Ep. 58: 2021 CCPA Litigation Report – Overview and Findings

May 11, 2022

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

I last sat down with two of today's guests a year ago to discuss what was then the firm's new *2020 CCPA Litigation Annual Report*. A year has passed, and much has happened in the world of litigation and class actions related to the California Consumer Privacy Act.

Akin Gump lawyers researched all of this litigation activity, compiled their findings, and analyzed their significance in the firm's brand-new *CCPA Litigation Annual Report - 2021 Trends and Developments*.

So, returning to the show today are the co-heads of Akin Gump's cybersecurity, privacy and data protection practice, Natasha Kohne and Michelle Reed, as well as counsel Lauren York. They'll be discussing the firm's new CCPA report, what they found out through their research, and what the rest of 2022 looks like for business in and about California.

Welcome to the podcast.

Lauren, welcome to the show. Natasha and Michelle, great to have you back. Our last episode, as I mentioned, looked at CCPA's first year, and we discussed that first report's findings and analysis. Coming back to the topic a year later, I'd like to share with our listeners where things stand and how they've developed.

To start, as I mentioned, it's been over a year since we last sat down to discuss the CCPA. Before we get into the numbers, and I know there's some very fascinating statistics coming out of this, but could you give listeners a brief description of what the CCPA is and isn't and then an overview of the trajectory of privacy-related litigation in California in 2021? Lauren, if I could ask you to lead off, please?

Lauren York: Sure. Thanks so much, Jose. The CCPA was the first comprehensive data privacy legislation to be enacted in the United States. As you alluded to, it went into effect on January 1, 2020. It really broke new ground in the world of data privacy legislation,

primarily because it provides a private right of action and the possibility of statutory damages to any consumer whose personal information is involved in a data breach resulting from a business's failure to maintain reasonable security. I think more noteworthy are also certain rights given to consumer-related personal information, including the right to know what information was collected about them and to opt out of having their personal information collected. In contrast to the private right of action, however, these rights can only be enforced by the California attorney general.

Turning to 2021, we saw courts really starting to clarify the meaning of certain CCPA provisions, such as which circumstances allow consumers to utilize that private right of action. Courts have uniformly decided in the last year that the private right of action is available only where a consumer's personal information has been accessed without authorization as a result of a business's failure to take reasonable security safeguards. So, more of what's really thought of as a traditional data breach. That's something that I think the report does a really good job of exploring as we look at the landscape over the last year.

Jose Garriga: Let's get into the report then. It's a terrific piece of work. I've had the pleasure of looking at it, and I will recommend it to our listeners. You can find it pinned to our LinkedIn page as well as on akingump.com. But looking at the report, Natasha, if you had to pull out one statistic that really told the story, what would it be?

Natasha Kohne: Thank you, Jose. It's great to be back. Thank you for inviting us back.

This is a really tough question. Our research revealed a significant number of pretty interesting findings. Overall, I think, one statistic is that we saw a 60% increase in the number of cases filed in 2021 versus 2020, and that's a significant statistic in and of itself.

But I think the headline statistic is really what Lauren already mentioned, and that is that we saw a major increase in the number of cases brought in the context of the data breach and a significant decrease in the number of cases brought where a violation of the CCPA was pled, but there was just simply no data breach in sight. In fact, over six unique defendants in 2021 brought cases outside of the data breach context. And that's out of the total of over 50 cases involving unique defendants.

At the close of 2021, there were only two cases not involving a data breach that remain ongoing or on appeal. For those of us who have been following CCPA data breach litigation, this is a real relief. I think the plaintiffs tried to take advantage of the wording in the statute that refers to "unauthorized access and disclosure," hoping that the courts would interpret that wording to fold in other types of data security instance. And so far, I think the courts have not yet, to date, bought into this more expansive interpretation.

Jose Garriga: Thank you, Natasha. Lauren, let's build on that a little bit. We've already identified some trends, but speaking a bit more broadly, what were the big trends that you would identify for listeners? And again, to what extent, and I think Natasha alluded to this, what extent did the extensive research you all conducted yield surprising or unexpected results?

