Brought to you by the publishers of COMPLIANCE WEEK

Companies still wrestle with **data privacy regulation**

An e-Book publication sponsored by opentext™

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is a business intelligence and information service on corporate governance, risk, and compliance that features a daily e-mail newsletter, a bi-monthly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. www.complianceweek.com

opentext™

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit opentext.com.

Inside this e-Book

Survey: Companies say lack of guidance, budget restrictions hamper CCPA compliance

Complying with CCPA provisions continues to be difficult for many companies, says a new CW & OpenText survey. **Aaron Nicodemus** explores.

A survey from Compliance Week and OpenText of 66 business executives whose companies fall under the purview of the California Consumer Privacy Act found nearly two-thirds (64 percent) would not be fully compliant by July 1, the law's enforcement date. The survey was conducted earlier this summer.

The biggest barrier to compliance is the CCPA's complexity and the lack of guidance from California regulators, according to 68 percent of survey respondents who said the privacy law affected them. Next was inadequate budget (50 percent) and needing more time (40 percent), followed by a lack of skilled resources (37 percent) and a lack of required technology tools (23 percent). Respondents could choose up to three responses.

One quarter (26 percent) of respondents represented financial services firms like banks and insurance companies, followed by high tech (15 percent) and professional services (9 percent). Other industries represented in the survey were manufacturing (8 percent); media and entertainment (6 percent); aerospace, defense, and intelligence (6 percent); as well as life sciences, retail, consumer goods, and nonprofit organizations.

Beyond avoiding enforcement actions by the California Attorney General's office, complying with CCPA brings with it other benefits, said Janet de Guzman, senior director of industry marketing and compliance at OpenText, a Canadian-based global information management technology vendor.

"Companies need to realize that there are no quick fixes to comply with CCPA or any global privacy regulation."

Roobi Alam, VP of Global Privacy and Compliance, OpenText

"Data privacy is becoming increasingly important to consumers globally, and customers will gravitate towards companies that can protect their personal information. Companies that become CCPA compliant are able to boast about their robust, superior security measures," she said. "A negative tweet, post, or review can cause millions in lost revenue. Citizen journalism is real and for better or worse can make a company's misstep very public, very quickly."

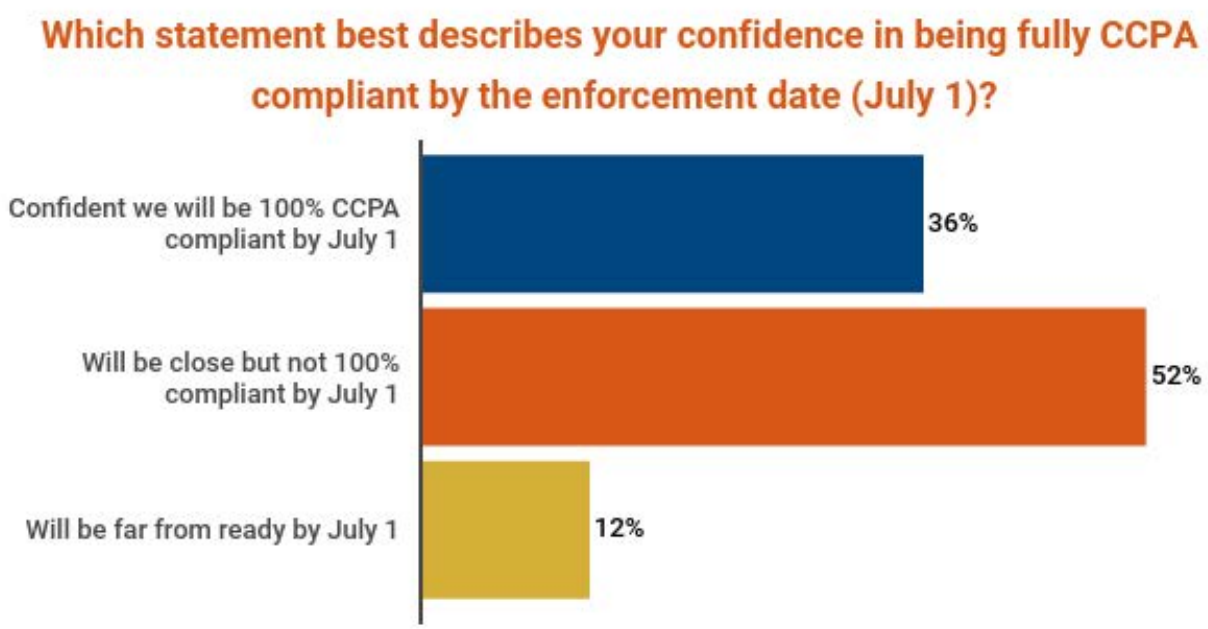
Most survey respondents said they are being asked to comply with the CCPA without much in the way of additional resources. Over the past three years, respondents said their privacy budgets have either stayed the same (44 percent) or increased slightly (36 percent). Only 17 percent of respondents said their privacy budgets significantly increased, while 3 percent said they actually decreased.

