Cybersecurity Law Report
An Acuris company

State Laws

CCPA Priorities: Turning Legislation Prep Into a Program Shift

Jun. 5, 2019

By Amy Terry Sheehan, *Cybersecurity Law Report*

The California Consumer Privacy Act is bringing sweeping change. This anticipated shift to the U.S. privacy landscape is just the beginning, with other states following California's lead, including Nevada, which enacted new privacy legislation just last week. While many affected companies approached the E.U.'s General Data Protection Regulation as a compliance project, they have now learned this growing trend requires a broader program shift. In this first installment of a two-part article series, we explore recommended privacy program goals in light of the CCPA, how to make the case for a holistic approach to implementation and why detailed compliance work should be ongoing. Part two will focus on how companies should prepare for two areas of the CCPA requirements – vendor management and data subject rights requests – which experts agree need to happen no matter what amendments to the law may pass.

Privacy teams should use the CCPA as an opportunity to advocate for resources and make lasting change. At the same time, those players must delve into the detailed work of compliance. "Companies should take a broader approach and look towards implementing enterprise privacy programs," Lindsay Hohler, a Grant Thornton senior manager, told the Cybersecurity Law Report.

See our two-part series on preparing for the CCPA: "Securing Buy-In and Setting the Scope" (Feb. 27, 2019); and "Best Practices and Understanding Enforcement" (Mar. 6, 2019).

Setting Privacy Program Goals

Privacy "is becoming more of a programmatic kind of function as opposed to just a project-by-project-based function," said Lindsey Tonsager, a partner at Covington. While some "companies are still just trying to implement something [and] they're just checking the box, most are really looking to implement enterprise programs and programs that will span the scale," Hohler said. Companies should try "to build something to scale for the future," she told the Cybersecurity Law Report.

There are a few common principles, priorities and goals experts shared with us that they advise companies to emphasize as they reshape their programs in light of the regulatory trend led by the CCPA.

See also "What to Expect From California's Expansive Privacy Legislation" (Jul. 18, 2018).

Proactive Approach

The goal is to stay ahead of the regulation race to shape a program that will meet the majority of any upcoming regulatory requirements, so that only updates for technological advancements or specific tweaks to address new legislation as it comes through are needed.

"Having a proper information governance and data privacy program internally is going to be key for all organizations going forward," Karen Hornbeck, a senior manager at Consilio, told the Cybersecurity Law Report. "This isn't a passing fancy. This is going to be coming up more and more – get in front of it and make the investment now in a proactive program," she added.

"Data regulations require scalable approaches. Instead of reacting to the changing regulatory landscape after each new regulation, the right data governance tools can put you one step ahead as a data-first, customer-centric business," Daniel Wu, privacy counsel and legal engineer at Immuta, told the Cybersecurity Law Report.

Wu recommended "creating automated data governance systems that allow you to get ahead of the curve," adding that "regulations require approaches that reduce human error by protecting data by design and save people time and money."

Dedicated Team

There is a growing recognition that "a dedicated professional staff can help the company comply with [regulations] and design products with privacy in mind. Depending on the organization type and how much personal data it processes, sometimes there is a large team led by a chief privacy officer and other times there might just be one person," Tonsager noted.

As long as there are dedicated people – with the number commensurate with the unique risk and size of the organization – companies can determine where to house the team based on their structure and needs. Companies house the function in different spots. "Sometimes it sits within compliance, sometimes it's in legal, sometimes it's in IT security," Tonsager explained.

See also "Advice From CPOs on Nurturing Privacy Programs on Any Budget" (May 17, 2017).

Cross-Functional Collaboration

"Often, if you don't have a mature privacy program, you may not have built a bridge yet between the privacy folks and IT security," Tonsager observed. "You might not have communicated with the businesses yet about why it is important to think about privacy throughout the life cycle of designing and launching a new website, mobile app or product."

For companies with less evolved programs, a foundational task is forming "the relationships within the business to start creating a culture of privacy," Tonsager said. "I think building those internal relationships and bridges is the most important because you need that culture in order to really make a shift in the company's practices."

See our two-part series on insights from Uber: "An Inside Look at Its Privacy Team Structure and How Legal and Tech Collaborated on Its Differential Privacy Tool" (Nov. 28, 2018); "Building Bridges Between Legal and Engineering" (Dec. 5, 2018).

Cybersecurity Framework

It is "really important to not get caught in the regulatory vortex," explained Paul Ferrillo, a partner at Greenberg Traurig. Adopting a framework helps avoid rushing to make major changes,

and "adopting a cybersecurity framework in a reasonable, prudent and efficient fashion won't cost you a fortune."

If you have the board involved when adopting a framework and stick to it, "then managing issues that come up like NYDFS or CCPA are much easier and you're not rushing around spending money like a chicken with its head cut off," Ferrillo told the Cybersecurity Law Report.

See also "NIST Program Manager Explains Pending Changes to Its Cybersecurity Framework" (Jan. 18, 2018).

Accountability

"There's a lot of talk about how the CCPA is a GDPR-like law, but it's really different; it's not an accountability-based law," said Nymity co-founder Terry McQuay, noting that in order to be "more proactive and not have fire drill after fire drill," companies should "restructure their approach" by putting in place "a privacy management infrastructure." This allows them to maintain accountability over time and to absorb and address any new privacy or data protection laws.

