COMPLIANCE WEEK

Data privacy activist Max Schrems at Compliance Week Europe

PRIVACY PAINS

Establishing best practices isn't easy considering flaws with the EU's GDPR, insufficient U.S. regulation, and Big Data feeding the beast.

SPECIAL REPORT: DATA PRIVACY

Dave Lefort
Editor in Chief

dave.lefort@complianceweek.com

Dave Lefort is an award-winning journalist with an extensive background in content management, digital strategy, and data analytics. He spent nearly two decades in digital leadership roles at The Boston Globe and ESPN.com.

{NOTE FROM THE EDITOR}

GDPR, Brexit keep compliance on its toes

Whenever compliance practitioners gather, the conversation usually centers around shared problems, collaborative solutions, and an overall "we're all in this together" vibe.

I was definitely feeling that vibe at the Compliance Week Europe conference in Amsterdam last month, but there was another sentiment that was equally pervasive among attendees: a stunning lack of clarity around two of the biggest issues facing the compliance community.

The 6-month-old General Data Protection Regulation (GDPR) and Britain's upcoming divorce from the European Union both have a tremendous impact on European compliance, but strategizing solutions around either one has proven to be difficult due to a lack of guidance and, in the case of Brexit, just plain chaos.

On GDPR, we brought in the vice chairman of the European Data Protection Board, whose message was, essentially, that they're still trying to figure out how this regulation is going to work in practice. For those looking for answers (and there were many), that wasn't exactly reassuring.

Interpretation and enforcement of the regulation is up to the data protection authorities in each of the 28 nations in the European Union, and no real precedents have been set that could indicate which aspects of GDPR are more likely to be enforced most stringently in which areas.

We also heard from a prominent data privacy activist, who said he expects the level of enforcement throughout Europe to be uneven and unpredictable. He called out European regulators for being lax on data privacy in the past and questioned whether GDPR would have the teeth many predicted it would when it was enacted.

And then there's Brexit, the soap opera that provides endless fodder for the British tabloids but almost no clarity for those tasked with making sure companies are in compliance with the rules that will govern the new relationship between Britain and the European Union starting next March.

British Prime Minister Theresa May and her cabinet presented their Brexit plan to the European Union, which approved the deal in late November. The fun, however, is just beginning, as the plan in its current form seems to have little chance of being OK'd by the U.K. Parliament, and EU leaders have no appetite for making adjustments. From overseas, it seems to be a game of chicken between politicians. From the front-row vantage point of the U.K. compliance community, it's nothing short of a nightmare.

One CCO at Compliance Week Europe put it bluntly: "We've made plans for every possible Brexit outcome, but we're not crazy enough to start implementing anything until we know for sure which way this is going."

For a group whose job it is to ensure rules are followed and who appreciates stability and transparency, compliance officers in Europe find themselves blindfolded by uncertainty and in need of a flexible game plan on a pair of issues that will have a huge impact on how they do their jobs in the foreseeable future. ■

The coming wave of DATA PRIVACY compliance challenges

International and domestic legislators and regulators threaten an end of the self-regulation of consumer data. **Joe Mont** has more.

Forget Bitcoin. The most common and profitable "virtual currency" today is personal data.

It is no small paradox that social media users—and there are billions of them globally—are willing to share the most intimate details of their life online, yet balk at the suggestion that those details will likely be shared and sold. The economic reality, however, is that data collection and analytics is, in large part, how giant tech companies have continued to grow and prosper.

The regulatory free ride of monetized data collection, however, may be coming to an end.

The shot across the bow was the May 2018 implementation of the European Union's General Data Protection Regulation.

Designed to bring EU data protection laws into the digital age, GDPR harmonized existing rules among member states to enhance consumer protections. It allows consumers and others to know what data a business possesses on them, empowering them with the right to demand its deletion.

Although the expansive nature of GDPR makes it a de facto global standard, domestic legislation and regulation is increasingly likely in the United States. States are also jumping into the fray, notably California with the Consumer Privacy Act of 2018, legislation many view as "GDPR-lite."

"I think there is a high chance that people realize that the days of the wild, wild West are over. There need to be some guardrails," said Sen. Mark Warner (D-Va.) at a September Senate Intelligence Committee hearing on digital privacy.

"A national standard for privacy rules of the road is needed to protect consumers," added Sen. John Thune (R-S.D.).

The catalyst for legislative interest is hardly surprising. Decades of self-regulation is proving to be no longer tenable as data collection efforts become ubiquitous and more brazen.

There are nearly daily news headlines that underscore how things can go very wrong when it comes to securing personal data.

Target, back in 2012, drew fire when its data-driven marketing efforts accidently broke the news of a teenager's pregnancy to her family. A 2017 Equifax data breach exposed the personal and financial information of 143 million Americans. In April, LGBT dating site Grindr was accused of sharing the personal information—including, allegedly, HIV status—of many of its approximately 3.6 million active daily users without their informed consent.

More recently, there were revelations that political intelligence firm Cambridge Analytica had illicitly acquired access to the personal data of millions of unwitting Facebook users.

Yet another Facebook breach, reported in September, saw the compromise of 30 million user accounts. Early November brought reports that hackers stole the private messages of more than 81,000 Facebook accounts, selling them for 10 cents per account on the "dark Web." In October, it was revealed that Google waited six months before notifying the public of a data breach that exposed the private information of nearly 500,000 users of the Google+ social media network.

These incidents, although noteworthy, are far from isolated. Nearly 64 percent of Americans have experienced a "significant data breach" of their personal data, claims a recent survey by the Pew Research Centre.

"More legislators and business leaders are stepping forward to say the time for overarching, federal-level privacy legislation in the U.S. has come," Dr. Andrea Jelinek, chair of the European Data Protection Board, told a Senate panel in October. "If we do not modify the rules of the data processing game with legislative initiatives, it will turn into a losing game for the economy, society, and for each individual."

"Businesses have started coming around too, not just because they need to comply with the GDPR, but because they see that their clients and employees alike expect their personal data to be treated in a safe manner," she added.

Breaches aside, legislators will also need to address what companies do with the data willfully placed in their care. Ongoing scrutiny hasn't necessarily chastened tech companies, many of whom continue to push the boundaries of their collection efforts.

Google, for example, has a patent on using in-home devices to monitor refrigerator access to analyze household eating patterns and determine the emotional state of the home's occupants based on voice and facial expressions, Alastair Mactaggart, chairman of Californians for Consumer Privacy, an architect of that state's new data privacy law, told a recent Senate Commerce Committee panel. With the patent, Google also seeks to track whether alcohol is consumed; whether there is smoking; whether teeth are brushed; and if foul language is used.

Advertisers are also pioneering "geofences" that can track and send advertisements to smartphones crossing a selected area. "As a result, through no overt action of a consumer, the companies know who is in rehab, who goes to AA, who just got an abortion, what your religion is, and whether you have a drug problem," Mactaggart said. "That information can be sold, and resold, simply because you have a mobile phone."

In the stories in this special report, we look at the data privacy rules, laws, and frameworks that are emerging—internationally and domestically—and what compliance challenges they pose. ■

ALSO IN THIS REPORT

Elements of a best-in-class data privacy program

Struggling to keep up with privacy regs? Stop the guesswork and follow these best practices for thinking strategically about how privacy practices fit into the overall business strategy. **Jaclyn Jaeger** has more.

As data privacy laws and regulations proliferate around the world, it's imperative that companies resist the urge to engage in a game of data-privacy whack-a-mole—attacking each one individually, until another one pops up.

According to the United National Conference on Trade and Development, 107 countries have in place some form of legislation to secure the protection of data and privacy, and many others have similar legislation in the works. Attempting to comply with each one without taking a holistic approach to all is not only a risky undertaking, but also has the potential to drastically increase data privacy compliance costs.

"Where you have some overlap between those various requirements, there are absolutely opportunities for efficiency and to streamline the way that things can be implemented," says Orson Lucas, a managing director and co-leader for privacy services in the cyber-security practice at KPMG. Take, for example, the handling of requests received from data subjects under both the EU's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act, both of which give consumers greater legal rights to demand that specific data be deleted from an online enterprise's databases. "With some tuning, you can often leverage the same technologies and a lot of the same processes to help fulfill both of those," Lucas says.

Recent data reveals that the struggle is real. According to a Thomson Reuters survey on data-privacy compliance, 44 percent of 1,000 data privacy professionals globally said they are presently failing to adhere to data privacy regulations, and 47 percent said they're struggling to keep up-to-date or are falling further behind.

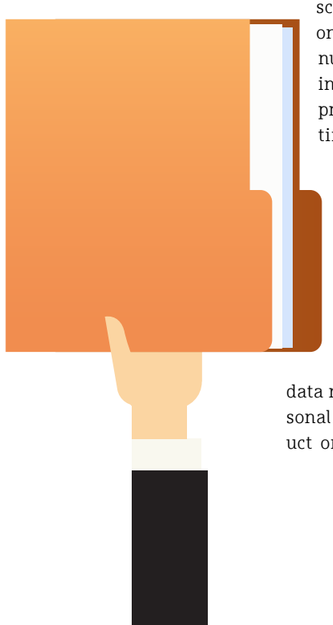
At a high level, implementing a robust data privacy compliance program is not just about satisfying regulatory obligations, but more broadly thinking strategically about how privacy practices fit into the company or organization's overall business strategy and making it a core part of the business model. "It's important at the outset to think about where the business wants to end up on the data privacy maturity scale to ensure alignment between risk tolerance and investment and leverage maturity targets to drive focus on privacy efforts," Lucas says.

Below are key elements implemented by leading companies as part of a best-in-class data privacy compliance program.

Map your data

Data map exercises—and specifically keeping up with the ever-changing products, service offerings, and systems of a global company—is one of the biggest undertakings to being, and staying, compliant with data privacy laws, like the GDPR. A data map, like any other map, will prevent you from getting lost, but only if you know how to properly follow it. In the context of data privacy, the elements of a data map include an assessment of what data the company collects that's subject to data privacy laws; how the data is processed; where it is stored; how the data is used; and how long it is retained.

To better understand just how monumental a task this can be, consider Mastercard's approach. Because the global payments and technology company authorizes, clears, and schedules card transactions on behalf of banks, those card numbers need to be protected in accordance with global data protection laws. At the same time, however, certain business lines within Mastercard collect and process more data than others—in the context of a marketing initiative or loyalty rewards program, for example.



To tackle this compliance hurdle, each business line was asked to provide a data map, documenting all the personal data it handles for each product or service. "We now have 122 data maps covering all our products and services and systems, which double up as our records of processing, should a [data protection authority] ever ask us about how we handle data," Loretta Marshall, senior regional counsel of privacy and data protection at Mastercard, explained on a recent Webinar. Mastercard also created an automated data inventory to track in real-time what data it has, on which platform it is stored, and what restrictions exist for each data point, she said.

Get a grip on data privacy obligations

Companies on the lower level of the maturity scale tend to have, at a minimum, a data privacy model that is documented, defensible, and repeatable—processes and procedures they can show regulators, should they come knocking. For some companies, once they meet those data privacy obligations, however, they stop there.

In contrast, companies further along the maturity curve tend to approach privacy as a business enabler. "Privacy done right can help to not only fulfil and satisfy your compliance and your risk-management objectives, but also better position you with consumers—both as a competitive differentiator and to enrich the relationships you have with your customers," Lucas says. "Approaching privacy in that way is not different from, but rather intertwined with, the need to develop a robust privacy program," he says.