Complying with the CCPA is proving to be a tough task for some companies, said Roobi Alam, OpenText's vice president of global privacy and compliance.

"Companies need to realize that there are no quick fixes to comply with CCPA or any global privacy regulation. The privacy landscape is growing and becoming quite complicated, therefore companies need to dedicate a budget/resources to meet these demanding requirements," Alam said. "The scope of the budget will depend on the industry, size, and global operations of the company."

Of the regulation's requirements, respondents said that they were most concerned about its data breach prevention and notification requirements, as 85 percent were either extremely or somewhat concerned. Equally concerning was knowing what data their firm holds, where it's stored, and how it's used (83 percent said extremely or somewhat concerned).

"You cannot comply with data privacy laws unless you know what personal data you hold," de Guzman said. A key first step toward compliance is to determine your firm's data footprint by identifying all the relevant departments that process personal information—including HR, finance, contracts/procurement, sales, and marketing. Find out from the departments how they use the personal informa-



tion; then create a centralized master record of all processing activities, she said. Finally, document a streamlined and defensible process that can be used to keep the inventory up to date.

"If privacy is having its big moment now, I would say that—albeit with less fanfare—records management is too," she said. "Organizations can't hold onto personal data forever anymore, which means that companies that have been meaning to and putting off developing a more robust records management program and review their retention schedules have good reason to do so now."

More than half of survey respondents (54 percent) said the most important factor in selecting a privacy management tool is its ability to integrate with existing business systems that hold personal data, closely followed by the price of the tool (53 percent). (Respondents could pick up to three answers).

Getting all your data systems out of their silos and into an integrated data and content management system is a key step to complying with data privacy laws like the CCPA, de Guzman said.