Lauren York: Thanks, Jose. That’s a good question. There were a lot of trends, really, that were pretty noteworthy, looking at the 2021 case law. Just the sheer number of data breaches is one that really stands out. And what's interesting there is that with these data breaches, as Natasha said, plaintiffs are getting a little bit better at really focusing in on the exact text of the statute. We're seeing these traditional breach cases. When we talk about unique

defendants, we say that because, from a lot of these breaches, we're seeing a variety of cases predicated on the same breach. The overall number of cases filed in 2021 has really exploded over 2020. It's that 60% statistic, where our unique defendants number hasn't really changed. And I think that's something that's very interesting, that if there's a data breach, as a defendant, you're very likely, depending on the size of the breach, the scale of the breach, of course, all those different things, to potentially face litigation in a variety of jurisdictions across the country.

The other part of that, of course, is that as the plaintiffs' attorneys are honing their litigation strategy, we saw the number of claims based on the CCPA decline from 28½% in 2020 to only about 11% of cases in 2021. That's really as a result of courts rejecting plaintiffs' attempts to use the private right of action under the CCPA as a basis for another claim, such as negligence or breach of implied contract, something like that.

Third and final, the development that maybe surprised us the most is some emerging case law involving companies who have argued that they're not covered by the CCPA's private right of action because they're service providers rather than businesses. On the one hand, we have a court saying a company can be both a service provider and a business, but not at the same time. In that situation, whether the private right of action applies depends on what hat the company was wearing when the data breach occurred. On the other hand, we have another court that's saying a company can either be a service provider or a business, but not both.

We're starting to really see what could be a split emerging there, and with a statute that's so new, I think over the next few years, and we'll, I'm sure, talk about this as we go on in the podcast, those are the kinds of things that are really going to guide where data privacy litigation is headed and really have big impact on businesses and consumers heading forward.

Jose Garriga: Thank you, Lauren. A reminder, listeners, we're here today with Akin Gump partners Natasha Kohne and Michelle Reed, who serve as the co-heads of the firm's cybersecurity, privacy and data protection practice, and counsel Lauren York, whom you just heard.

To pick up a theme from our previous two episodes, and I want to bring Michelle in on the conversation here, regarding the CCPA, is the law's impact and influence on privacy legislation in other states. What's the legislation landscape like outside California nowadays, Michelle?

Michelle Reed: Emerson once said, "Do not go where the path may lead, go instead where there is no path and leave a trail." That's what California has done with the CCPA. They have gone where there was no path. There was no one who had comprehensive privacy legislation in the United States like they have in Europe and around the world. And California forged its own path. The other states have the choice on whether or not they're going to follow that path, or they're going to take their own trail. In 2021, Virginia and Colorado, they enacted their own laws. Utah joined them in 2022, and we're soon to have Connecticut joining while we wait the governor's signature on new legislation in Connecticut.

The CCPA, however, remains the most comprehensive of all of these laws, and it's the only one with a private right of action. We've seen comprehensive privacy legislation introduced in almost 30 different states, and we expect that the number of states with enacted laws will increase over time.

Ultimately, the frequency with which the plaintiffs are suing and the implications of having that private right to sue have strong implications in how many cases are brought and how often they're brought. We know that cases where there are statutory damages have damages that are more easily calculated and more certain than damages where we don't have statutory damages.

All of those things come into play as plaintiffs decide who, when, and where to sue. That also, therefore, has implications on what state legislatures do. And it looks like, so far, the states have fallen out where they're letting the state authorities be the enforcer as opposed to the private plaintiffs' bar. And when you look at the report and the statistics that Natasha and Lauren just went over, you can see why, because the number of suits that are being filed is truly growing astronomically every year.

Jose Garriga: Thank you. Shifting gears a bit, we've been talking about the CCPA. The CPRA, the California Privacy Rights Act, we started discussing it last year, and the deadline for final regulations implementing CPRA amendments is a few months away. So, Natasha, could I ask you, please, to bring listeners up to speed on the impact that CPRA will have on California and privacy litigation?

Natasha Kohne: Sure. If you look closely at the CPRA amendments to 1798.150, which is the private right of action provision, the CPRA amendments do not really change the private right of action much. You have the 30-day cure period, which is still in effect, but the statute makes clear that implementing reasonable security following a data breach does not constitute a cure. And the definition of personal information expands slightly, but that's pretty much about it.

