Ep. 31: CCPA: Impacts and Significance for Business

April 15, 2020

Jose Garriga: Jose Garriga: Hello, and welcome to *OnAir with Akin Gump*. I'm your host, Jose Garriga.

Privacy and data security are headline issues for consumers, and top-line agenda items for businesses around the U.S. and internationally. One state that has taken strong legislative action on the topic is California, whose California Consumer Privacy Act, or CCPA, took effect January 1.

Analogous to, and perhaps inspired by, the EU's General Data Protection Regulation, the CCPA is broad in scope, and vigorous in its assertion of rights and penalties. Given the oft-cited statistic that California's would be the world's fifth-largest economy were it a sovereign nation, its laws and its markets are unignorable by other states and even the federal government.

In this episode, Akin Gump cybersecurity, privacy and data protection practice co-heads Natasha Kohne and Michelle Reed will be discussing the CCPA, its significance on the state and federal levels and some of the key issues and implications raised by the CCPA that listeners should be aware of.

Welcome to the podcast.

Natasha, Michelle, thank you both for appearing on the show today. We have a lot of ground to cover, so let's get started. To begin with, Michelle, could you provide listeners a bit of background concerning the CCPA and why it's considered significant as a bellwether for state-level and even federal privacy legislation?

Michelle Reed: Sure. The CCPA is the innovation of real estate developer Alastair Mactaggart. His story really began with a conversation that he had with a Google engineer. That engineer told Mactaggart that he would be horrified to know how much data Google collects on its users. After that, Mactaggart, who really, by all accounts, is a political novice, learned about the ballot initiative process in California, which is a very powerful but often controversial tool that Californians use to ultimately drive state policy, and that resulted in an extensive negotiation that became a legislative effort, the CCPA.

The reason CCPA is considered so important on the privacy landscape is because CCPA is the first comprehensive privacy law enacted in the United States. Before its passage, the only privacy laws in the United States were generally sectoral, so, if you think about HIPAA [*Health Insurance Portability and Accountability Act*] for health care or Gramm-Leach-Bliley Act for financial services, COPPA [*Children's Online Privacy Protection Act*] for children's online privacy, and various others.

Europe had actually made sweeping changes to its comprehensive privacy law with the passage of GDPR, and the CCPA really doesn't follow in the GDPR's footsteps but does only to the extent that it is really a comprehensive privacy legislation. So, it's not aimed at a single industry. It's not aimed at a single right or a single responsibility, but, rather, addresses privacy on a comprehensive scale.

Jose Garriga: Thank you. Michelle.

Natasha Kohne: Just to add to what Michelle said, the CCPA was a catalyst for producing state legislation across the country, and, by our count, since the CCPA passed, around 26 states introduced legislation across the country. Also, this catapulted the federal government into action. I mean, some businesses spend around a hundred thousand to millions of dollars just in getting ready for the CCPA, so I think businesses are really vying for the federal government to act and to potentially preempt the CCPA.

Jose Garriga: Thank you. Let's stay with you, Natasha. There are a few terms noted in the CCPA that stand out, and I think have been commented on fairly extensively in the public forum. One of them is “private right of action,” and the other is “reasonable security.” Could you explain what they mean and their significance?

Natasha Kohne: Sure. These are some of my favorite subjects as it relates to the CCPA. I think that the private right of action is really a game changer, and just specifically to describe it, it gives California residents an explicit right to sue businesses if their personal information is compromised, and if their personal information is compromised as a result of a business's failure to maintain reasonable security.

Now, the main issue with the private right of action is that the statute calls for statutory damages, and those damages include $100 to $750 per consumer per incident, whichever is greater. Now, let's just put that into context for a little while. If there is a breach of unencrypted and unredacted personal information for, let's say, around 100,000 California residents, then the potential minimum exposure at $100 per consumer—for one incident—is $10 million. This is a significant sum of money for a relatively small breach and definitely more than we've been seeing generally in settlements.

So, the bottom line is: We do expect to see an uptick in data breach litigation, and we think the inclusion of these statutory damages really incentivizes plaintiffs’ lawyers to bring claims, not just against some of the larger companies, which is what we've seen historically, but also against the smaller and midsize companies. That's because, in the 9th Circuit especially, plaintiffs may now believe that, because of these statutory damages, it'll be easier to establish harm, they might have an easier time getting past the initial stages of litigation and then they can tee up a settlement quickly since many of these companies may not want to spend the resources to continue to summary judgment or trial, which, in turn, I think, continues to incentivize plaintiffs to bring cases when breaches are just frankly smaller in numbers.