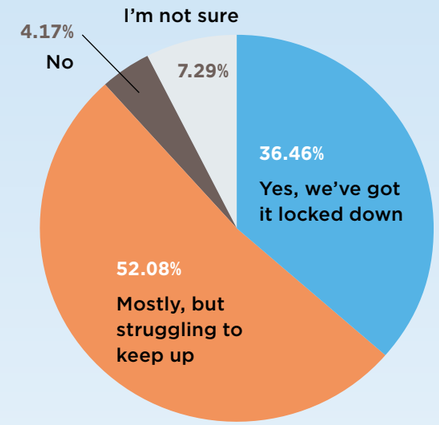
> "We now have 122 data maps covering all our products and services and systems, which double up as our records of processing, should a [data protection authority] ever ask us about how we handle data."
>
> Loretta Marshall, Senior Regional Counsel of Privacy and Data Protection, Mastercard

Privacy-by-design is one such best practice—and, in fact, an express legal requirement under the GDPR, mandating that data protection and privacy controls be considered from the outset. Going back to the example of Mastercard, the company has developed a checklist to help business lines make decisions about what data they collect and process. As part of that checklist, business lines are encouraged to think about how long they need the data; who has access to it; and

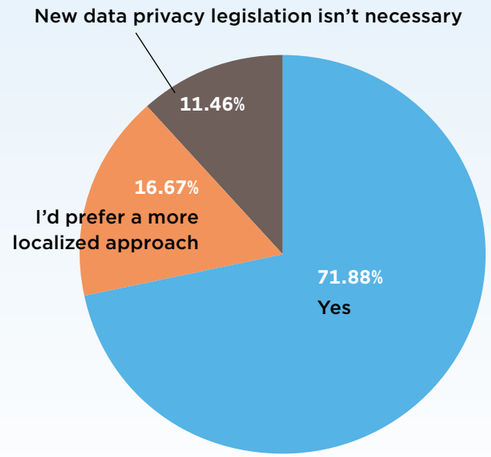
{CW'S DATA PRIVACY SURVEY}

In partnership with RSA, CW asked more than 100 compliance professionals involved with data protection at their companies 15 questions related to their privacy programs.

Is your data privacy program in compliance with state, national, and international (if applicable) regulations?



Are you in favor of national legislation governing data privacy in the United States?



in which systems the data is stored. They are also encouraged to think about best practices around data minimization, security measures, de-identifying data where possible, and instances in which card numbers can be replaced with tokenization.

Mastercard's marketing business line, specifically, is encouraged to think about what is meant by embedding privacy into the design of marketing products and services to anticipate and prevent potential privacy threats, Marshall said. They are encouraged to think about what data they really need, or whether the product or service can function without a particular data field.

Assign ownership

A data privacy program without clear ownership of risk will fail. For companies that fall under the umbrella of the GDPR, appointing a Data Protection Officer (DPO) isn't enough. The DPO acts as a single source of contact for the relevant supervising authority and is tasked with overseeing compliance with the GDPR, specifically, but that individual still needs to be steered in the right direction.

That is where a steering committee comes into play. From a global data privacy perspective, best practice is to have in place a steering committee with representatives from business units most heavily impacted by privacy obligations. In addition to IT, this steering committee should include reps from privacy, risk and compliance, legal, HR, marketing, and other functions.

The role of internal audit

"For privacy, internal audit is a critical third-line function," Lucas says. "For mature organizations, internal audit actively participates as a part of the cross-functional privacy governance steering committee, actively engaging in consultative input on governance and to get early visibility into risks to shape and streamline the audit plan."

"While there is no prescriptive 'right answer' about internal audit cadence in the privacy space, many organizations are taking an iterative approach, using the initial audit to drive out compliance posture and gaps and the output of that to drive internal audit and ongoing monitoring frequency," Lucas adds. "Regardless, regular communication between internal audit, those with operational responsibility for privacy program design and management, and business stakeholders is a critical success factor to the development and monitoring of a better practice privacy program."

Board and senior-leadership support is key

For any data privacy and data protection compliance program to function properly, ongoing support at the board level and steering committee level is crucial. "I can't emphasize that enough," Lucas says.

Getting (and keeping) buy-in from senior leadership helps to ensure that data privacy and data protection initiatives are not only prioritized through the lens of other business objectives and risk appetite, but also ensure ongoing resources and funding for compliance efforts—such as for the necessary training of employees and implementing new technologies.

According to the Thomson Reuters survey, 75 percent of respondents at global organizations said upper management and boards struggle to understand the implications of their data privacy obligations. Such a lack of understanding can seriously hinder data protection and compliance professionals from getting senior-level buy-in if they don't properly understand the necessity of the investment.

This finding speaks to the importance of speaking the business language of senior leadership, such as the potential for exponential fines. The one that should strike the most fear into companies is the GDPR, with fines up to four percent of total annual global revenue or €20 million (U.S. $25 million), whichever is higher. The avoidance of reputational and legal risk and privacy as a business enabler are other ways to speak the business language of senior leadership.

Mind the costs

Senior-leadership buy-in is also important when considering

> "For privacy, internal audit is a critical third-line function. For mature organizations, internal audit actively participates as a part of the cross-functional privacy governance steering committee, actively engaging in consultative input on governance and to get early visibility into risks to shape and streamline the audit plan."
>
> Orson Lucas, Managing Director, Cyber-Security Practice, KPMG

the cost of data privacy compliance. According to the Thomson Reuters survey, the total global costs of data protection issues cost organizations an average of U.S. $1.4 million annually. Data privacy professionals in the United States reported the highest costs of any country, at $2.1 million, followed by organizations in Singapore (U.S. $1.6 million), and organizations in Hong Kong (U.S. $1.5 million).

Annual global costs of data protection issues for organizations in France and the United Kingdom each showed costs of U.S. $1.2 million, while organizations in Canada and Germany each showed costs of U.S. $1.1 million.

Data privacy training

"Training represents the final mile of mobilizing your workforce to be part of your data security strategy," says Mark Dorosz, vice president of compliance learning at Interactive Services, a provider of online compliance training. "You can have the best data privacy control framework, but if your people aren't skilled to adhere to the process and know when to take action, it's not going to work."

The best way to deliver impactful training is by making content role-specific: "Relevance drives engagement," Dorosz says. "Choose data privacy topics based on employees' real-life responsibilities."

To make training completion easier to manage at an enterprise level, "aim for one enterprise training program per week that every employee must complete, regardless of role," Dorosz says. "You can even brand it 'Data Privacy Week.' Beyond that, run awareness campaigns throughout the year that touch the physical environment, with workplace posters and elevator bank commercials through to banner ads on you company's intranet site, and spotlight videos featuring real-life employees contributing your data privacy strategy."

All told, whether needing to satisfy state, national, or international data privacy laws, the best approach is a holistic approach, and that starts with a cultural shift of looking at privacy as a business advantage—not a regulatory obligation. Take it step-by-step: Establish a cross-functional steering committee; get a grip on the data, with input from reps on the steering committee; and then be prepared to show (not just tell) senior leadership the value of the company's privacy obligations.

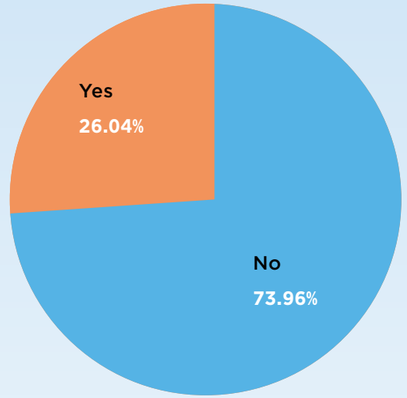
From there, train employees who handle sensitive data to understand their responsibilities—and the importance of those responsibilities.

Finally, audit and monitor the progress of your data privacy compliance program. Practice may not make perfect, but it definitely makes progress. ■

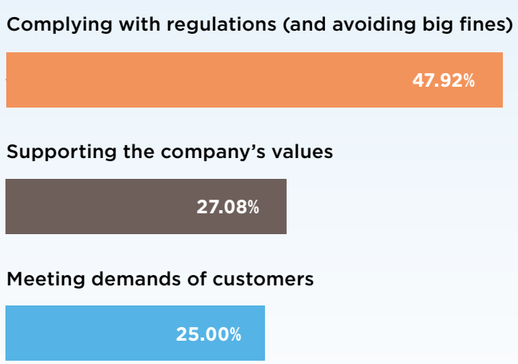
{CW'S DATA PRIVACY SURVEY}

In partnership with RSA, CW asked more than 100 compliance professionals involved with data protection at their companies 15 questions related to their privacy programs.

Do you feel like you have the necessary level of commitment (both financially and philosophically) from the board and C-suite on data privacy?



What's the best argument for a robust data protection program?



FAQ

A glimpse at current & possible U.S. privacy protections

What U.S. laws and regulations are already on the books?

The issue isn't that the United States doesn't already have rules governing data privacy, but rather that those existing rules are either narrow (in terms of audience or industry) and often focus more on breaches than the misuse or misapplication of data.

The most controversial regulation isn't domestic at all. Europe's General Data Protection Regulation (GDPR), within its 99 articles, places demands on U.S. companies that do business with (and collect data from) EU residents.

It inspired California's state-crafted law, the Consumer Privacy Act of 2018. Similar to GDPR, California customers will have the right to demand that specific data be deleted from an online enterprise's databases.

The legislation will: grant consumers the right to request deletion of personal information; give consumers the right to know what personal information is shared or sold to third parties; and authorize consumers to opt out of the sale of personal information by a business.

The Children's Online Privacy Protection Act, crafted and enforced by the Federal Trade Commission, requires commercial Websites or online services to obtain parental consent before collecting personal information from children under 13. The Health Insurance Portability and Accountability Act, passed in 1996, imposes data privacy and security provisions for safeguarding medical information.

The Gramm-Leach-Bliley Act requires that banks and other financial institutions send annual privacy notices to customers that describe how non-public personal information is shared. These notices must describe the privacy practices of financial institutions, including whether and how they share customers' nonpublic personal information.

What is happening in Congress?

There was a lot of activity in the current, lame duck session of Congress to take up improved data-focused legislation. The question, for now, is whether any of those efforts, informed by committee hearings in both chambers, will move forward, or need to wait for a new session with newly elected officials in 2019.

Among the developments to watch is the successful reelection of Rep. Ro Khanna (D-Calif.). Working with Tim Berners-Lee, the creator of the World Wide Web, Khanna has unveiled an "Internet Bill of Rights," with assurances citizens should have when it comes to consenting to the collection and dissemination of their personal data.

In a separate white paper, Sen. Mark Warner (D-Va.) has outlined data privacy rights that could form the basis of legislation. Notably, he pitched a "fiduciary duty" for those who collect and share personal information.

Sen. Ron Wyden (D-Ore.) has made public the draft of proposed legislation that would require senior executives of companies with more than $1 billion in annual revenue, or data on more than 50 million consumers, to file annual reports with the FTC detailing whether or not they complied with the privacy and data security standards. The bill could include criminal penalties for making false statements in these reports.

Senators Amy Klobuchar (D-Minn.) and John Kennedy (R-La.) introduced legislation that would: give consumers the right to opt-out of data collection and keep their information private by disabling data tracking and collection; and require that terms of service agreements be in plain language.

In September 2017, Equifax announced that hackers had stolen the sensitive personal information of more than 145 million Americans. In response, Sens. Warner and Elizabeth Warren (D-Mass.) introduced the Data Breach Prevention and Compensation Act. It seeks to create an Office of Cyber-security at the FTC tasked with supervision of credit rating agencies, imposing penalties for breaches of consumer data and compromised personal identifying information.

The latest twist on legislation: a bill proposal released by chipset-maker Intel in early November.

"We recognize the need for a legal structure to prevent harmful uses of the technology and to preserve personal privacy so that all individuals embrace new, data-driven technologies," the company said in a statement. "The U.S. needs a law that promotes ethical data stewardship, not one that just attempts to minimize harm."

The proposal builds upon Fair Information Practice Principles from the Organization for Economic Cooperation and Development's "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data."

"The OECD FIPPs are 'the Global Common Language of Privacy' and many of the privacy laws around the world are based on them," Intel says.

The legislative pitch would require that most uses of data will require a risk/benefit analysis that will restrict an organization from using data in a way that creates undue risk for individuals. Organizations must also state their purposes for collecting and processing data, "described narrowly and specifically," and adopt "reasonable measures to protect personal data."

The FTC would be tasked with enforcement with increased autonomy, authority, and responsibilities.

What is the Trump administration doing?

Since taking office, President Trump has periodically called in tech leaders for "listening sessions" to debate potential ways the White House could, or should, develop a policy for consumer data privacy. Among the resulting, in-play initiatives is an expanded framework for consumer privacy by the National Institute of Standards and Technology.