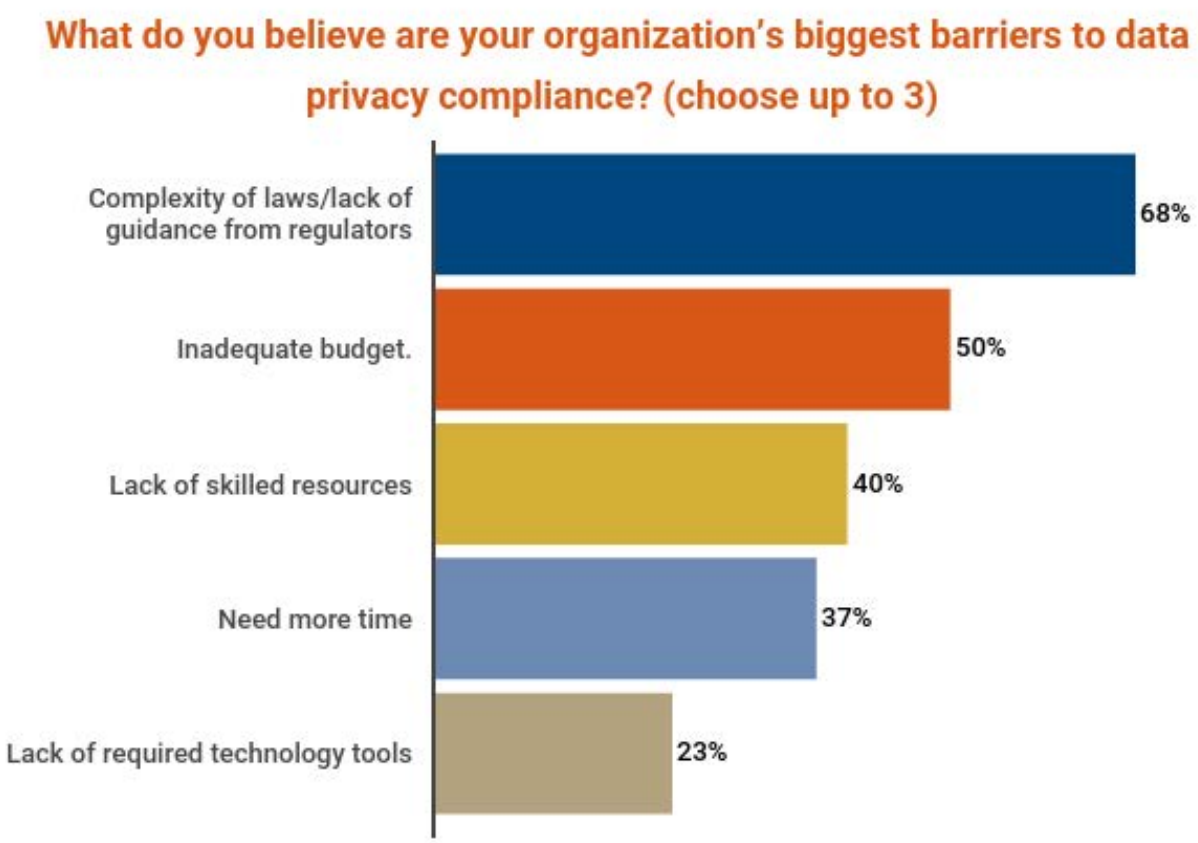
"More and more, organizations are seeing the benefits of a single technology partner over the multi-vendor approach," she said. "When companies and governments go with a single strategic technology partner—one with a broad product portfolio—it allows them to collaborate on a multi-year strategy to meet agreed upon objectives together."

CCPA, and CCPA 2.0—a.k.a. CPRA

California Attorney General Xavier Becerra's office began enforcing the CCPA on July 1, but it has not yet issued an enforcement action. Dominique Shelton Leipzig, a Los Angeles-based attorney with the law firm Perkins Coie, said a source within the AG's office told her that on July 1, notification letters were sent to companies identified as not in compliance with the law. The companies had 30 days to respond.

After that, the AG could decide the company resolved the issues and close the inquiry; extend the time period for the company to come into compliance; or file a lawsuit against the company through the state court system.

Shelton Leipzig said Becerra, through public statements,



indicated the AG's CCPA enforcement priorities would be placed on protecting the data of children, as well as on digital marketing companies that monetize the consumer data they collect. Companies that handle a large amount of personally identifiable consumer data—think utilities, telecommunications, social media, and others—may also draw the attention of the AG's office.