Lastly, I think that leads me to the issue of reasonable security. We do think that reasonable security will be heavily litigated now because it's an element of the private right of action in California under the CCPA. And whether a business has reasonable security is such a fact-intensive inquiry. Plaintiffs may ask all sorts of intrusive questions during discovery about the implementation of the business' information security plan and pick at any flaws in those plans or the implementation of those plans. And as we all know, it's almost impossible to maintain perfect security. So, it's a real dilemma for businesses because plaintiffs' lawyers will hone in on some of these inevitable weaknesses.

So, the narrative around what a business does to ensure the safety of consumer data will even be more important for us to focus on before and after a breach occurs.

Jose Garriga: Thank you, Natasha. So, let's circle back a bit. We had talked about state-level legislation a little bit, and Michelle, how does CCPA compare with other state-level privacy legislation from the business perspective, and are states copying CCPA in their own bills?

Michelle Reed: That's a great question. So, there are only three states that currently have privacy laws on the books: California, Maine, and Nevada right now. They differ pretty significantly at this point. California gives lots of rights and plenty of requirements: right of deletion, right of portability, right of opt out, right of action for data breaches as Natasha outlined, notice and transparency requirements, and prohibition on discrimination for exercising rights.

The other states are a lot more narrow than the California. For example, Maine has a right of restriction, so it has the right to restrict a business's ability to process personal information about the consumer. It has opt-in requirements, notice and transparency requirements and has a similar prohibition on discrimination but doesn't have several of the other rights that are outlined in the California legislation, particularly the private right of action.

Nevada's even, I think, more narrow than that, which provides a right of opt-out and has notice and transparency requirements. Also their privacy legislation tax on data breach notification requirements, which, frankly, all 50 states and all the U.S. territories now have. So, the reason why California, ultimately, serves as the bellwether is because it's the most comprehensive.

Now, there's many states that have proposed legislation that, really, substantially mimics it. There was a competing proposal in Washington, really, which took a more GDPR-like approach than the CCPA did. Ultimately, that bill failed because the House and the Senate in Washington were disagreeing particularly on whether there should be a private right of action included in that. We'll see if it gets proposed again and what the next steps are. I don't think it's down and out forever, but certainly at this point, it's considered not passed.

There are bills pending in Florida, Hawaii, Illinois, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey, New York and Wisconsin, and there's active task forces that have replaced bills in Connecticut, Hawaii, Louisiana, Massachusetts, North Dakota and Texas. So, I think as the next years unfold, you're going to see lots of legislation that pops up all over the United States. I think it's going to differ from state to state.

Clearly, the hottest point on these legislation that's causing the most contention amongst houses and senates and the various governing bodies is the private right of action. Obviously, a lot of people consider that to be very concerning and adding a lot of costs and risks for businesses, and, on the flip side, the privacy advocates claim that, without a private right of action, it's going to be without teeth. I think it remains to be seen where it ends up.

I think that the CCPA is ultimately going to serve as a really important data point on whether or not a private right of action passes another stage because if they see tons and tons of litigation at high cost in California, I think it's unlikely that the private right of action will pass in the others. But if you see a more measured approach in California, I wouldn't be surprised if, ultimately, you saw more private rights of action included.

Natasha Kohne: And just to that end, I think, at the federal government level, the private right of action is also a contentious point that our federal government cannot seem to agree upon. In addition to what is preemption going to look like as well as what is the role of the FTC, will the FTC actually have more power and more teeth to issue fines, or will it be business as usual and the status quo?

Jose Garriga: Thank you Natasha. Let's stay with you because another topic that stands out is attorney-client privilege. What are some of the things listeners should be considering in the context of the CCPA?

Natasha Kohne: Thank you for that question, and this question might be a bit self-serving, but I think, honestly, the CCPA makes it more imperative for businesses to think through how to use lawyers, not just when they experience a data breach, but also before any breach actually occurs. For example, it's commonplace now for regulators in certain industries to require businesses to conduct risk assessments of their information security programs.

Now, these risk assessments often identify gaps in a business' programs, and then they prioritize risks within that organization. But the problem is that these risk assessments can also sometimes serve as roadmaps for security flaws within an organization, and plaintiffs' lawyers may ask for them during a data breach litigation. So, businesses should really think through ensuring that these risk assessments are conducted under the privilege. Consider: what are some of the best practices businesses can use to maximize the privilege?

I think it's also very important for businesses even more so now to ensure that outside counsel or, at a minimum, their in-house counsel is involved in their data breaches from the very beginning. The likelihood of being sued is even higher now, and businesses really cannot risk that their entire data breach investigation is deemed non-privileged because it wasn't conducted at the direction of lawyers or under the umbrella of the attorney-client privilege.

There is an abundance of case law in the data breach contexts where some companies were successful in maintaining the privilege of their forensic reports, for example, and some were not. So, I'd recommend that businesses and their outside counsel know these rulings cold and when the privilege sticks and when it doesn't.