NIST, a non-regulatory agency of the Department of Commerce, provides and oversees one of the nation's most widely-used cyber-security frameworks for both private and public entities. In September, it launched a collaborative project "to develop a voluntary privacy framework to help organizations manage risk."

The envisioned privacy framework will provide an enterprise-level approach that helps organizations "prioritize strategies for flexible and effective privacy protection solutions."

"NIST's goal is to develop a framework that will bridge the gaps between privacy professionals and senior executives, so that organizations can respond effectively to these challenges without stifling innovation," NIST Senior Privacy Policy Advisor Naomi Lefkovitz said.

Parallel with the NIST initiative, the Commerce Department's National Telecommunications and Information Administration (NTIA) is developing "a domestic legal and policy approach for consumer privacy."

It recently issued a request for comments on a proposed approach to consumer data privacy, "Developing the Administration's Approach to Consumer Privacy." The deadline for that feedback was Nov. 9.

With the goal of publishing "high-level principles" for building better privacy protections, the NTIA had sought industry feedback on the following assumptions: Organizations should be transparent about how they collect, use, share, and store users' personal information; users should be able to exercise control over the personal information they provide to organizations; the collection, use, storage, and sharing of personal data should be reasonably minimized in a manner proportional to the scope of privacy risks; and organizations should take steps to manage the risk of disclosure or harmful uses of data.

What are states doing?

State attorneys general are flexing their muscles regarding data breaches and what they view as improper uses of data.

In June, New Jersey Attorney General Gurbir Grewal announced plans to create a new civil enforcement unit, known as the Data Privacy & Cybersecurity Section, within his office. It will enforce laws that protect New Jersey residents' data privacy and cyber-security by bringing civil actions against violators. Another role of the Section will be to provide legal advice to the State's Executive Branch agencies on compliance with cyber-related state and federal laws and standards.

Among other projects, it will assume responsibility for the Office's ongoing investigation into Facebook's transfer of personal information to Cambridge Analytica.

Legislatively, in addition to a plethora of data breach notification laws, Illinois enacted the Biometric Information Privacy Act, a restriction on face recognition, thumbprint scans, and other identifiers. Facebook currently faces a class-action lawsuit on its use of this technology, without user consent, for "tag suggestions." Texas and Washington also have biometric identifier laws on the books.

Besides enacting the Consumer Privacy Act of 2018, California passed the nation's first law covering the Internet of Things. Starting Jan. 1, 2020, any company selling an internet-connected device must ensure "reasonable" security features that prevent unauthorized access and data disclosure.

Colorado has a new law that requires covered entities to: develop and maintain written policies on the disposal of personal information and "implement reasonable security procedures and practices commensurate with the sensitivity of personal data processed as well as the size and complexity of the entity."

Earlier this year, Vermont enacted a law that imposes controls on data brokers. It requires data brokers to register with the state on an annual basis. Those registrations must include disclosures on whether, and how, consumers may opt out of having their personal data used. The state attorney general is tasked with enforcement of the new law.

Tech companies push for national privacy framework

Commonalities among tech companies, when it comes to U.S. data privacy legislation, include a single-standard approach, elevating the FTC, and mandating a risk-based methodology. **Joe Mont** reports.

With a few exceptions, companies that broker in consumer data are sticking close to the same script when it comes to the potential for regulatory demands in the United States.

Amid headline-grabbing breaches and exposés on shady data sharing practices, technology giants—Google, Facebook, Apple, and Amazon among them—seem resigned to the fact that national data privacy laws and regulations are in the offing.

While they await congressional action on that issue, a strategy has emerged: Let trade associations tackle much of the public-facing policy pushing; and support federal legislation to the degree it can reduce the confusion and compliance burden of state-by-state regulation.

In testimony, Web posts, and correspondence, there also seems nearly universal agreement that the Federal Trade Commission should continue to serve as the lead U.S. regulator for data privacy. The sincerity of that demand, however, is undermined by objections to giving that agency expanded tools, enforcement authority, and a less hamstrung ability to fine companies.

Some corporate leaders are more outspoken than others. Apple CEO Tim Cook recently described privacy as "a fundamental human right." Unlike others who see it as too prescriptive and restrictive, he said that his company supports a U.S. data protection law that mirrors Europe's General Data Protection Regulation.

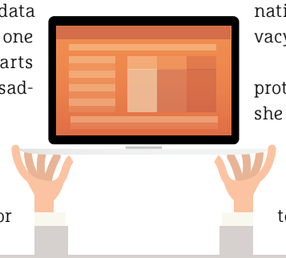
Microsoft CEO Satya Nadella has similarly urged the promulgation of national privacy legislation.

"We will respect your local privacy laws and fight for legal protection of your privacy," he wrote on Microsoft's Website, addressing the company's data privacy policies.

Brendan Eich, former CEO of Mozilla who now holds that title at Brave Software, lobbied members of the Senate Commerce Committee for "GDPR-like standards" in the United States.

"I view GDPR as a great leveler," he wrote in a letter to senators. "[It] establishes the conditions that can allow young, innovative companies [like ours] to flourish."

As regulators broaden their enforcement of the new rules in Europe, the GDPR's principle of "purpose limitation" will prevent dominant platforms from using data that they have collected for one purpose at one end of their business to the benefit of other parts of their business in a way that currently disadvantages new entrants.



"In general, platform giants will need 'opt-in' consent for each purpose for which they want to use consumers' data," he explained. "This will create a breathing space for new entrants to emerge."

There is also an international angle to consider for domestic lawmakers.

In the coming months and years, common GDPR-like standards for commercial use of consumers' personal data will apply in the EU, Britain (post-EU), Japan, India, Brazil, South Korea, Argentina, and China, for civil and commercial use of personal data. "A common standard reduces friction and uncertainty, allowing companies from these countries to operate and innovate together with greater efficiency," he wrote.

During a September hearing convened by the Senate Commerce Committee, top technology and communications firms were called upon to testify on data privacy.

Rachel Welch, SVP for policy and external affairs at Charter Communications, was among those supporting "a single national standard that protects consumers' online privacy regardless of where they live, work, or travel."

"Whether a consumer's information is adequately protected should not differ based on which state he or she is logging in from," she said. "A patchwork of state laws would be confusing for consumers, difficult for businesses to implement, and hinder continued innovation on the internet—which is a borderless technology."

A view from beyond the tech giants

Another bellwether of how companies are responding to the prospect of national data privacy regulation can be found in public comments responding to the National Telecommunications and Information Administration's development of "a domestic legal and policy approach." NTIA, an agency of the Commerce Department, recently issued a Request for Comments on a proposed approach to consumer data privacy, "Developing the Administration's Approach to Consumer Privacy." The deadline was Nov. 9; the comments were made public on Nov. 13.

The Credit Union National Association was among the groups weighing in on the NTIA process. Its priorities are:

- A flexible, scalable standard;
- A notification regime requiring timely notice to impacted consumers, law enforcement, and applicable regulators when there is a reasonable risk that a breach of unencrypted personal information exposes consumers to identity theft or other financial harm;
- Consistent, exclusive enforcement of the new data security and notification national standard by the Federal Trade Commission (FTC) and state attorneys general; and
- "Clear preemption of the existing patchwork of often conflicting and contradictory state laws for all entities that follow this national data security and notification standard."

"The compliance costs are particularly heavy for smaller operators with less discretionary spending," the Association noted. The Computer & Communications Industry Association asked that policies include safe harbors and flexibility for firms to evolve with changing technology. "Good policy has the potential of setting a national baseline for privacy across sectors and supporting innovation, while allowing companies' flexibility in how they deliver a level of privacy consumers expect based on the sensitivity of particular data," CCIA President & CEO Ed Black says.

Public Knowledge, a consumer advocacy group, said privacy regimes should, "at a minimum, account for risks beyond traditional harms, such as financial loss, to include damages such as reputational harm and undermining public trust." It urged the NTIA to consider "the full panoply of risks" that may arise from misuse of personal data." "Although the NTIA articulates a number of important outcomes and high-level goals for federal action, notably absent are outcomes and goals around fairness, consumer protection, and equal opportunity," says Allie Bohm, NTIA policy counsel. "The proposal also leans too heavily on a risk-based approach and on 'reasonableness,' a term that individuals and businesses likely interpret very differently."

With similar concerns, 34 civil rights, consumer, and privacy organizations joined forces to outline concepts "that any meaningful data protection legislation should incorporate at a minimum," including: Privacy protections must "be strong, meaningful, and comprehensive"; data practices must protect civil rights and prevent unlawful discrimination; and governments at all levels should play a role in protecting and enforcing privacy rights.

"The big banks and the big tech companies all say that they want a federal privacy law, but the law that their phalanx of lobbyists seeks isn't designed to protect consumers," said Ed Mierzwinski, senior director for Consumer Programs at U.S. PIRG. "Instead, it's designed to protect their business models that treat consumers as commodities for sale; it fails to guarantee that their secret sauce big data algorithms don't discriminate; it eliminates stronger and innovative state laws forever; and it denies consumers any real, enforceable rights when harmed. We can't allow that."

Conversely, Citizens Against Government Waste President Tom Schatz also submitted that group's recommendations. He made reference to the California Consumer Privacy Act. "The bill, which was rushed through the legislature in a few days, imposes extremely onerous requirements on how companies must store and provide access to consumers' personal information, as well as harsh restrictions on the types of product and service options and discounts companies may offer to their customers," he wrote.

-Joe Mont

Google is among the companies that has published a proposed framework for data-protection legislation on its corporate Website.

"Industry accountability programs and safe harbors can incentivize best practices, particularly in providing more flexible approaches to dealing with evolving technologies," it wrote. "Also, enforcement and remedies should be proportional to the potential harms involved in the violation."

Google pushed back against the extra-territorial application of privacy regulations.

"It unnecessarily hampers the growth of new businesses and creates conflicts of law between jurisdictions," it warned. "Small businesses shouldn't have to worry about running afoul of foreign regulators merely because a few people from another country navigate to their Website or use their service."

As for the trade associations, they are actively promoting various data privacy frameworks with hopes that the tech industry can more effectively shape the regulations to come.

In October, the Information Technology Industry Council released its "Framework to Advance Interoperable Rules (FAIR) on Privacy." Among its members are Apple, Adobe, Amazon, IBM, Twitter, Facebook, Dell, and Dropbox.

"Consumer trust is a key pillar of innovation, and our industry must do everything we can to deepen that trust and meet consumers' expectations when it comes to protecting their privacy and personal data," says Dean Garfield, president and CEO of ITI.

He expects that the document will continue to take shape as his association works "alongside lawmakers and consumers to develop meaningful privacy legislation."

Among the goals, Garfield says, is creating alignment with the privacy protections of other privacy regimes across the globe.

The ITI framework "can serve as a model for governments worldwide and a workable alternative to a patchwork of laws that could create confusion and uncertainty over what protections individuals have," he said.

Companies, it says, should make it clear to consumers how their personal data will be used; how long it will be retained; and whether it may be accessed by or transferred to third parties.

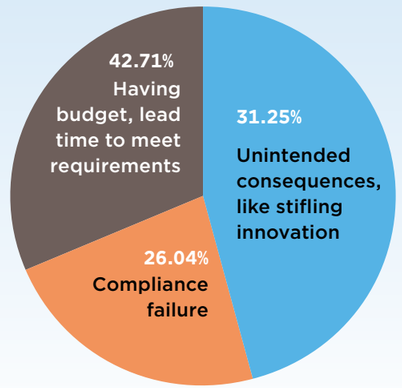
The U.S. Chamber of Commerce has also published a series of "privacy principles." The Chamber, like others, supports a nationwide privacy framework that preempts state regulation.

"Consumers and businesses benefit when there is certainty and consistency with regard to regulations and enforcement of privacy protections," it wrote. "They lose when they have to navigate a confusing and inconsistent patchwork of state laws."

The document also stresses that privacy protections should be "risk-focused and contextual."

{CW'S DATA PRIVACY SURVEY}

What's your biggest worry if the United States adopts a GDPR-like national regulation on data privacy?