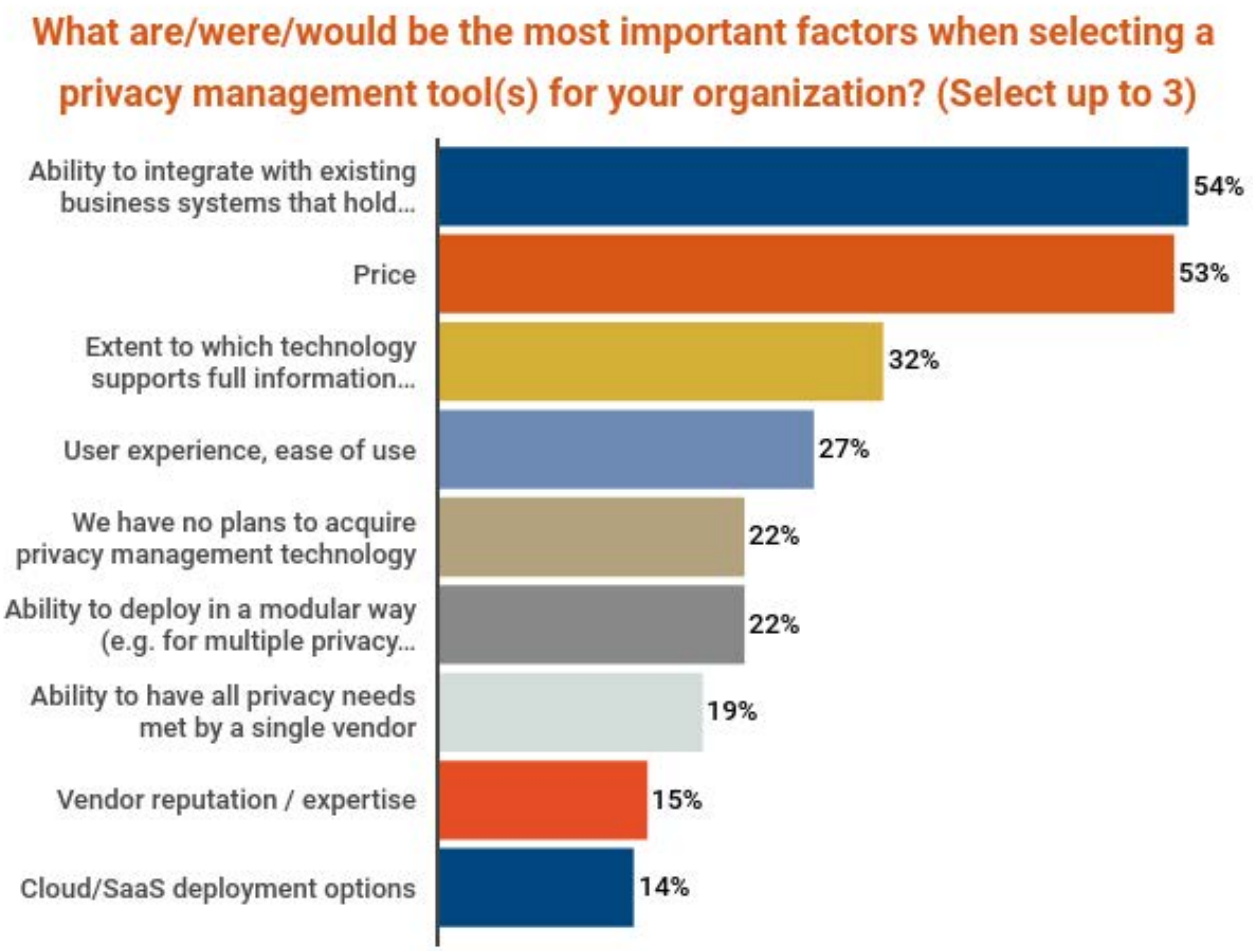
And there's another, stricter data protection law on California's November ballot, which has been called CCPA 2.0. Proposition 24 asks voters to enact the California Privacy Rights Act (CPRA) of 2020.

The ballot question has strong public support, according to an Aug. 3 poll paid for by the ballot question's proponent, Californians for Consumer Privacy. The poll found that among of 605 likely California voters, 81 percent support the measure. Proposition 24 has generated some opposition, including the American Civil Liberties Union of California and several other civil rights groups.

