Cybersecurity Law Report
An Acuris company
cslawreport.com

February 27, 2019

STATE LAWS

Preparing for the CCPA: Securing Buy-In and Setting the Scope

By Amy Terry Sheehan, *Cybersecurity Law Report*

If preparation is not underway for compliance with the California Consumer Protection Act, it should be. The effective date of January 1, 2020, is approaching quickly, and the law is more complex, takes more time and is relevant for more companies than many realize. To obtain buy-in, company advocates need to be prepared to correct and counter several misconceptions that are keeping some organizations from launching their compliance efforts.

Organizations should start by gaining an understanding of their data and inventory their current controls in order to conduct a gap analysis and determine the compliance plan budget, scope and action list. Further, experts agree that organizations should take discussions surrounding CCPA as an opportunity to transform practices that they will need to change in the near future whether they fall under the GDPR or CCPA. Trying to "skate by" with the status quo is a "huge mistake," Davis Polk partner Avi Gesser told the Cybersecurity Law Report.

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

Start Now and Obtain Buy-In

The CCPA goes into effect on January 1, 2020. While July 1, 2020, is the official enforcement date, there is not a grace period as the state will be able to bring enforcement actions for noncompliance beginning January 1, 2020.

Companies should not wait any longer to begin preparations and hopefully have already started the process to determine if they fall under the law. Cynthia Larose, a partner at Mintz Levin, is advising clients "not to sit on the sideline. This takes longer than anyone thinks it does. We have clients that are still struggling to implement GDPR and they started 18 months before May 25th. But everyone needs to pay attention to developments because there are a lot of moving parts here."

It is important to start the process and limit the compliance issues going forward. Each year companies increase the amount of data and number of devices connected to their system, Gesser explained. "Companies aren't static; they're growing all the time, and the sooner this process is started, the sooner they stop acquiring businesses or practices that are inconsistent with these kinds of obligations," he said.

As soon as possible, senior executives and/or the board need to be made aware of the CCPA in order to obtain buy-in and support for

CCPA-compliance initiatives.

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

Five Mistaken Justifications for Non-Compliance

Several misconceptions may be preventing some companies from launching their compliance initiative, including the following five misunderstandings:

1) We Aren't Consumer-Facing

Certain companies misunderstand the scope of the CCPA and think the law does not apply to them because they are not a consumer-facing company.

Often, "when legal tries to go in and sell the need for compliance resources, the business side" may push back because they incorrectly think that they do not need to comply because they do not sell to consumers, Larose said. However, "consumer" is "a misnomer in the title of the California Consumer Privacy Act. 'Consumer' is defined as a resident of California, period. You don't need to enter into a transaction with a person for them to qualify as a consumer under the California statute."

When the legal team makes its pitch for the funds it needs, it needs to understand the law and be ready to explain why the company falls under it.

The law defines "business" as an entity doing business in California that:

- has annual gross revenues in excess of $25 million;
- alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households or devices; or
- derives 50 percent or more of its annual revenues from selling consumers' personal information.

2) We Already Prepared for GDPR

Certainly, companies that have prepared for the GDPR are in a better position to prepare for the CCPA. However, companies should certainly not assume that because they prepared for GDPR they are compliant with CCPA.

Companies that went through a compliance process for GDPR often did it only for their European data. In addition, there are important differences between the regulations, which will be discussed in part two of this article. "Some US companies that analyzed GDPR compliance separated [data] out. They isolated the European data and said, 'we're going to apply this to all of our European data,'" Larose said, noting, "They may have chosen not to apply certain standards or GDPR-type rights to the U.S. data."

Companies may hold data in multiple locations. "Very few companies have their European data and their California data in the same places doing the same things," Gesser said. As a result, "even if a company went through the GDPR compliance process, it may not have dealt with part of the business that didn't have any European customers there." Companies that assume their GDPR preparation will suffice for

CCPA compliance "may be surprised how many areas within the company" were not included because no European data was involved.

See also "The GDPR's Data Subject Rights and Why They Matter" (Feb. 28, 2018); and "EY Global Data Analytics Survey Finds Lack of GDPR Preparedness and Need for Cross-Functional Collaboration" (Mar. 28, 2018).

3) Changes to the Law Are Coming

Some companies believe that they should wait for any and all amendments or clarifications to the law and for the implementing regulations from the California State Attorney General. However, "gaming" the potential changes to the CCPA "is very tough," Gesser said. Advocates on both sides continue to press for amendments. While business representatives have testified at state legislature hearings about how burdensome the requirements are, a pending bill that the California State Attorney General recently endorsed would expand the CCPA's private right of action, among other changes.