Michelle Reed: I think that there are some really complex considerations that companies have to make when they're going through these investigations because any kind of reporting that comes out of a data breach is going to be desired by many different parties. So, you know, clearly, if you're sued in a class action related to it, the plaintiffs will want to see

that report. If you've maintained the privilege, you can protect it. But, on the flip side, oftentimes you have the auditors who want to see the report. You have state attorneys general who want to see the report. You have Department of Justice or other agencies who would like to see the report.

So, there's some really serious strategic considerations on how to compile the reports, who to share the report with, how to maintain the privilege on the report. Because, newsflash, when you share it, it can be challenging to maintain the privilege; not impossible, but it can be challenging. All of these considerations need to be made by experienced counsel and experienced consultants who deal with this on a day-to day-basis so that you set up the company for success.

Jose Garriga: Thank you both. A reminder, listeners, we're here today with Akin Gump cybersecurity, privacy and data protection practice co-heads Natasha Kohne and Michelle Reed discussing the impact and implications of the California Consumer Privacy Act.

Natasha, you mentioned the California plaintiffs' bar. Previously, we've discussed the plaintiffs' bar on the show. What are the principal CCPA-related issues that are being raised by the plaintiffs' bar that business owners should know about, and are class actions being filed under CCPA?

Natasha Kohne: Yes, this is a good question, and it's actually a question we've been waiting for ever since January 1 has passed, and, predictably, we are seeing CCPA claims being filed already. We saw one very early in January, then many being filed in February. But, interestingly, we're also seeing CCPA claims being filed not just in the context of a data breach. So, the private right of action really only relates to the context of the data breach. We were concerned that the plaintiffs' bar would try to use the private right of action and expand it outside of a data breach violation, and so was the California legislature, and they even addressed this issue when they amended the CCPA to make clear that nothing in the statute should serve as a basis for a private right of action under any other law.

And, yet, we are seeing CCPA claims being filed in cases where the crux of the case is about, for example, the failure by companies to give proper notice. So, there was a recent case where a plaintiff's lawyer cites to section 100B of the CCPA to argue that California residents require notice at or before the time of collection of personal information being collected by the business. Yet this type of cause of action is clearly prohibited by the CCPA. So we'll see how this all pans out in litigation, and whether plaintiffs will drop these claims, or whether these businesses are going to have to go ahead and fight these claims and hopefully get them dismissed.

We're also seeing cases where plaintiffs' lawyers are citing to the CCPA, not within a cause of action, but to show that a company, for example, knew of the risk of the CCPA because they cited it as a risk factor in their public filings. Or plaintiffs' lawyers might cite to the CCPA to argue that California has a strong interest in privacy rights, and that California resident data is valuable. So, we expect to see all sorts of different types of arguments, and we're monitoring these cases and not surprisingly, we're sitting here in March, and there are a number of cases that have already been filed with CCPA claims.

Jose Garriga: Thank you. Let's look at something else. You mentioned it's March. The CCPA took effect January 1st, but, just last month, the California Attorney General Office issued revised proposed regulations regarding CCPA. How do these proposed regulations change the legislation? Natasha, please?

Natasha Kohne: Well, I think just to back up and provide the timeline, I think that's important and interesting here. I mean, the attorney general first issued draft regulations last October; they were definitely more than what we bargained for. He seemed to go out of his way at the time to add additional requirements to the CCPA that can be viewed not just as interpretations of the law.

Just to give you an example—I like examples—he had businesses required to respond to consumer requests even when those requests were deficient. He's also requiring businesses to tell third parties not to further sell personal information when those businesses received opt-out requests. These were requirements that were not in the law, and we think actually go beyond just interpreting the law. Then, in February, he issued extensive modifications to the regulations, and I think, on balance, we viewed those as a little bit more business friendly.

Just to give you another example, for a long time, it wasn't really clear how service providers could disclose personal information to their own subcontractors without triggering a sale. So, it seems that, in February, the attorney general cleared that up along with a few other business-friendly modifications. Then, actually just around two days ago, we got additional modifications—we can call that sort of “version 3.0”—and I think some of these comments continue to be helpful to businesses. But one of the most controversial modifications that he made back in February where he actually tried to clarify what the definition of “personal information” is, well you can say that, that potential clarification backfired. He ended up deleting this modification completely at the behest of some of the privacy advocates.

So, I think overall, this has really been an iterative process, where we're sort of taking two steps forward, maybe one step back. For every clarification, we sometimes get a little bit more confusion or some more onerous requirements on businesses. But we are getting there, and I think the first question that our clients are asking us is, "How many more rounds are we going? When is this going to stop?" My hope is that we are almost to the finish line on these regulations.

Jose Garriga: Thank you. So, now in closing, how would listeners know if they have CCPA compliance obligations and what are some next steps that listeners should take to ensure they're compliant with CCPA? Michelle, if you would, please.