"Data controls should match the risk associated with the data and be appropriate for the business environment in which it is used," it says.

Other highlights:

» Privacy laws and regulations should not include mandates that require businesses to use specific technological solutions.
» A national law should include safe harbors and other incentives to encourage "the development of consumer-friendly privacy programs."
» Enforcement provisions should only apply where there is concrete harm to individuals.
» Congress should adopt policies "that promote the free flow of data across international borders."

Also jumping into the fray is the Internet Association, which counts Google, Amazon, eBay, and Facebook among its members.

A U.S. standard should "protect individuals and their personal information through clear notifications, define a harm-based trigger for notification to avoid notice fatigue, and allow companies flexibility in how they notify individuals of unauthorized access to their personal information," it wrote.

A national framework should also be both technology neutral (no specific technology mandates) and sector neutral (applying to online and offline companies alike), it added. ■

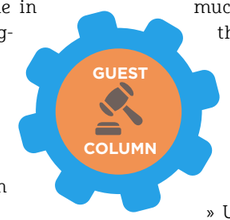
What federal data privacy legislation might look like

By Hilary Wandall, Chief Data Governance Officer, TrustArc

Existing privacy laws create parameters into which a federal privacy mandate will likely fit. More generally, a proposed federal law will likely be more flexible than what we have seen with European-style legislation; and, it is unlikely that the mandate will be as narrowly tailored as that which we've seen in U.S. state-level legislations.

It is likely that a federal law would include a requirement for a comprehensive privacy program at the corporate level, rather than focusing solely on individuals' interactions. In fact, a federal privacy mandate is likely to include the following components:

» **Organizational governance:** A federal mandate will require corporate leadership to set the right tone in terms of understanding responsibility for managing consumer data without doing harm. Leaders must own stewardship of this responsibility and push it down to the rest of the organization.
» **Risk management:** Organizations must understand their privacy priorities and risks and focus their resources on reducing the risk of harm to individuals.
» **Comprehensive policies:** Federal legislation will require that companies handle privacy programmatically by establishing organizational standards to ensure that operational processes recognize and deal with privacy issues on an ongoing, rather than an ad hoc, basis.
» **Training program:** A federal law will likely mandate that organizations have a training program for employees in place. A training program will work to highlight organizational security obligations and how those relate to privacy. One piece of a training program will likely hinge upon breach notifications and how to respond in the event one occurs.



These components, which already exist in enacted privacy laws, will likely compose a significant portion of a federal privacy mandate. As corporations push for privacy laws and states continue to impose fragmented regulations, the need for a federal standard that preempts those laws to some degree is growing ever dire. Every single U.S. state now has its own data breach notification law, and a federal law will include more commonality across state borders to make it less challenging for organizations to manage privacy burdens.

To the extent privacy and digital trade have become significant issues, a lack of a comprehensive standard puts regulators in a tough position. The draft new U.S.-Mexico-Canada trade agreement (USMCA) includes a provision on digital trade, which, among other things, requires the parties to the USMCA to adopt legal frameworks that protect the personal information of users of digital trade. A U.S. federal privacy law will likely take into consideration the critical role the United States plays in international trade dialogues and, as such, the U.S. federal government will surely include language that allows the United States to have a much stronger footing in discussions of privacy issues that involve one or more countries in which American corporations do business.

Though no federal privacy law currently exists, organizational leaders can still take steps to prepare for incoming legislation. When it comes to privacy management, best practices include:

» Understand what data relates to people—customers and employees—as well as the sensitivity risks associated with that information.
» Implement processes that allow organizations to manage data for proper business uses.
» Practice good data governance, security, and data quality assurance.

Regardless of the specifics of a potential federal mandate, leaders should prepare for two major components: Legislation will likely aim to give the United States a strong voice in international trade dialogues, and the law will also lean toward driving the economy and spurring innovation.

The law should cause people to think before they use data in a way that might cause individual or societal harm. By turning their attention to good data use, business leaders can begin to prepare for incoming legislation in a manner that will not only ensure compliance, but that will also build a competitive edge through innovation. A federal mandate is likely on its way, and organizations should start to get ahead of compliance considerations today. ■

Sidley Austin Senior Counsel **Cameron Kerry** explains why the federal government should be in charge of creating one uniform data privacy regulation.

Point

Privacy is the feds' job

America has a checkerboard of laws to protect privacy and data—a matrix of federal and state statutes, common law decisions, and public and private enforcement. This body of laws has real strengths but, as an information Big Bang explodes the data universe, there are growing gaps. It is time for the federal government to set a consistent baseline for privacy protection across the country.

The current checkerboard covers specific sectors or categories of data. These address much of the most sensitive data, such as heath and financial records, genetic information, and data from children. And broad enforcement by the Federal Trade Commission and state attorneys general aimed at breaches of privacy and data security have done much to strengthen business privacy practices.

But today, most of the data we generate through Web searches, social media, e-commerce, and smartphone apps falls outside these sectors and categories. Widespread deployment of connected devices in everything from watches to cars, appliances, and traffic signals (among countless other things) blurs their boundaries. Privacy policies are necessary statements but insufficient to protect individual privacy.

States and even municipalities are stepping in to fill these gaps. Most notably, California adopted a broad law in June establishing detailed requirements for what companies that collect personal data about California residents must disclose and giving consumers greater control over their data. A number of states are considering adopting California's model, and states have adopted varying laws on privacy for data brokers, biometrics, drones, education technology, and other data collection that causes public concern.

That public concern has been magnified by high-profile data breaches, growing consciousness about how much of our data can be tracked, and increased awareness that the European Union has a comprehensive and detailed law on privacy and data protection. These same factors have driven interest in federal law, and Senate Commerce Committee Chairman John Thune opened hearings on legislation this fall by saying "the question is no longer whether we need a federal law to protect consumers' privacy. The question is what shape that law should take."

The push for federal legislation also gets a strong drive from a desire for a federal baseline that can preempt state laws. This makes a great deal of sense.

Only the federal government can fill enough of the gaps in the current matrix and harmonize regimes in a comprehensive way. State law is necessarily piecemeal.

Only the federal government can protect all Americans. Consider the example of state data breach notification laws, which have had significant impact on information security. California adopted the first such law in 2002; earlier this year, Alabama became the 50th state to adopt a breach notification law. People in Alabama should not have to wait 16 years for comprehensive privacy protection; nor should those in other states have to wait 5 or 10 years.

For businesses, a federal law that spells out their obligations and people's privacy rights is an opportunity to establish privacy expectations that will be consistent across the country, avoiding a patchwork of state laws that vary, overlap, or conflict and increasing consumer protection and trust in new technologies without stifling innovation. This is why broad-based business organizations like the Business Roundtable and U.S. Chamber of Commerce, as well as technology trade associations and a growing number of individual companies, have endorsed the passage of federal legislation. Their proposals have included individual rights, such as access to one's data and the ability to correct it—ideas that would have been non-starters for businesses not long ago.

A federal law can be a win-win solution, a grand bargain of strong protection in return for federal preemption. That's a win for business, a win for privacy advocates, and a win for consumers. ■

Cameron Kerry is senior counsel at Sidley Austin and former general cunsel and acting secretary at the U.S. Department of Commerce.

Counterpoint

Common Sense Media Founder and CEO **James Steyer** lays out the three key reasons why individual state privacy laws would trump a federal mandate.

States should steer data privacy

The American system of online privacy protection is broken. That is bad for adult consumers—and even worse for kids. As a parent and an educator, that terrifies me.

The genius of the American system of government is that it contains the solutions that we need to address this problem—in the states and territories. Our states have developed powerful, complex tools to protect consumers whose rights are being violated. Why states and not the federal government? There are three key reasons.

» First, the federal government has, despite decades of concerns, not even tried to lead on addressing privacy issues online (except for narrow issues such as protecting health information, or young children on certain sites and services.) The federal government's track record has been so bad that it fell to the European Union to pass the world's first broadly based law protecting consumer privacy online. The federal government's lack of interest on real privacy protections seems likely to continue. There are only a handful of stalwart privacy advocates on the Hill. The major tech companies are powerful lobbies in Washington—and they are already calling for a federal law specifically designed to preempt the basic protections in California's new privacy law, the California Consumer Protection Act (CCPA). That is a bad-faith effort.

» Second, the states are the right place to protect consumer privacy, because they have always been the first line of defense against consumer scams and unfair business practices. That is their job. State tort law has traditionally been the first line of defense for protecting the privacy of our homes and persons. If your house was intruded upon, if your personal information was maliciously exposed, or if your image or identity was stolen, you could turn to your state and its tort law. States are uniquely powerful in protecting consumer privacy.

» Finally, states must take the lead on protecting our privacy online because they can match the speed and innovation of technology companies. Look at the response to data breaches; while the federal government has failed to act (even in the face of massive Equifax breaches affecting over 140 million consumers), all 50 states passed laws cracking down on data breaches, providing relief to consumers. It is the same with student privacy; as a whole generation of educational technology began to surveil students, it fell to the states to pass laws protecting student privacy.

A major reason that the states can innovate is because State Departments of Justice have incredible regulatory, prosecution, and law enforcement capabilities. These are typically strong pro-consumer agencies—taking the lead on everything from tobacco to opiods and social media—that are directly accountable to voters.

These DOJs and Attorneys General are increasingly focused on online consumer protection, as citizens have decried the federal government's inaction and incompetence. University of Maryland Francis King Carey School of Law Professor Danielle Citron noted that "state attorneys general have been nimble privacy enforcement pioneers, a role that for practical and political reasons would be difficult for federal agencies to replicate. Because attorneys general do not have to wrestle with the politics of agency commissioners or deal with layers of bureaucracy, they can move quickly on privacy and data security initiatives. Career staff have developed specialties and expertise growing out of a familiarity with local conditions and constituent concerns. Because attorneys general are on the front lines, they are often the first to learn about and respond to privacy and security violations."

Americans overwhelmingly demand progress now on privacy rights. We are all online, our kids are even more online, but we are not able to protect ourselves or them. We need a stronger web of protections—and that will only happen with a movement to update state laws and ensure that state DOJs have the resources to protect us and citizens have the tools to protect themselves. ■

James Steyer is the founder and CEO of Common Sense Media, a non-profit organization dedicated to creating a powerful voice for kids and families in the 21st century.

Compliance is feeling GDPR's growing pains

Six months after its enactment, the EU's data privacy regulation still hasn't provided the clarity many were looking for … and it might not come for a while yet. **Neil Hodge** has more.

If Europe's data regulators hoped for a smooth transition to new rules, they are in for a shock.

Six months on from when the European Union's General Data Protection Regulation (GDPR) came into force, organisations still say that there is a lack of clarity about what they can—and cannot—do with personal data, or in what circumstances they might be flouting the law.

Added to that, several EU member countries—Czech Republic, Finland, Portugal, Greece, Poland, and Slovakia—have not updated data protection laws to align to the regulation, and others have been slow to pass theirs (Spain and Italy only did so in August and September, respectively, while France passed legislation in August to take effect retrospectively from May).

While lawyers say that in the absence of refreshed domestic legislation companies would need to follow GDPR, they admit that there could perceivably be a question about whether regulators in those countries would be able to enforce the regulation without new legislation. Another complication is that without implementing legislation, organisations don't get the details they need to be able to comply easily.

"Complications for international businesses have arisen because a number of countries around Europe haven't implemented their local laws supplementing GDPR," says Mark Taylor, a partner specialising in data protection at law firm Osborne Clarke. Added to that, he says, "where those local laws do exist, they have adopted variations of GDPR to a greater extent than we might have ideally hoped for. So while GDPR has made international compliance easier, it hasn't unfortunately made it a one-size-fits-all approach everywhere."

GDPR is meant to bring uniformity in data protection across the European Union, as well as ensure that the regulatory approach and level of enforcement is consistent across the 28-nation bloc. The regulation, however, does provide some leeway. For example, Article 9 gives member states latitude to decide on local exceptions to the ban on the processing of special categories of personal data, such as data about ethnic origin, religious beliefs, health, and sexual orientation. Member states can allow the processing of such data in order to enable research or to support employment law or the public interest, but they need to clearly spell out their derogations in their implementing acts aligning national data protection laws to GDPR. As a result, GDPR may not be as uniform in practice as the European Commission, the EU's executive body, had hoped it would be.