If passed, the CPRA would give consumers additional rights regarding their personally identifiable information (PII) over and above those granted by the CCPA. Some of those new rights include the right to correct PII; the right to delete PII; and the right to limit the disclosure of PII. A consumer opting out of the sale of PII under the CCPA could also opt out of the sharing of PII under the CPRA. Perkins Coie compares the two measures in this checklist.

The CPRA would also establish a new agency, the California Privacy Protection Agency, overseen by a five-member board and executive director to investigate violations and bring enforcement actions.

Firms could take more than three years to prepare for the rules, as the CPRA would not take effect until Jan. 1, 2023. ■



U.S. companies in limbo after Privacy Shield scrapped

Despite a ruling to scrap the EU-U.S. Privacy Shield, it's apparently still alive and well in the United States. Time to move on, opines **Aaron Nicodemus**.

Why are U.S. regulators keeping the Privacy Shield on life support? Is it because fashioning a real fix is too difficult?

For European regulators, the EU-U.S. Privacy Shield died July 16, killed by a European court decision. The legal protections that provided 5,300 American companies with safe access to EU citizens' data—without fear of legal reprisals under EU privacy law—died with it. The body in charge of enforcing EU data regulations, the European Data Protection Board (EDPB), later clarified the Court of Justice of the European Union (CJEU) ruling that it provided "no grace period."

The Privacy Shield, set up in 2016 to protect the personal data of Europeans when it is transferred across the Atlantic for commercial use, was voided because the court ruled U.S. surveillance laws clash with EU privacy laws.

Despite the ruling, the Privacy Shield is apparently still alive and well in the United States—with all of the regulatory and enforcement apparatus that accompanies it.

On the same day the CJEU handed down its decision, the U.S. Department of Commerce asserted it "will continue to

"We really need a political solution. It is unreasonable to put this burden onto companies."

Miriam Wugmeister, Co-Chair, Global Privacy and Data Security Group, Morrison & Foerster

administer the Privacy Shield program, including processing submissions for self-certification and re-certification to the Privacy Shield Frameworks and maintaining the Privacy Shield List," the Department said in a press release.

In an Aug. 5 statement, Federal Trade Commission Chairman Joe Simons backed the Commerce Department's stance in testimony before the Senate Committee on Commerce, Science, and Transportation.

"We will continue to hold companies accountable for their privacy commitments, including promises made under the Privacy Shield," Simons told the Committee.

From a purely pragmatic standpoint, that doesn't make sense. Businesses applied to the Privacy Shield program for the legal protections it provided. Those protections have disappeared.

Why would U.S. regulators like the FTC tell companies they should keep their Privacy Shield statements up-to-date, honor the EU-U.S. Privacy Shield Principles and Supplemental Principles, and complete a timely annual recertification with the Commerce Department?

Sure, it makes sense to comply with the spirit of the Privacy Shield principles. But do companies really need to keep filing the paperwork?

Theoretically, if companies don't comply with the Privacy Shield regulations, then they could still face potential lawsuits from the Federal Trade Commission, which "has taken law enforcement action against dozens of companies that made false or deceptive representations about Privacy Shield participation," the regulator noted a few weeks before the CJEU decision.

Even more crazy is that any business seeking to withdraw from the Privacy Shield List still has to notify the Commerce Department, complete a questionnaire, pay $200, and then decide whether to "return, delete, or continue to apply the Privacy Shield Principles to the personal information that it received while participating in the Privacy Shield." Let's face it: Without a valid Privacy Shield agreement to withdraw from, the process of withdrawing from the Commerce Department's Privacy Shield List might best be described as Kafkaesque. Or soul-crushing. Or just plain crazy.

What's really happening from the American side of the pond is a kick-the-can-down-the-road mentality. The "America First" Trump administration has its eyes on bigger trade victories than fixing the Privacy Shield and will likely punt any solution to, ahem, a second term. If Democrat Joe Biden becomes president, where do you think fixing the Privacy Shield will fall on his presidential to-do list?