Michelle Reed: Sure. So, the CCPA applies to businesses that do business in California, that collect personal information, that ultimately alone or jointly with others determines the purposes or the means of processing that data. Then they have to satisfy at least one of the following things. They have to either have annual gross revenue in excess of $25 million; they have to alone or in combination annually buy or receive for commercial purposes personal information of at least 50,000 consumers, households or devices; or they have to derive at least 50 percent of its annual revenues from selling consumers’ personal information.

Now, there's some other details that obviously you want to do a real analysis of how it applies to you, but I think, in general, most businesses that do more than $25 million and have California residents, they're going to be stuck having to comply with the CCPA. So that leaves, I think, the most important question, which is what should they be doing?

There's a lot of companies that really had a mad scramble at the end of 2019 to comply. I'll say throughout this year, we've definitely advised clients on CCPA as other

companies, a lot of times outside of California, realize that the CCPA applies to them. So, the first step is to determine whether or not you are covered by the CCPA. If you are, the next best step is to conduct a data inventory or some kind of mapping exercise that assesses what data flows and how personal information is used, processed, shared across all the various entities of your organization.

That's a really extensive process. It requires time and effort and for people to really dig in and see how data is being used. Then another really important consideration is to identify key vendors and whether or not you're going to characterize them as service providers or third parties. The CCPA treats vendors differently if they are service providers with the proper contractual provisions or if they are ultimately considered third parties. So, evaluating the vendor program is critical. Then making sure that you adopt mechanisms to provide the required notice at or before you collect personal data. You update privacy policies, online privacy policies, and make sure that if you're selling data that you have a "do not sell" button on your website, and you have procedures to facilitate that opt-out.

It's important to have a consumer request tracking and response system. There's rights that consumers have, and they're going to send it in, and if you don't have a way to track it, you're likely not going to be able to comply with the very short requirements on responding to those requests. Then you want to make sure that your employees are trained and that your internal policies and procedures are updated to comply with the CCPA.

Then, I think this gets a little bit to what Natasha was talking about earlier, you want to lay the groundwork for later application of safe harbors. For example, using redaction and encryption when you're dealing with personal information and then making sure that you have procedures in place that you could characterize as reasonable security so that you can ultimately use the safe harbors. You want to adopt or create a system for tracking violation notices—they require you to monitor that.

Then this is a key tip that I think a lot haven't necessarily thought through, but you want to evaluate customer incentive programs. If you have differential pricing for something, you give rewards for sharing information or for providing information, you want to really evaluate that to make sure two things: Number one, that you're not discriminating against people who say, "I don't want you to have my information," and number two, if you say, "No, we're not discriminating against it. It's just that we put a value on your information," think through what that value is. Because sometimes I've seen companies look at it, and they have some sort of promotion, they use it through a loyalty program, and then they later discover that, that differential pricing that they say is used so that they can essentially have their data, the access to their personal data, can get thrown back at them in litigation and can really start, in a plaintiff's mind, to quantify damages.

Obviously on the defense side, we would dispute that as an unreasonable approach, but certainly something to consider when you're looking at a differential pricing option. So, there's lots of things to do, lots of work to be done. But I think companies are working hard at trying to comply.

Natasha Kohne: Just to add to what Michelle said, in particular focusing on the data mapping exercise, the CCPA has a number of exemptions in it. Now those exemptions are really based on personal information. They're not exemptions based on institutions or entities. So, I think it's important, in thinking through your obligations, to determine what data is protected by

Gramm-Leach-Bliley? What data is protected by HIPAA? How much employee data do you have? What data do you collect in the B2B [*business-to-business*] context?

Right, now there are exemptions that exist for each of these situations. Almost all businesses have additional data outside of these circumstances that they have to think through. So the data mapping exercise is super important to determine what groups of data sets are applicable to the CCPA. I think the last thing also to emphasize is that virtually every exemption that the CCPA has is not a full-scale exemption. So, even if you have an employee exemption right now in place for the next year, that it's not a full-scale exemption, and you still will have obligations to your employees under the CCPA. So, just remember that exemptions are not a full exemption of the CCPA. There are provisions that are still applicable.

Jose Garriga: Thank you. Listeners, you've been listening to Akin Gump cybersecurity, privacy and data protection practice co-heads Natasha Kohne and Michelle Reed. Thank you both for making time to appear on the show today and specifically for providing listeners with this terrific roadmap to this business-critical legislation.

And thank you, listeners, as always, for your time and attention. Please make sure to subscribe to OnAir with Akin Gump at your favorite podcast provider to ensure you do not miss an episode. We're on, among others, iTunes, SoundCloud and Spotify.

To learn more about Akin Gump and the firm's work in, and thinking on, CCPA and related matters, look for cybersecurity, privacy and data protection under Practices at akingump.com, and take a moment to read Natasha and Michelle's bios on the site as well.

Until next time.