Compliance professionals believe that there is still a lot of detail around GDPR that is unclear. "Every week I am asked by management whether we are fully GDPR compliant and I don't know how to answer," said one compliance officer attending the Compliance Week European Conference in Amsterdam in November. Others said that their main concern was that "legitimate interest," which relates to how personal data is used and how long it is retained for, was too vague. One compliance officer was unsure whether a request to check a candidate's criminal record would now be considered illegal under GDPR, despite his company routinely conducting such checks previously.

Some compliance officers said that another key problem was that they did not know whether national regulators would take a proactive approach to check on companies' compliance with GDPR, or if they would be more "reactive" and only act on specific complaints or industry-wide concerns, such as the way financial services firms use personal data for direct marketing, for example.

Privacy campaigner Max Schrems told delegates during his keynote address at Compliance Week Europe that there is a lot of "legal uncertainty" regarding GDPR and said he believed, "we'll have some kind of 'GDPR 2.0' sooner or later, because so many of these issues are so unclear that we'll have to update the law somehow."

Several conference attendees said that they are awaiting the first "significant" enforcement cases under GDPR to give them a better understanding of the regulation and how it is likely to be enforced.

During a keynote address, Ventsislav Karadjov, chair of Bulgaria's Commission for Personal Data Protection and vice-chair of the European Data Protection Board, the body set up to assist and monitor how data regulators across the European Union enforce GDPR, told delegates they could be in for a long wait. He said: "2018 was the year for making companies aware about the new rules, to prepare data protection authorities to prepare for the new competencies, and also to familiarise individuals—the data subjects—with their rights. I would say that 2019 will be the year for GDPR implementation."

Lawyers agree that there is still a great deal of confusion surrounding GDPR. They add, however, it is not necessarily the fault of data regulators. "Certain myths about the GDPR still persist," says Robert Lands, a partner at law firm Howard Kennedy, "including that it's all about getting consent for everything you want to do with personal data (it's not) and that GDPR does not apply to small businesses (it does)." Sophie Chase-Borthwick, director of privacy services at data specialists Calligo, says that companies are still confused by what they need to do, but adds that "how much of this is wilful is unclear."

"Most confusion among the companies we engage with seems to come down to scope—both geographic and what personal data actually is," she adds. "Many appear to be confused over their lawful reasons for holding and processing personal data. But, upon questioning, you realise this is because there is no lawful reason, and yet they want to still carry on with their activities without defensible, transparent, and lawful grounds to do so."

Generally, however, most experts believe that organisations and compliance functions are working well toward their GDPR preparations. "Companies that had inadequate procedures under the old data protection legislation are likely to struggle under the new GDPR," says Jonathan Compton, a partner at law firm DMH Stallard. "But companies that had adequate structures and controls in place are likely to find adjustment to the new legislation fairly straightforward."

Brian Craig, legal director at U.K. law firm TLT, says that "generally, companies have their heads around compliance, but putting their programmes into practice is a whole new challenge. We are seeing a lot of 'GDPR in practice' questions relating to specific business activities, including how compliance programmes apply to the actual day-to-day running of a business and what needs to change." He adds: "There is a lot more guidance available now than in the run up to 25 May—compliance officers should feel a lot better equipped to deal with any challenges that present themselves."

Several data lawyers believe that clarity over some of the GDPR's finer points will come when companies see how stringently some national data protection authorities are prepared to investigate complaints and enforce the rules. Germany, for example, has a data regulator in each state and they have started proactively auditing companies for compliance: One of these regulators, the Bavarian Data Protection Authority (the BayLDA), is currently undertaking a number of targeted audits into, for example, the secure operation of online shops and accountability for large corporations. The Dutch Protection Authority is similarly actively auditing businesses to ensure they are achieving GDPR compliance.

"Historically, certain EU regulators, such as the Austrian, French, German, and Spanish regulators, have been seen by some as having a more stringent approach to privacy en-

forcement," says William Long, a partner in law firm Sidley Austin's privacy and cyber-security practice. "It remains to be seen whether and how these patterns will translate to the post-GDPR world, especially now that all EU regulators have the same enforcement powers," he says, "but we have noted that while some regulators are more fully up-to-speed with the GDPR, others may not be in a position to take enforcement action at this stage, mainly due to the lack of resources."

GDPR cases are beginning to come through the pipeline. Besides Schrems' high-profile class-action-style complaints against Facebook and Google for coercing user consent, in October the French data protection regulator (the Commission nationale de l'informatique et des libertés) decided to take enforcement action against Vectuary, a marketing agency that was processing individuals' geolocation data for marketing and profiling purposes, but reportedly without valid user consent or another legal basis for such processing. Also in October, the U.K.'s data regulator, the Information Commissioner's Office (ICO), issued its first enforcement notice under the GDPR against a Canadian company called Aggregate IQ Data Services in respect to its processing of personal data for political organisations, such as "Vote Leave" during the 2016 Brexit referendum.

Other potential enforcement actions by the ICO may be forthcoming, with speculation mounting that there is likely to be regulatory action against British Airways for a data breach between August and September 2018 that affected 380,000 customers.

"This could be the first 'mega' fine delivered by the ICO, possibly exceeding £1 million [(U.S. $1.27 million)]. No one can be sure exactly what will happen here, but it is the most obvious case to watch for a large post-GDPR fine," says Matthew Holman, a principal at EMW Law.

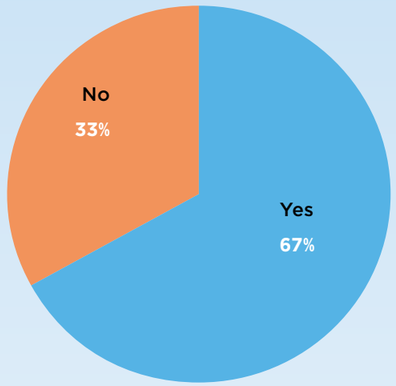
Horne—and others—also point out that there is continued interest over the case of U.K. supermarket chain Morrisons and a disgruntled employee who stole and deliberately leaked the financial and personal records of thousands of company workers. The case led to the first class-action-style lawsuit in the United Kingdom under the country's previous data protection rules; and while the Court held that Morrisons had adequate data protection procedures in place, it also deemed the company "vicariously liable" for the breach. The Court of Appeal did so, too. Morrisons has said that it will take the case to the Supreme Court.

"If you wanted to watch a big case in the world of data protection, you won't be able to find one attracting more attention than the appeal of the Morrisons decision to the Supreme Court which, if it goes ahead (and we believe it will), is likely to be heard in 2019," says Horne. "This case could open the floodgates for class-action GDPR cases in the U.K." ■

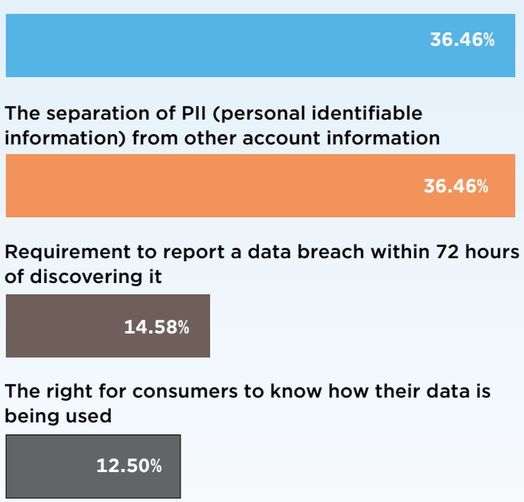
{CW'S DATA PRIVACY SURVEY}

In partnership with RSA, CW asked more than 100 compliance professionals involved with data protection at their companies 15 questions related to their privacy programs.

Is your company fully GDPR compliant?



Which of these provisions of GDPR have been/would be most difficult to implement?



Privacy advocate Schrems sees GDPR lax enforcement

Speaking at the recent CW Europe conference in Amsterdam, leading privacy campaigner Max Schrems cast doubt on whether the newly enacted GDPR would have any teeth, writes **Neil Hodge**.

A leading privacy campaigner who is behind the first European class-action complaints against tech giants Facebook and Google has criticised the penalties that can be meted out under the EU's new data regulation and has slammed Europe's historically poor record of enforcement over data privacy issues.

Max Schrems, founder of NOYB ("None of Your Business")—European Centre for Digital Rights, believes that the level of fines available to national data protection authorities under the EU's newly enacted General Data Protection Regulation (GDPR) are so high that they will simply force companies to contest the complaint and any penalty rather than accept any wrongdoing, thereby stalling judgments.

Under GDPR, national data regulators can issue fines of up to €20 million (U.S. $23 million), or up to 4 percent of annual global revenues—whichever is greater. Yet Schrems is unsure whether such strong fines are an appropriate deterrent and believes that "€100,000 (U.S. $114,170) would have been sufficient for most companies."

"I was actually pretty unhappy about the €20 million as a general price tag," said Schrems, speaking at Compliance Week's European conference in Amsterdam in November. He dismissed the €20 million figure as "a populist big number that you can just put out in the newspaper."

In front of an audience of more than 200 compliance professionals and other attendees, Schrems also suggested that the top-line fine of 4 percent of global turnover may not be quite the sizeable fine that it appears to be.

"If you're really big and data's your main business, a case like that usually takes 5 to 10 years to resolve [and the fine] is only 4 percent of your annual turnover anyway," said Schrems. Consequently, he said, it may be a "worthwhile investment" for data companies to continue as they are and legally challenge data regulators' complaints and investigations for years. That

way, he said, they can continue to generate massive revenues before they are required to change their practices.

"So I wonder if, for these guys, the 4 percent [penalty] is even sufficient," he said.

Schrems believes that data protection in Europe has been let down in the past by lax enforcement. The "big criticism," he said, is that while "we walk around and say we're the biggest privacy protectors the world has ever seen … the bottom line is that … there are all these fundamental rights and privacy law in Europe, but if you don't really comply, nothing is ever going to happen anyway."

Referring to the previous EU data protection directive, Schrems said: "The reality is we had a nice law, but no one ever enforced it in practice," adding that "financially, it made more sense for most companies to just totally ignore it than follow the law" because the cost of compliance was disproportionately larger than any penalty. In Austria, for example, the maximum fine for a data breach under its data protection laws was just €25,000 (U.S. $28,000): Compare that to the £500,000 (U.S. $639,000) maximum that Facebook received in October from the U.K.'s Information Commissioner's Office.

Despite the fact that the GDPR—as well as the European Data Protection Board—is supposed to ensure uniformity, however, Schrems thinks that the level of enforcement on privacy issues may continue to be uneven throughout the European Union.

He also thinks there are likely to be differences in the approach and "culture" that national regulators take. For example, he says, some national data protection authorities will try to help companies comply, "which, in practice, we don't do in most other fields, because we know that their actions are massive violations of the law," while others will simply fine them—possibly taking on smaller companies (the "low-hanging fruit," as he referred to them) first. Some may also be keener than others to try out GDPR's extensive powers.

According to Schrems, when he brought his first complaints against Facebook to the Irish Data Protection Authority in 2011, the Authority's office was based in a small town outside of Dublin and was situated above a supermarket. It had a staff of just 20 people—none of whom was a lawyer or a trained technical expert. With the onset of GDPR, however, the regulator now has a staff of more than 100 people and has in-house legal and technical experts.

"It's going to be interesting because certain data protection authorities now have, for the first time, serious power to enforce stuff or to raid a company and really say, 'We want to see what's on your servers,' " said Schrems.

"Certain DPAs are being—at least in public—very bold and are saying, 'We're now going to use these powers as well,' while others have already said, 'We're more or less going to continue to help companies.' So that's going to be interesting to see how the culture changes," he added.

But he declined to name which regulators would be most or least aggressive. "We don't really have a ranking so far," said Schrems, though he added that "we're doing a mapping exercise to understand the possibilities of where to enforce stuff."

Compliance Week Europe conference attendees take in a keynote presentation on data privacy.

