conduct and other compliance materials in a user friendly, consumable format that promotes a higher level of understanding and retention of the information. To learn more visit convercent.com

In an excerpt from a recent self-published essay, presidential candidate Elizabeth Warren outlined her plan to break up Big Tech and restore competition.

Point

Big Tech has too much power

Whether to break up America's largest technology companies has become a hotly debated topic in the United States, garnering attention from educators, public companies, and government. The following text is excerpted from presidential hopeful Elizabeth Warren's essay, "Here's how we can break up big tech," which outlines Warren's argument for breaking up the fearsome four.

"Today's big tech companies have too much power — too much power over our economy, our society, and our democracy. They've bulldozed competition, used our private information for profit, and tilted the playing field against everyone else. And in the process, they have hurt small businesses and stifled innovation.

Weak antitrust enforcement has led to a dramatic reduction in competition and innovation in the tech sector. Venture capitalists are now hesitant to fund new startups to compete with these big tech companies because it's so easy for the big companies to either snap up growing competitors or drive them out of business. The number of tech startups has slumped, there are fewer high-growth young firms typical of the tech industry, and first financing rounds for tech startups have declined 22% since 2012.

With fewer competitors entering the market, the big tech companies do not have to compete as aggressively in key areas like protecting our privacy. And some of these companies have grown so powerful that they can bully cities and states into showering them with massive taxpayer handouts in exchange for doing business, and can act—in the words of Mark Zuckerberg—'more like a government than a traditional company.'

My administration would restore competition to the tech sector by taking two major steps:

First, by passing legislation that requires large tech platforms to be designated as 'platform utilities' and broken apart from any participant on that platform.

Companies with an annual global revenue of $25 billion or more and that offer to the public an online marketplace, an exchange, or a platform for connecting third parties would be designated as 'platform utilities.' These companies would be prohibited from owning both the platform utility and any participants on that platform. Platform utilities would be required to meet a standard of fair, reasonable, and nondiscriminatory dealing with users. Platform utilities would not be allowed to transfer or share data with third parties.

For smaller companies (those with annual global revenue of between $90 million and $25 billion), their platform utilities would be required to meet the same standard of fair, reasonable, and nondiscriminatory dealing with users, but would not be required to structurally separate from any participant on the platform.

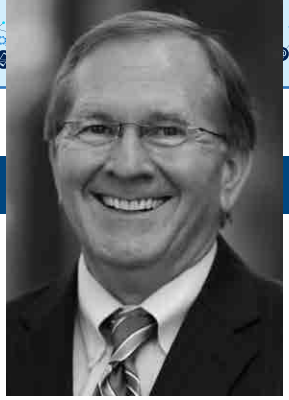
To enforce these new requirements, federal regulators, State Attorneys General, or injured private parties would have the right to sue a platform utility to enjoin any conduct that violates these requirements, to disgorge any ill-gotten gains, and to be paid for losses and damages. A company found to violate these requirements would also have to pay a fine of 5 percent of annual revenue. Amazon Marketplace, Google's ad exchange, and Google Search would be platform utilities under this law. Therefore, Amazon Marketplace and Basics, and Google's ad exchange and businesses on the exchange would be split apart. Google Search would have to be spun off as well.

Second, my administration would appoint regulators committed to reversing illegal and anti-competitive tech mergers. Current antitrust laws empower federal regulators to break up mergers that reduce competition. I will appoint regulators who are committed to using existing tools to unwind anti-competitive mergers, including: Amazon: Whole Foods, Zappos; Facebook: WhatsApp, Instagram; and Google: Waze, Nest, and DoubleClick. Unwinding these mergers will promote healthy competition in the market—which will put pressure on big tech companies to be more responsive to user concerns, including about privacy.

Healthy competition can solve a lot of problems. The steps I'm proposing today will allow existing big tech companies to keep offering customer-friendly services, while promoting competition, stimulating innovation in the tech sector, and ensuring that America continues to lead the world in producing cutting-edge tech companies. It's how we protect the future of the Internet." ■

Counterpoint

Mark Jamison of the American Enterprise Institute discusses why breaking up Big Tech would be bad for consumers, startups, and more.



Consumers embrace Big Tech

Imagine someone saying that we should break up India because it has too many people or the New England Patriots football team because it wins too often. Or that we should limit the number of votes that incumbent political candidates can receive so that lesser candidates have a fair chance? Or that we cap the salaries of professors at Ivy League universities so that universities with fewer financial resources can compete for top talent?

These are obviously bad ideas. Yet, they parallel arguments made to break up the Big Tech companies: Breakup proponents say the companies are too big and too successful, their customers are captured by brand names, and they have so much data and money that rivals can't compete.

Let's start with the bigness and success issues. When did making customers happy become a bad thing? People choose to use Big Tech's services. They choose Google 75 percent to 90 percent of the time worldwide. Google isn't diverting searches from Bing or DuckDuckGo. Nor is Google even offering the search services that Yelp or Facebook provide.

And, according to an article on eMarketer, U.S. online shoppers prefer Amazon over all others 45 percent of the time. Amazon isn't suppressing Wal-Mart or eBay; nor is it controlling customers: U.S. customers provide Amazon with 206.1 million unique visitors per month but 109.4 million visit eBay.

Some of the market share data that breakup proponents and the media report is misleading. Recently the *Wall Street Journal* tried to make the case that Facebook is dominant by reporting that 95 percent of young adults on the internet use Facebook. But Pew Research says 35 percent of U.S. teens use Snapchat more than any other social media, and 32 percent use YouTube more than any other. Facebook and Instagram together are most used by only 25 percent of U.S. teens. So Facebook is, at best, number three for this important demographic.

Now let's look at the value of these companies' brands. Are the differences real or imagined? eBay is a well-known rival to Amazon—attracting 2 billion transactions per day worldwide, notes Parade.com, compared to Amazon's peak of 26.5 million transactions on Cyber Monday in 2018, according to Business Insider. But while eBay is significant, 206.1 million U.S. customers choose Amazon over eBay each month. What would happen to these customers if a breakup or regulation forced Amazon to be more like eBay (which is what Elizabeth Warren proposes)? Denying U.S. consumers the Amazon they love would cost them about $167 billion per year.

Most proposals to breakup Facebook suggest spinning off Instagram. But Facebook made Instagram successful: Facebook paid $1 billion for Instagram in 2012, according to Engadget.com, and in seven years made it worth about $100 billion, according to an article on Investopedia. Who loses if Instagram goes back to its old ways? About 75 percent of U.S. businesses plan to use Instagram in 2020, notes an article on Hootsuite, and 1 billion people use it every month. Where would these businesses and users go if Instagram declines? Facebook?

What if the government forced a decline in Google so that it was more like its two nearest competitors, Bing and Yahoo!? Considering the differences between their user satisfaction scores and how much users value search, knocking Google down would cost consumers about $700 billion per year.

Lastly, let's look at how financial resources drive startups and innovation. When investors decide whether to put money into tech, they consider the profit potential of the winners and the possible financial losses for the about 90 percent of tech startups that don't make it. The 90 percent number means that the most profitable tech companies need profits that are more than nine times the losses of the biggest financial failures.

So winners not only must make up for their own start-up costs, they must make up for the start-ups that ultimately fail. If the message from the government is that high profits won't be tolerated, there will be less money for startups.

Breaking up tech companies is a solution in search of a problem. Big-is-bad may have political appeal, but voters would lose in the end. ■

Mark Jamison is a visiting scholar at the American Enterprise Institute, where he works on how technology affects the economy, and on telecommunications and Federal Communications Commission issues.