Making the Case for Program Change

Privacy, legal and compliance professionals can and should use the CCPA as an opportunity to advocate for program resources and change. There are numerous reasons to make these changes, and the CCPA helps provide compelling and timely arguments to justify budget.

Getting buy-in is not always easy but it is necessary. "Going out and hiring outside counsel, consultants or a technical software vendor provider isn't going to get you where you need to be if within the company you don't have that buy-in that privacy protection matters," Tonsanger said. In addition, to successfully advocate for change, Wu recommends "understanding the pain points of the stakeholders you wish to gain the support of."

See "Fifteen Tips for an Effective Cybersecurity Board Presentation" (Oct. 10, 2018).

CCPA Is Here

Some leaders may ask "why is now the right time?" Because companies are going through CCPA preparation right now, there is an opportunity for that work to be harnessed far beyond preparing for the CCPA effective date next year.

While some companies will be able to leverage the work they did for GDPR compliance to address CCPA compliance, others could "leverage what they are doing in California to either kickstart a privacy program or lay a foundation for putting privacy management structures in place," McQuay explained. They should focus on "how can this work can be used [beyond] just for California."

More Regulation Is Coming

The CCPA is one law within a growing trend domestically and internationally. "A number of different countries and regions have enacted their own data protection or privacy laws including Europe, China and Brazil, and India is also considering regulation," Tonsager said. "In addition to California, many states are considering their own versions of these laws."

U.S. federal regulation is also on the horizon. “No one expects CCPA to be the last regulation in this space. We all believe there will be further federal regulation at some point,” Hohler said.

“Whether it’s California, Washington, Illinois or New York, it doesn’t matter, more regulations are going to be coming and, similar to how the current breach notification laws are slightly different for each state, there is absolutely the possibility that each state’s privacy regulations might be just a little bit different,” Hornbeck said. “But ultimately, it still goes back to needing a strong information governance and data privacy program."

Further, the laws that are enacted will continue to change in this dynamic area. “The laws will continue to evolve with the technologies and the types of data that are being collected and what regulators see as the biggest privacy risks,” Tonsager explained. “That’s why it is so important to think about these things programmatically rather than just thinking you can snap your fingers, say ‘I’m done’ and move on to the next thing.”

See also “Analyzing New and Amended State Breach Notification Laws” (Jun. 6, 2018).

It’s What Consumers Want

The CCPA itself came from consumer-referendum efforts. “We know that regulations are driving a lot of this change, but the reason behind it is also coming from consumers. They want to be able to trust where they are handing their data over to,” Hohler said. “This is a shift caused by what the consumer is telling us.”

It is important to “build customer trust and digital ethics around you are going to use the data once you receive it and try to look at the privacy program as more of part of the customer experience,” Hohler said. “It is not just about the compliance side.”

Reputation Protection

High-profile privacy and data security issues in the news have helped “privacy professionals demonstrate the case for why this kind of more programmatic approach is needed because privacy isn’t just a legal or a compliance issue anymore. It’s a reputational issue,” Tonsager explained. “No member of a board and no CEO wants to wake up and find themselves or the company on the front pages. I think people are more sensitive to privacy being a critical piece of product design and how the company operates at a broader level.”

The CCPA enforcement and private right of action provisions mark increase risk of regulatory enforcement as well as private class action litigation. As a result, the CCPA only increases the risk for reputational harm.

What Will Not Work

Quick Technology Fixes

Technology can play a valuable role in meeting regulatory requirements and expectations, however, it is not a substitute for thoughtful planning and effective leadership.

Hornbeck receives a lot of questions about what technology clients can and should use to comply with the CCPA. Clients ask, “‘Can we just put a tool in place to fix this or to handle it?’ And while there are some tools out there, this is much larger than just a technology issue,” she said.

"Technology can help a lot in terms helping you understand what you have and where it's stored," Hornbeck said. And "technology can help if you put the right processes in place, but you still have to have an overall approach to what you're doing."

GDPR Repeat

Certainly, companies that went through GDPR prep are in much better shape than those that did not. For example, "organizations that put in place a 'records of processing activities' (required under Article 30 of the GDPR) are leveraging this to address many compliance aspects of the CCPA," Teresa Troester-Falk, chief global privacy strategist at Nymity, told the Cybersecurity Law Report.

But simply repeating the GDPR preparation project for California will not work. In addition, many companies do not want to repeat certain mistakes they feel they made while preparing for GDPR. "GDPR was a boondoggle for many vendors. There were a lot of scare tactics going on," Ferrillo said.

"A lot of clients who are trying to determine if they can take what they did for GDPR and just reuse it for the most part. And, while there is a lot of overlap, obviously not everything is identical between the two pieces of regulation," Hornbeck explained. "So, when they ask, 'Can't I just reuse it if for GDPR?' The answer is mostly 'no.'"

Differences between the GDPR and CCPA include the specific rights provided to consumers and business requirements such as the CCPA mandate for businesses to include communication channels for their users to opt out of data sharing," Wu explained. In addition, CCPA goes beyond GDPR's third-party requirements in Article 28, he added.

See also "Using Technology to Comply With the GDPR" (Feb. 14, 2018).

This material has been printed by and is for their consumption only. The full Terms of Use are available at www.cslawreport.com.
UNAUTHORIZED USE OR DISTRIBUTION IS UNLAWFUL