Experts do not expect the requirements to become much less burdensome. Plus, if they reduced the CCPA obligations too much, there would be another voter ballot initiative or "other states would step up as well as federal legislation," Gesser said.

"I think we'll see some clarifications from either the legislature or the Attorney General, because there are drafting inconsistencies and missing definitions," Larose said, noting, for example, that there is no definition for "household" or "device within a household." These potential clarifications, however, should not stop or slow the preparation process, as substantial claw backs are not expected. For example, regarding the expansive definition of personal information in the statute, while there may be clarification, Larose does not "expect the definition of PI to narrow because the breadth of the definition is key to the ballot initiative advocates."

See also "The Growing Role of State AGs in Privacy Enforcement" (Nov. 28, 2018); and "Understanding the Potential Implications of Pennsylvania's Newly Recognized Common Law Duty to Protect Personal Information" (Dec. 12, 2018).

4) We Don't Meet the Definition of a Business

While, most of the CCPA focus has centered on the requirements for "businesses," the statute regulates three different types of entities: businesses; service providers; and third parties. As such, companies should consider the obligations imposed by the other two categories as well. "A given entity could fall under all three categories, depending on its activities. And many entities will have more than one type of data flow subject to CCPA," Mintz Levin partner Brian Lam emphasized in a recent webinar where he presented with Larose.

5) We Don't Need to Comply

Even if a company is not subject to the CCPA, it should consider this an opportunity to put its data in order and prepare for the inevitable, experts repeatedly told the Cybersecurity Law Report. There are numerous state laws based on the CCPA that have been proposed in recent months and federal privacy legislation is becoming more likely.

Experts agree that organizations will need to

transform how they collect, store and share data in the near future, regardless of whether they are subject to the GDPR or the CCPA. "It's highly unlikely that you will not have to comply with these rules in the next two or three years one way or the other, whether it's California or some other state or federal regulation," Gesser said.

When the GDPR was first passed, Gesser similarly advised companies to use it to "justify to the board and management to spend the money to become GDPR-compliant" if possible because these types of requirements are not going away and companies will need to go through the process eventually to comply with state, federal or international law.

"Some companies couldn't get buy-in for GDPR because they didn't fall under it and did not collect EU-origin personal data. The issue is different when you look at California. Privacy departments have been advocating to map the data and have gotten resistance; [the CCPA] could be what they need to get the resources from the business," Larose suggested.

Understand the Project Scope

Once companies have determined that they need to comply with the CCPA, they need to take initial steps to understand how large and time-consuming that process will be. There are several factors that will contribute to how expansive the process will be, including whether the business will need to fundamentally change, how much relevant data the company has and what controls are already in place.

Will the Business Need to Change?

Depending on how a company gathers and uses data, complying with the CCPA may require fundamental changes to how it interacts with customers and how the business is set up. The company should know if these changes are necessary as soon as possible because they will be time- and resource-intensive and may require hard decisions.

"There are many companies that don't realize that a big part of how they get and profile customers is through the gathering, use and/or sale of alternative data like consumer profile data, credit card data, location data and internet traffic," Gesser explained. "And companies may be surprised what limitation the CCPA rules that require disclosure and consumer consent to use or sell that data places on the business."

Companies need to go "through enough of the analysis to understand whether becoming compliant will take a lot of work and time and may be disruptive to the company's business model," Gesser explained. "If the business model is dependent on some movement or use of data that is arguably inconsistent with the California law that will mean the company may have to change the way it conducts business in a meaningful way."

If a company determines it is unlikely to need to change the way it does business, it still may need to undertake certain technical changes, like changing the privacy notice, for example, Gesser added.

Know Your Data

Companies need to start the data inventory and mapping project immediately, if they have not begun already, experts agree. This initial step is crucial before companies can understand the scope of the project and start taking further

compliance steps. "After getting buy-in from executives, you have to understand what data [the company has and] where it is, so that we understand where our critical risks are," Alex Scheinman, a director at ACA Aponix, explained during a recent webinar.

The first thing companies need to do if they have not already is "undertake a comprehensive data-mapping exercise in which they determine where they are getting personal information and how they're collecting it," Joseph Facciponti, a partner at Murphy & McGonigle told the Cybersecurity Law Report. He offered several questions companies can ask to assess the data they hold, collect or share:

- Are they collecting it directly from consumers?
- Are they collecting it from other entities?
- Where is it stored?
- What is the data's lifecycle?
- With whom is the data shared?
- To whom is the data sold ?
- What kinds of permissions are in place?
- What kind of business relationships do they have with respect to that data?
- Is the company aggregating that data?
- Is the company de-identifying the data such that the law would no longer apply to it?
- How and when do they destroy that data?