> "GDPR now foresees emotional damage in the sense of, 'You lost a million data sets, these million people now have the emotional fear of the data somewhere in Russia.' And there is going to be a price tag on that."
>
> Max Schrems, Founder, NOYB

Schrems' NOYB is a non-profit organisation set up to champion consumer rights and launch "strategic" court cases under GDPR, the proposed EU ePrivacy directive, and on privacy issues in general. Under Article 80 of the GDPR (which refers to representation of data subjects), not-for-profit organisations can make class-action-style compensation claims for consumers if the case is in the public interest. On 25 May, when the regulation came into force, Schrems filed the first complaints using GDPR against Google and Facebook over the way both companies coerced consumers into accepting their data policies to use their services. The companies could face combined penalties of up to €7 billion (U.S. $8 billion) under GDPR, but it is likely to be a lengthy—and expensive—process, he admits.

While data companies are likely to be key targets, Schrems believes that few other companies have woken up to the real threat that Article 80 may pose, as GDPR allows people to claim for "emotional damages"—a new concept for many EU jurisdictions, he says, and one that has a "price tag."

"GDPR now foresees emotional damage in the sense of, 'You lost a million data sets, these million people now have the emotional fear of the data somewhere in Russia.' And there is going to be a price tag on that," said Schrems.

"We don't know the price tag, and it is going to be very different in member states. For example, Austria has very limited damages awards. But there are some member states that have much higher ones. The interesting thing is usually these cases are mass damages, so if you have a database with a million people, you have a million people that have a claim against you," he added.

Schrems noted that in Canada, for example, a single privacy violation can cost a company up to €20,000 (U.S. $23,000) in damages. "If you multiply that by a million people, then you get price tags that go way beyond the €20 million in damages and penalties," said Schrems. And while regulatory penalties can be lowered if companies can prove they had measures, protocols, and procedures to mitigate risks of a breach, for example, damages awards do not. "Damages are calculated on the damage you did. It doesn't matter if you tried to comply with the law or totally ignored it—the damage is the same," warned Schrems. ■

During Max Schrems' session on GDPR, he engaged in a debate with fellow keynoter and European Data Protection Board Vice-Chairman Ventsislav Karadjov.

EU regulator pushes for global consensus on data ethics

At a recent event, European Data Protection Supervisor Giovanni Buttarelli decried the fact that there is "no ethical consensus" around personal data and urged regulators to get together on privacy law. **Neil Hodge** explores.

BRUSSELS—Data regulators need to push for a "global consensus" around the ethical use of personal information, particularly as technologies such as Artificial Intelligence (AI) are taking a greater role in decision making, says one of the EU's top privacy enforcers.

European Data Protection Supervisor Giovanni Buttarelli told attendees at the 40th International Conference of Data Protection and Privacy Commissioners in Brussels that there is currently "no ethical consensus" about data use.

"We do not have a consensus in Europe, and we certainly do not have one at a global level," said Buttarelli. "But we urgently need one. Because digital technologies and data flows are already intensely global." He also warned that "self-regulation alone is not the solution."

Buttarelli said that ethics is among the "most pressing strategic challenges" for data protection authorities and warned that regulators need to "understand technology" so that they can "articulate a coherent ethical framework."

"Otherwise, how can we perform our mission to safeguard human rights in the digital age?" he asked.

In particular, Buttarelli singled out algorithms that can make "informed" decisions as a key risk area, citing the fact that such technology is already responsible for deciding around 70 percent of the content that is viewed on the internet and social media sites through processing personal data—not necessarily responsibly.

"We need a critical understanding of the ethics informing decisions by companies, governments, and regulators whenever they develop and deploy new technologies" said Buttarelli, as "we are fast approaching a period where design, deployment, and control of new technologies and technological processes are delegated to machines."

Buttarelli flagged up several areas where crucial decision making has been left to machines, such as in killer drones, and pointed out that in September at the United Nations, "delegates were unable to reach agreement even to start discussions on how to control them."

Other areas of concern include using algorithmic decision making in criminal sentencing and by social media companies "whose unaccountable algorithmic decision making has been weaponised by bad actors in ethnic conflict zones, with at times appalling human consequences, notably in Myanmar."

On 23 October, the day before the conference began, data commissioners from several EU member states, as well as Canada, Hong Kong, Argentina, and the Philippines, agreed to a set of guiding principles regarding ethics, monitoring, and enforcement on AI. These underlined that developments and increased use of the technology need to ensure fairness, transparency, and accountability and that users must retain control over their own data.

Buttarelli told attendees that guiding principles and best practices can ensure that users' rights to privacy and data protection remain paramount, even when they are meant to be enshrined in legislation—namely the EU General Data Protection Regulation (GDPR).

"The fact is that the European legislator did not think about ethics when it drafted the GDPR. In fact, the regulation only refers three times to ethical considerations in specific professions, like research," said Buttarelli.

"This is not a criticism of the GDPR. It is a reality check on the limitations of any law, even a comprehensive one. Laws establish the minimum standard. Best practices are assumed to go beyond the minimum standard. So for me, compliance with the law is not enough," he added.

Apple, Facebook, and Google were among the major technology and social media companies that took part in the conference and all pledged to improve how they use data and promised to give users better control over how their personal information is managed.

Apple Chief Executive Tim Cook said the company supports a U.S.-style data protection law that mirrors GDPR and criticised companies that profited from people's data that was then used to manipulate political campaigns and incite violence. ■

'No-deal' Brexit risks U.K. and EU data transfer problems

In the event of a "no-deal" Brexit, EU data commissioners are warning of data transfer restrictions between the European Union and the United Kingdom, which will be treated as a third country. **Neil Hodge** has more.

BRUSSELS—EU data commissioners have said that the United Kingdom would be treated as a "third country" in the event of a "no-deal" Brexit next March and have confirmed that data transfers would be "restricted."

"Until the European Commission rules that data protection in the U.K. is on a par with that in the EU, the U.K. will be considered as a third country and there will be restrictions on data flows," said Elizabeth Denham, U.K. Information Commissioner, at the 40th International Conference of Data Protection and Privacy Commissioners in October.

Despite the U.K. and EU agreeing a Brexit withdrawal agreement, there is no guarantee that U.K. Members of Parliament will back it, so a "no deal" scenario still looms large.

An Information Commissioner's Office (ICO) spokesperson said: "The draft Withdrawal Agreement provides that during the implementation period to December 2020, the General Data Protection Regulation (GDPR) will continue to have effect in the U.K. So personal data will continue to flow within the European Economic Area, just as it does now, with no need for special measures." She added: "The political declaration also makes clear the importance of trying to achieve an adequacy decision during the implementation period and ensure future regulatory cooperation."

The U.K. government had already set about warning U.K. businesses during the summer of the risks of potential disruptions in data flow. On 13 September the Department for Digital, Culture, Media, and Sport (DCMS) issued technical guidance outlining the consequences for U.K./EU data protection under a "no-deal" Brexit.

The guidance clarifies that while the United Kingdom will retain GDPR, and that personal data transfers from the United Kingdom to the European Union will remain valid, the legal framework governing the transfer of personal data from the European to the United Kingdom will change—and will require "specific safeguards"—unless a deal is agreed.

The U.K. government has already set about warning U.K. businesses of the risks. On 13 September, the Department for Digital, Culture, Media, and Sport (DCMS) issued technical guidance outlining the consequences for U.K./EU data protection under a "no-deal" Brexit.

The guidance clarifies that while the United Kingdom will retain the EU General Data Protection Regulation (GDPR) and that personal data transfers from the United Kingdom to the European Union will remain valid, the legal framework governing the transfer of personal data from the European Union to the United Kingdom will change—and will require "specific safeguards"—unless a deal is reached.

Under the GDPR, organisations within the European Union are only permitted to transfer personal data outside the European Economic Area (EEA) if certain conditions are met.

The U.K. government wants to secure an "adequacy determination" within the ultimate withdrawal treaty to maintain a free flow of data between the United Kingdom and the European Union. An adequacy determination would mean that the European Commission deems the U.K.'s level of personal data protection essentially equivalent to that of the European Union and would enable data to flow unrestricted.

Presently, however, such an outcome remains uncertain; and the U.K. government advises organisations to take contingency action, such as using standard contractual clauses. These are model data protection clauses that have been approved by the European Commission and enable the free flow of personal data when embedded in a contract.

Also, given the lack of movement on Brexit negotiations, law firms such as Norton Rose Fulbright and DLA Piper suggest firms make contingency plans and consider such clauses.

"Regarding the U.K. as a third country is not the best way forward," said Denham. She added that "the U.K. has contributed a great deal to EU data privacy issues, and I think it would be a hard task for the European Commission to find the U.K. inadequate in terms of data protection."

Giovanni Buttarelli, European data protection supervisor, echoed her thoughts, noting that "the U.K. has made an important contribution to data protection and privacy issues as an EU member." Buttarelli says he hopes an "agreement can be reached." ■

Regulators raise problem of AI in decision making

Are companies transferring too much decision-making power to machines? EU data regulators think firms should "think seriously" about disclosing to investors that automatons are now in charge of their data, writes **Neil Hodge.**

BRUSSELS—EU data regulators are increasingly concerned about the potential impact that organisations' growing reliance on artificial intelligence and algorithms could have on business decision making.

Regulators are concerned that management accountability will be impaired if companies delegate too much of their responsibility for decision making to machines. They also admit that this "grey area" presents problems for them about how best to hold companies to account if algorithms, AI, and machine-learning technologies are largely responsible for how personal data is used (or misused).

Speaking at the 40th International Conference of Data Protection and Privacy Commissioners in October, U.K. Information Commissioner Elizabeth Denham said that companies' ability to ensure transparency, fairness, and accountability "remain core" to how personal data is used—and protected—in the digital world, adding that "regulators can't tackle these issues on our own."

She also said that organisations need to "think seriously" about how they explain to customers and stakeholders that machines are in charge of how people's data is used and for what purpose.

"Companies need to explain to customers, their boards, investors, and regulators why algorithmic solutions are being used to make important decisions, and to what extent," said Denham. "They also need to explain what controls are in place to ensure that the decisions made due to these algorithms are in the company's best interests and that personal data is not being misused in the process."

She added that "few companies think about this, currently."

Giovanni Buttarelli, European Data Protection Supervisor, had earlier told attendees at the conference of the need to understand the ethics behind increased around AI usage and how technologies use data to inform decision making. "We are fast approaching a period where design, deployment, and control of new technologies and technological processes are delegated to machines," he warned.

Buttarelli flagged several areas in which algorithmic decision making has been left to machines, such as in killer drones and criminal sentencing, and by social media companies "whose unaccountable algorithmic decision making has been weaponised by bad actors in ethnic conflict zones, with at times appalling human consequences, notably in Myanmar."

Regulators have already agreed a response. On 23 October data commissioners from several EU member states, as well as Canada, Hong Kong, Argentina, and the Philippines, agreed to a set of guiding principles regarding ethics, monitoring, and enforcement on AI. These underlined that developments and increased use of the technology need to ensure fairness, transparency, and accountability and that users must retain control over their own data.

Leading tech companies are beginning to question their use of personal data, as well as how technology uses it. Apple CEO Tim Cook told attendees that "advancing AI by collecting huge personal profiles is laziness, not efficiency" and said that "platforms and algorithms that promised to improve our lives can actually magnify our worst human tendencies."

In May, Facebook—following criticism surrounding the Cambridge Analytica furore—announced that it is testing a tool called "Fairness Flow" that it hopes can determine whether a machine learning algorithm is biased against certain groups of people based on race, gender, or age.

However, Pascale Fung, professor at the Department of Electronic & Computer Engineering, Hong Kong University of Science and Technology, urged caution when considering regulating algorithms and their development and use.

"When people talk about regulating algorithms, I don't know what they mean," she said. "In terms of design, the same algorithms that have influenced politics on social media are technically similar in many ways to those that are being used to develop breakthroughs in medicine and research. We must not regulate for the sake of regulating. In the long run that can be just as harmful." ■

Leveraging GDPR Compliance Initiatives to Comply with the CCPA (California Consumer Privacy Act) and LGPD (Brazilian General Data Protection Law)

Author: Paul Breitbarth, Director – Strategic Research & Regulator Outreach, Nymity Inc.