"We really need a political solution," said Miriam Wugmeister, co-chair of law firm Morrison & Foerster's Global Privacy and Data Security Group. "It is unreasonable to put this burden onto companies."

Companies are left to sort out solutions on their own, such as standard contractual clauses (SCCs), which businesses have relied on for nearly 20 years to facilitate data transfers. The EU's General Data Protection Regulation has yet to provide updated language for SCCs.

The U.S. Chamber of Commerce encouraged the European Union and United States to "swiftly negotiate a new framework to support those companies that rely on Privacy Shield for transatlantic data flows." Any such solution would be Privacy Shield 2.0.

The Commerce Department announced recently that it had entered into discussions with its EU counterpart "to evaluate the potential for an enhanced EU-U.S. Privacy Shield framework." That ought to happen quickly, right? Six months to hammer out definitions, another six to haggle over them.

Wugmeister predicts that there won't be another Privacy Shield and that organizations are going to have to rely on new guidance from the EDPB on updated wording for standard contractual clauses.

Meanwhile, the Electronic Frontier Foundation, a nonprofit privacy advocacy group, proposed the long-term solution would be for Congress to overhaul the Foreign Intelligence Surveillance Act (FISA). "Fix U.S. mass surveillance, or undermine one of the United States' major industries," the EFF said.

This Congress? Overhaul FISA? Not likely. After all, they can't even seem to agree on whether to pay unemployed people an extra $600, $400, or $200 per month during a pandemic. ■

Oracle, Salesforce targeted in class-action GDPR lawsuits

Aaron Nicodemus has more on a recent lawsuit from a European Privacy Group alleging Oracle and Salesforce violated the GDPR.

A European privacy group recently announced the launch of a class-action lawsuit in Dutch court directed at American tech firms Oracle and Salesforce for alleged violations of the EU's General Data Protection Regulation (GDPR).

The group, The Privacy Collective, says it is preparing to additionally file a similar lawsuit in England and Wales. The group estimates damages sought through successful litigation could exceed €10 billion (U.S. $11.9 billion).

The lawsuit addresses "one of the largest cases of unlawful processing of personal data in the history of the internet," said Privacy Collective lead attorney Christiaan Alberdingk Thijm in a press release. It is also the first time a class action has been filed in the Netherlands related to alleged violations of the GDPR, according to the group.

The Privacy Collective alleges Oracle and Salesforce use cookies, bits of code that mark an internet user visiting a website, to collect personal information from individual Dutch users. The cookies are used to create "shadow profiles" of those users without their consent, according to the Privacy Collective. Under the GDPR, companies are obliged to ask permission of EU citizens before using their personal information.

The data contained in those profiles is "used, among other things, to offer personalized online advertisements and unlawfully shared with numerous commercial parties, including ad-tech companies," the group said.

The privacy group says it will also claim Oracle and Salesforce did not have informed consent to feed users' data to other companies who would then use it for advertising in a process known as real-time bidding (RTB), according to The Daily Telegraph in the United Kingdom.

Although the data is allegedly collected via cookies on online platforms like Amazon and Spotify, those companies are not named in the lawsuit.

Dorian Daley, executive vice president and general counsel for Oracle, said in a statement that The Privacy Collective "knowingly filed a meritless action based on deliberate misrepresentations of the facts.

"As Oracle previously informed the Privacy Collective, Oracle has no direct role in the real-time bidding process (RTB), has a minimal data footprint in the EU, and has a comprehensive GDPR compliance program.

"Despite Oracle's fulsome explanation, the Privacy Collective has decided to pursue its shake-down through litigation filed in bad faith. Oracle will vigorously defend against these baseless claims."

A spokesman for Salesforce told the Telegraph that the company "disagrees with the allegations and intends to demonstrate they are without merit." ■

opentext™

Empower your Privacy Office

Automate compliance workflows with intelligent and integrated privacy management capabilities, underpinned with the strongest information governance in the business.

Learn more at

www.opentext.com/data-privacy