"Having this information will allow them to start thinking about what it is they need to do to comply with the law and what kind of technical systems they need to institute to comply," Facciponti added.

"In order to be able to do a gap analysis, you have to know the data," Larose emphasized, elaborating that it is "really hard to come up with a compliance plan, timeline and budget, without knowing what data you have, how it moves and what third parties you're sharing it with," Larose said.

See also "Tracking Data and Maximizing Its Potential" (May 17, 2017).

Excluded Data

When analyzing what data an organization collects, holds, uses, shares and sells, it is important to understand what types of data are excluded from CCPA requirements. This includes the following:

- public information that's not considered personal information;
- de-identified or aggregated data that's not considered personal information;
- consumers that are not residents of California;
- data utilized to comply with local, state and/or federal laws (i.e., HIPAA, GLBA);
- data utilized to cooperate with law enforcement; and
- data involved in mergers and acquisitions that is not considered selling personal information under the CCPA.

Hedge Fund Case Study

For example, "a hedge fund may buy a whole bunch of data including credit card, location and satellite data, and use it for trading algorithms. The algorithm crunches all the data and predicts that a company is going to have a bad quarter based on the year-over-year change in the number of people at the stores' parking lots, the credit card purchases and the movement of people physically in the stores based on the location data. And based on that the fund shorts the stock," Gesser explained.

This type of algorithm "may be a huge part of the business, but the fund now looks under the hood and realizes a lot of this data isn't anonymized very well so that the location data can be easily reverse-engineered to reveal who the people are because the location data tells where they live and work. Once that is known, you can connect the credit card numbers, and automobile identity and other great data," Gesser said.

In a situation like this, the company needs to "make sure that when it gets this data, it's anonymized so well that it can't be reverse-engineered to figure out who the people are," he added.

Conduct a Gap Analysis

This data inventory and map analysis is necessary in order for companies to then "identify the gaps and put them in order of necessary remediation before January 1," Larose advised.

Once data mapping is complete or underway, companies should "assess [their] control environment," starting "with identifying any gaps in policies, procedures and the privacy notices," Scheinman explained. In addition, companies should "review third-party contracts for appropriate terms."

Leverage Existing Controls

When considering what changes to implement, "it is critically important for companies to leverage their existing controls and capabilities," Scheinman said. Companies don't want to "reinvent the wheel each and every time a new regulation comes up."

For example, if the company has recently gone through GDPR implementation, "while not all of the policies, procedures and notices can be leveraged for CCPA prep, there are certainly aspects to be utilized," Scheinman suggested. Following GDPR prep, "the workforce has heightened awareness around privacy," and the company has also implemented controls and updated policies and procedures. It has "a wealth of experience that it can leverage to create efficiency in its compliance exercises." But first, in order to leverage them, a company needs to inventory and understand what it has in place.

Consider Consumer Expectations

In addition to evaluation controls, after understanding what data there is and how it is used and shared, understanding customers' privacy and data protection expectations and comparing those expectations to reality is an important step in order to determine the scope of change that may be needed.

Following the mapping exercise, a "company should then ask itself if it were to disclose to people what data it has and how they use it and/or share it, what reaction would they get," Gesser said. "Do they expect consumers will think it's fine (making consent easy) or will they say they didn't know the company had their data, let alone what it was doing with it (making consent difficult)." If the latter, "companies should next analyze if they really need the data and if they do, how will they get consent," he advised.

Make a Compliance Plan

After determining the scope of the project through data mapping, control inventory and gap analysis, companies can set a more detailed plan of what needs to be done to

achieve CCPA compliance by January 1. Scheinman set out this suggested compliance 2019 timeline:

- First Quarter:
  - plan for CCPA roll-out;
  - inventory and map data;
  - determine implicated third parties; and
  - start privacy readiness assessment.
- Second Quarter:
  - issue vendor diligence;
  - complete privacy readiness assessment, work through results;
  - document your data inventory and identify high risk processing; and
  - implement new security controls as necessary.
- Third Quarter:
  - update vendor contracts with data processing addendums and other control requirements
  - update privacy notice;
  - send new privacy notice to clients/ employees;
  - post new privacy notice on website;
  - issue website for verifiable consumer request (VCR) submission; and
  - obtain toll- free number for VCR submission.
- Fourth Quarter:
  - update incident response plan;
  - run through sample request submission and steps to take;
  - deliver staff training; and
  - review insurance coverage.