On 1 January 2020 the California Consumer Privacy Act (CCPA) will enter into application. A few weeks later, the new Brazilian Data Protection Law (LGPD) will start to apply. Both new laws will provide for extensive consumer rights, including a right of access, data portability and deletion. And even though the application date is still some time away, many impacted organizations have already started their preparations to comply with the law.

This is yet another big law to comply with, so shortly after the EU General Data Protection Regulation (GDPR) has entered into application. This may seem daunting to many, but it doesn't need to be. If you have put in place the right accountability mechanisms or even better, a more comprehensive privacy program infrastructure to maintain compliance with the GPDR, it may be relatively easy to leverage your work to deal with CCPA and LGPD compliance. In this short paper, we will show how an accountability approach to privacy management can produce compliance outcomes for both the GDPR, CCPA, LGPD and a multitude of other laws with similar compliance obligations.

Scope of GDPR vs. CCPA

It is worth noting that GDPR, CCPA and the LGPD are not fully comparable. Firstly, GDPR and LGPD are omnibus laws, applicable in, respectively, 31 countries (the 28 EU Member States and the three countries of the European Economic Area: Norway, Iceland and Liechtenstein), the full territories of one country (Brazil), whereas CCPA applies solely in the State of California and mainly deals with consumer rights. Topics like data transfers, data security and data breaches are not covered by this law.

General Data Protection Regulation (GDPR)

- Applies in the EU and the EEA and to organisations offering goods and services to persons in the EU
- Omnibus legislation covering most aspects of data protection law
- Fundamental right > no nationality requirement for rights to apply
- In force since 25 May 2018 – accompanying laws in 19 EU Member States in place

California Consumer Privacy Act (CCPA)

- Applies in the State of California and to organisations doing business there
- Legislation focuses on data subject rights
- Rights only extended to California residents
- Will apply as of 1 January 2020; changes to the body of law still possible

LGPD Brazilian General Data Protection Law

- Applies in Brazil and to organisations offering goods and services to persons in Brazil
- Omnibus legislation covering most aspects of data protection law
- Will apply as of 15 February 2020
- No supervisory authority in place yet

Using the Nymity Privacy Management Accountability Framework™

An accountability approach to compliance means organizations implement and embed relevant policies, procedures and other measures throughout the organization, and assign responsibility for these activities to be completed. Ideally, the activities are also reviewed on a regular basis (for example annually). Such reviews lead to documentation, such as minutes of meetings, memos preparing decisions, the actual policies and procedures, and log files, which can serve as evidence to demonstrate compliance to regulators and other stakeholders.

Through years of research and hundreds of on the ground workshops with organizations and Regulators around the globe, Nymity has developed the Nymity Privacy Management Accountability Framework™ ("Framework"): a menu of 139 privacy management activities, or technical and organizational measures. It is a practical Framework to help organizations operationalize privacy management and can be used to implement, maintain and demonstrate compliance with a a privacy program and a multitude of laws. Thousands of organizations around the world use the Nymity Framework to structure, plan and report on privacy compliance and specifically, GDPR compliance.

When preparing organizations for the GDPR, Nymity mapped the text of the Regulation to the Framework and identified 39 Articles of the GDPR that require evidence of a technical or organizational measure in order to demonstrate compliance. Those 39 Articles mapped to fifty-five privacy management activities (technical and organizational measures) that if implemented, may produce documentation to demonstrate compliance with the requirements. The other 60 provisions of the GDPR do not require evidence of technical or organizational measure to demonstrate compliance from organizations, but deal with definitions, the role of the DPAs and the Commission and other non-operational legal requirements.

Mapping the Framework to the CCPA and LGPD

For the CCPA, Nymity has made a similar mapping. Out of the 23 provisions of CCPA, we have identified nine provisions that require evidence of a technical or organizational measure in order to demonstrate compliance, linked to 9 privacy management activities. The fact that there are fewer mandatory activities than for GDPR, is caused by the different scope of the two laws. For the LGPD, Nymity has identified 43 privacy management activities, linked to 24 provisions of the law.

Privacy Management Categories	Technical and Organizational Measures	GDPR Article Reference	CCPA Provision Reference	LGPD Article Reference
9. Respond to Requests and Complaints from Individuals	Maintain procedures to address complaints			50
	Maintain procedures to respond to requests for access to personal data	15	1798.100 (a) 1798.130	6, 18, 19
	Maintain procedures to respond to requests and/or provide a mechanism for individuals to update or correct their personal data	16, 19		18
	Maintain procedures to respond to requests to opt–out of, restrict or object to processing	7, 18, 21	1798.115 (d) 1798.120 (a) 1798.130 1798.135 (a)(1) -(6) & (c)	8(5), 18, 20
	Maintain procedures to respond to requests for information		1798.100 (a) 1798.115 (b) 1798.130	18
	Maintain procedures to respond to requests for data portability	20	1798.100 (d) second para, 1798.130	18
	Maintain procedures to respond to requests to be forgotten or for erasure of data	17, 19	1798.105 (a) 1798.130	18

The mapping of the laws completed, it was a minor effort to make a comparison between them. After all, when dealing with both laws, it helps to get a quick overview of what additional work remains to be done. The mapping includes an overview of privacy management activities from the Framework, linked to the provisions of both GDPR, CCPA and LGPD, including the relevant provisions of each law.

SPONSORED CONTENT

From GDPR to CCPA and LGPD

When looking at GDPR, CCPA and LGDP, it is immediately clear that there is a fair amount of overlap among the three laws, especially where data subject rights are concerned. Given the omnibus character of GDPR and LGPD, their overlap is even bigger. When identifying the overlap among the three legal frameworks, it also becomes possible to identify the so-called outliers: the elements of the law that are specific to a single jurisdiction, for example specific deadlines or time constraints. Those are the ones where your focus during implementation could be. For the areas that do overlap, it is likely possible to re-use existing policies and procedures to deal with data protection requirements in new jurisdictions, especially if your program is based on a framework like Nymity's Privacy Management Accountability Framework™.

Not all privacy management activities overlap. Two activities required for CCPA are not as explicit in the GDPR. And for LGPD, there are activities that do not overlap with GDPR, and certainly several that do not overlap with CCPA.

More detail on the mapping of the CCPA to the Nymity Privacy Management Accountability Framework™ can be found in the Nymity CCPA Accountability Handbook™, together with the comparative table between CCPA and GDPR. The Handbook is available as a free download on our website and available in hardcopy at privacy conferences around the world. A similar Handbook for the Brazil LGPD is forthcoming in Q1 2019.

Steps towards compliance

The approach to deal with compliance with CCPA or LGPD, can also be used to deal with any other data protection law in the world. Once the theoretical overlap between laws is clear, you can set to work to adapt your privacy program to deal with any new law.

1. To get started, first identify which of the mandatory privacy management activities that apply to the law you have based your privacy program on, and the law that you want to deal with next, have been embedded in your organization, and which policies and procedures you have implemented to ensure compliance. These policies and procedures are now up for review, and you will need to verify that all elements that are embedded in the new laws' legal provisions are also part of your internal policies and procedures.
2. Step two is to take a look at the privacy management activities that are considered as mandatory for the new law you are dealing with, but are not part of your existing data protection compliance program. It may very well be that you have nevertheless implemented these activities in your organization, for example as part of your security program. If so, you can repeat the check you have done described under step 1. If not, new policies and procedures are likely required.

Conclusion

The introduction of a new law, or changed requirements of an existing law, will always require some effort of an organization to double check whether or not they are compliant. However, when taking an accountability approach to compliance, based on the Nymity Privacy Management Framework™, it becomes much easier to leverage existing accountability mechanisms to meet your revised compliance goals. Nymity has over 15 years of experience supporting organizations with their accountability and compliance requirements for privacy and data protection, both with free resources like the GDPR and CCPA toolkits, and privacy management software that will help you automate parts of your privacy program.

Should you have any further questions, contact us via www.nymity.com or info@nymity.com.

SURVEY:

Uncertainty lingers regarding data privacy compliance

Results from a recent Compliance Week survey on data privacy show how companies are prepping for data protection laws in the United States, despite concerns of what just such laws will entail. **Kyle Brasseur** shares the results below.

As Europe settles into life under the General Data Protection Regulation (GDPR), the United States is grappling with potential legislation of its own to protect consumer information.

Questions remain about what U.S. data privacy legislation might look like, but companies have already begun to strategize. In partnership with RSA, Compliance Week conducted a survey asking U.S. firms whether they're doing enough to stay compliant with data protection laws; the survey garnered 100 responses from individuals whose scope of responsibility included helping ensure data privacy. Of the respondents, only 36 percent felt their data privacy program is in compliance with state, national, and/or international regulations, while 52 percent felt they were almost there but struggling to keep up.

"I think this uncertainty is largely due to the continuing changes going on with the regulatory landscape around privacy," says Marshall Toburen, a risk management strategist with RSA Archer. "There continues to just be so much new regulation around privacy—I'm not at all surprised that there's a majority of organizations that aren't quite sure that they've got their house completely in order."

Roughly **70%** of the respondents said they collect more data from customers today compared to three years ago, yet over **80%** said less than **25%** of their compliance budget is dedicated to data security. Of that group, **44%** said it was less than **10%** of the budget.

Even those respondents that answered in the negative—4 percent—have likely "spent time analyzing the regulations that they think they have an obligation to comply with and done something, but they just don't feel that they've done enough yet," says Toburen.

Roughly 70 percent of the respondents said they collect more data from customers today compared to three years ago, yet over 80 percent said less than 25 percent of their compliance budget is dedicated to data security. Of that group, 44 percent said it was less than 10 percent of the budget.

"I think organizations that have been involved with GDPR—that were heavily affected by that regulation—they're in the category of spending the higher amount," says Toburen, who added that if the federal government were to come out with a significant umbrella privacy regulation "you would see a much higher percentage of budget devoted to compliance."

For those not receiving what they feel is the necessary level of support—26 percent—from the board and C-Suite on data privacy, Toburen recommends illustrating the risks of a data breach. When asked what they would worry about more in the event of a breach, 74 percent of respondents picked reputational damage over fines incurred.

Similarly, 48 percent of respondents said complying with regulations is the best argument for a robust data protection program. Supporting the company's values garnered 27 percent of the vote, while meeting demands of the customers represented the remainder.

"I think leaders are talking about all three of these things," says Toburen. "Maybe for a particular reg it's a big fine, but the ones that are being successful are talking about all three of these impacts from a privacy breach to try to get the budget and commitment to the problem."

The threat of a privacy breach is ever-present. When asked if their company has suffered a breach within the past five years, 29 percent of respondents said yes. The remainder answered "not that I know of," as there is never truly a way a company can definitively say no.

"I think organizations that have been involved with GDPR—that were heavily affected by that regulation—they're in the category of spending the higher amount."

Marshall Toburen, Risk Management Strategist, RSA Archer

So what is the best answer for U.S. data privacy? A majority of respondents—72 percent—said they were in favor of national legislation governing data privacy in the United States, a statistic Toburen believes is a reflection of compliance individuals whose companies operate in numerous states across the country. Meanwhile, 43 percent of respondents said having the budget and lead time to meet the requirements would be their biggest worry if the United States adopts a GDPR-like national regulation.

Regarding GDPR specifically, 67 percent of respondents said their company was fully compliant with the EU regulation when compared against those who answered no. The right for consumers to ask that their personal data be deleted and the separation of PII (personal identifiable information) from other account information were considered the most difficult provisions of GDPR to potentially implement. Toburen notes both provisions stem from what is perhaps the most complex area of GDPR: providing a compliant answer when a customer asks, "What data have you collected on me?"

If and when U.S. data privacy legislation is enacted, companies will have work to do. Of CW respondents, 66 percent said they would describe their current data privacy program as "somewhat vulnerable, but improving." Time will tell what potential legislation might look like, but it would behoove those in charge of data privacy compliance at their company to begin taking steps toward getting their program in line with potential legislation.

"Organizations kind of have to start thinking, if they aren't already, 'what is the impact to the individual?' " says Toburen. "We need to be aligned to that pain." ■

Three unintended consequences of data privacy rules

Data privacy rules are undoubtedly in the best interest of the consumer, and they're also an integral part of any best-practices compliance program.

Robust regulations, however, are not without their drawbacks. Some will argue a strict privacy regime will have a negative effect on growing companies, create conflicting requirements in other instances, and potentially cause impediments to corporate investigations. We explore all three consequences below ...

1. Slowing innovation among smaller companies

Will national and international consumer data privacy laws hit the brakes on what has been a years-long period of rapid innovation?

From a big business perspective, at least one CEO emphatically says no. In October, Apple CEO Tim Cook, speaking at the International Conference of Data Protection and Privacy Commissioners in Brussels, said his company supports a national U.S. data protection law that mirrors Europe's General Data Protection Regulation.

> While large corporations can boast about the benefits of transparency and consumer trust, the current wave of data privacy laws, which include state efforts like California's, run the risk of stifling innovation and overall growth at small- to medium-sized companies that lack the resources and manpower needed for compliance.

Cook added that critics who claim data privacy legislation will hinder technology innovation are "not just wrong," but "destructive."

In written testimony for the U.S. Senate's Commerce Committee in September, Keith Enright, chief privacy officer at Google, expressed concerns with various proposals for regulatory regimes, but added that there was a corporate benefit in ensuring public trust. "Collection and use of personal information can create beneficial and innovative services," he wrote.

While large corporations can boast about the benefits of transparency and consumer trust, the current wave of data privacy laws, which include state efforts like California's, run the risk of stifling innovation and overall growth at small- to medium-sized companies that lack the resources and manpower needed for compliance.

This effect, the National Association of Manufacturers wrote, commenting on data privacy rules under consideration by the U.S. Commerce Department, would be exponentially exacerbated if they do not statutorily preempt conflicting state laws. It also called for "international solutions to harmonize the U.S. rules with those in other regions of the world."

Researchers are also putting some numbers to the problem and parsing the unintended effects of GDPR.

In a working paper published by the National Bureau of Economic Research, Jian Jia and Liad Wagman of the Illinois Institute of Technology and Ginger Zhe Jin of the University of Maryland studied "The Short-Run Effects of GDPR on Technology Venture Investment."

"The negative effects manifest in the overall dollar amounts raised across funding deals, the number of deals, and the dollar amount raised per individual deal," they wrote.

The paper notes that public concerns over the use of personal data have increased. Recent Pew surveys found that 91 percent of respondents believe they have lost control over how personal information is collected, and 66 percent said current laws are insufficient for protecting their privacy.

The enactment of GDPR, however, while satisfying these concerns, will have a negative effect on growing companies, particularly when it comes to venture capital and funding needed to innovate, produce, and expand. This manifests itself, particularly for start-ups, in the overall number of financing rounds and the overall dollar amount raised across rounds.

Their findings suggest a $3.38 million decrease in the aggregate dollars raised by EU ventures (per state, by industry category), a 17.6 percent reduction in the number of weekly venture deals, and a 39.6 percent decrease in the amount raised [by European companies] in an average deal following the rollout of GDPR," the paper says.

The researchers later add: "One may argue that higher compliance costs may have a positive effect on innovation. We demonstrate that younger firms are particularly susceptible to the consequences of data regulation." ■

—Joe Mont

2. Conflict between KYC and privacy regulations

For years, financial institutions have had to walk a regulatory tightrope, striking the right balance between compliance with regulations governing anti-money laundering with that of conflicting global data protection laws. But the far-reaching impact of GDPR creates further tension between these two compliance priorities.

On the one side, AML regulations require financial institutions to collect and process a vast array of personal data on entities and individuals during the onboarding process, or before engaging in certain business transactions with them, to defend against money laundering and terrorist financing practices. Know-your-customer (KYC) due-diligence procedures are a critical component of a robust AML compliance program.

Even as regulators around the world continue to expand the scope of financial institutions' obligations to identify and verify their customers' identities, the GDPR significantly restricts how they acquire and manage that customer data, creating numerous sticking points in a firm's overall AML compliance framework.

"It might seem like those two things are in conflict when, in reality, they're not," says Stephen Ritter, chief technology officer at Mitek Systems, a firm that specializes in digital identity verification and mobile capture. The GDPR doesn't prevent firms from satisfying their KYC obligations, but rather establishes requirements on how to do so in a secure fashion, he says.

Satisfying AML and GDPR obligations is possible—and, in fact, necessary—but it requires both a change in mindset and in the way that financial institutions operate. Start by understanding where AML regulations overlap with the GDPR, and then adjust AML and KYC policies and procedures accordingly.

> Even as regulators around the world continue to expand the scope of financial institutions' obligations to identify and verify their customers' identities, the GDPR significantly restricts how they acquire and manage that customer data, creating numerous sticking points in a firm's overall AML compliance framework.

At a high level, firms should have in place data-driven policies and procedures that comply with the GDPR's enhanced data-subject rights; make changes in the way they manage and interact with customers on a consent-based level; and implement data security controls and monitoring and auditing procedures, all of which can—and should—be automated with the newest privacy technologies that enable compliance with both GDPR and KYC obligations. ■

—Jaclyn Jaeger

3. Limitation on corporate investigations

Differing data privacy regulations from country to country and corporation to corporation could seriously impede internal investigations.

Prior to the 2015 Schrems decision by the European Court of Justice, which invalidated the Safe Harbor provision for transfer of personal, private data from Europe to the United States, U.S.-based law firms could use and analyze information from investigations conducted in Europe. That decision, however, along with the implementation of the U.S. Privacy Shield Framework and the enactment of the European Union GDPR, has brought several internal investigation concerns—especially those around data privacy—into the light.

Unlike data privacy rules for U.S. corporations, employee e-mails and other types of employee data in EU and U.K. companies are covered by the privacy rights afforded to individuals and are not considered company property. Under the GDPR, the ability of a U.S. corporation to access that information and take it back to the United States is therefore hindered.

To move forward, an organization must first obtain the consent of the individual who is under investigation. Obtaining such consent, however, can raise a host of other problems. For example, for consent to be considered valid it has to be fully explained or, in legal parlance, informed consent.

Consent cannot be a condition of employment. This means the organizstion must inform the person whose data is being collected that it could be turned over to the U.S. Department of Justice and the person could then be subject to extradition to the United States under a criminal indictment.

Moreover, when the EU line of employee privacy rights is coupled with the new Foreign Corrupt Practices Act Corporate Enforcement Policy, trouble brews for any company seeking cooperation credit, as it will be required to turn over any and all information to the Justice Department as soon as possible. And, even if companies are able to gather facts and data through internal investigations by using local law firms, they might still not be able to get that information back to the United States to use.

Further, preosecutors in the European Union and the United Kingdom will likely be unsympathetic to people whose investigations are conducted in violation of EU privacy laws.

The U.K. Serious Fraud Office has already lost one bribery prosecution in which a U.S. firm conducted an investigation that did not align with then-U.K. privacy laws. A corporate investigator will need a lot of careful thought to structure data transfers and even to structure interviews.

What does all of this mean for corporate compliance programs?

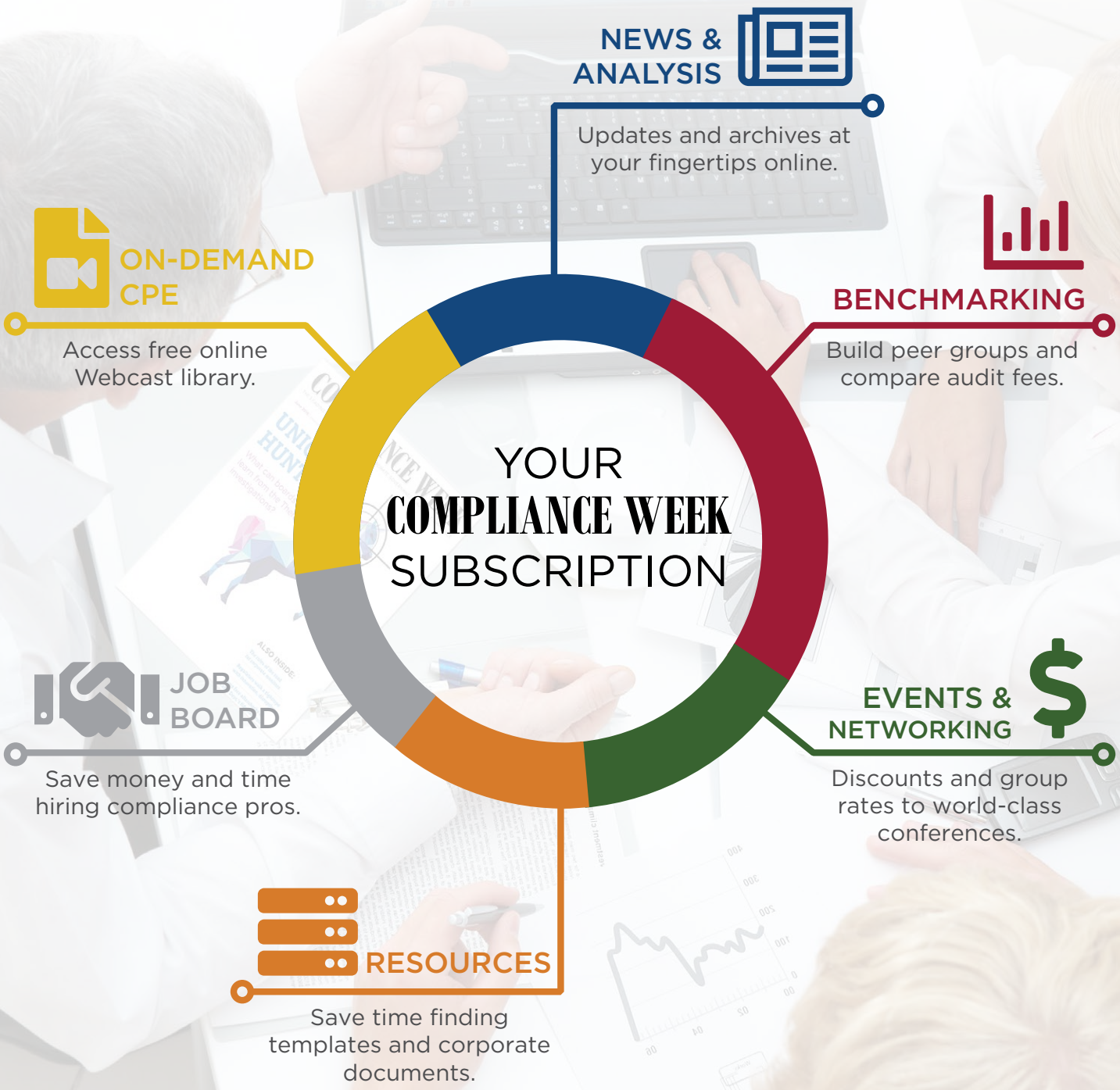
If one cannot use two of the key components in a best practices compliance program, based on the Justice Department/Securities and Exchange Commission Ten Hallmarks of an Effective Compliance Program or another related standard, it will put significant pressure on other parts of the program.

A compliance program will have to be structured more rigorously to prevent compliance violations through the use of internal controls and transaction monitoring tools. Chief compliance officers and other compliance practitioners will also have to be more involved and have more visibility into the entire lifecycle of transactions so they can determine how to begin to move from prevention to proscription—a task easier said than done. ■

—Tom Fox

A compliance program will have to be structured more rigorously to prevent compliance violations through the use of internal controls and transaction monitoring tools. Chief compliance officers and other compliance practitioners will also have to be more involved and have more visibility into the entire lifecycle of transactions so they can determine how to begin to move from prevention to proscription—a task easier said than done.

Are you taking advantage of all your benefits?



Questions about how you and your team can maximize your subscription perks?
Contact Elizabeth Sucher to learn how Compliance Week can elevate your program.

www.complianceweek.com • subscriptions@complianceweek.com • (617) 570-8605