The real impact the CPRA amendments have on privacy in California is that the privacy compliance and regulatory obligations on businesses are significantly enhanced. And the CPRA amendments bring the CCPA closer to the EU's comprehensive data protection legislation, the GDPR, which may truly require a fundamental shift in the way businesses think about their data practices.

Let me give you an example. Data retention practices and disclosures change significantly under the CPRA amendments, and how businesses will adapt to data minimization requirements when we're used to, frankly, over-retaining data remains to be seen. Other major adjustments we might see from businesses include how to treat sensitive personal information, as defined by the CPRA amendments, which may be a different data set from how a business's own industry defines sensitive personal information.

The CPRA amendments could very well spur additional litigation. There are new obligations that might inspire plaintiffs to bring a new wave of cases outside of the traditional data breach context. But if that happens, I don't think that's going to impact any of the outcomes that we have seen. Courts will likely continue to interpret the private right of action in a more narrow context, especially since the language of the CPRA amendments, as it relates to the private right of action, changes only slightly.

Jose Garriga: Thank you, Natasha. To wrap up, two years of the CCPA behind us. Michelle, I'll ask you to take this one, please. What would you say are the lessons that you all have learned about litigation defense and litigation deterrence that you think might be helpful to our listeners in the business community? And going back to a few points made earlier

regarding the plaintiffs and the plaintiffs' bar, have plaintiffs' tactics changed substantially from year one to year two? What do you think, Michelle?

Michelle Reed: Well, of course, the best litigation deterrence strategy is to implement reasonable security safeguards and compliance programs to prevent CCPA violations from occurring, so you don't have a breach. That's the best litigation deterrent. But I think, really, what people listening need to think about, since we're at the point where data breaches are not a matter of if, but when, they're going to happen, is a different question, which is, number one, what are you doing to decrease your data footprint?

Over-retention, that Natasha spoke about a little bit earlier, is critically risky for companies. The more data you have and hold unnecessarily, the more likely you are going to have notifications that are required, and, therefore, people potentially with statutory damages claims in the event of a breach. Companies really need to look closely at what they're doing to minimize data. What are they doing to understand what data they have, what data they need to have, and whether it's worth the business risk of carrying certain types of particularly sensitive personal information.

Under the CPRA amendment, we are going to have companies with a legal obligation to minimize the amount of data that they retain. I think that plaintiffs will use that very closely in their data breach suits that they bring to say, "You shouldn't have even had my data," and, therefore, maybe even see them making arguments of moving from a lower penalty to a higher penalty based on the violation. We'll have to see how they approach it.

The next recommendation I'd have is to shore up the vendor management practices. This is really tough because companies have so many different counterparties and so many businesses with which they share data. In 2021, we saw several vendor breaches that resulted not only in liability for the vendor itself, but also for the downstream customers of those vendors. Accellion is the most prominent example that you saw, where you saw individual companies being sued and a bunch of different lawsuits being brought all over the country, not just against Accellion.

Comprehensive vendor management program is great because it allows you to take a reasonable security safeguard. And then it also helps companies understand which vendors have access to which data, and how they can appropriately restrict access.

Now, your last question is, have plaintiffs' tactics changed from year one to year two? There has definitely been a change of litigation tactics. The big headline out of our report that was issued in 2021 was that plaintiffs were suing for any predicate violation, meaning any privacy violation that they saw that violated CCPA, we saw more of those cases than we saw of the data breach cases.

This year, that is not the case. The real exposure, from a private cause of action standpoint, is the data breaches. This doesn't mean that companies shouldn't be worried about CCPA compliance or the other privacy requirements. In fact, we know there is going to be administrative enforcement that will be increasing with the creation of the CPPA [*California Privacy Protection Agency*] by the CPRA amendment. Companies should keep an eye out on guidance from the attorney general, and they should be looking and staying up to date on enforcement priorities and common violations so that they can minimize risk, both at the private cause of action level and then also at the government AG enforcement level.

Jose Garriga: Terrific. Thank you. Listeners, you've been listening to the co-heads of Akin Gump's cybersecurity, privacy and data protection practice, Natasha Kohne and Michelle Reed, along with counsel Lauren York. Thank you all for making the time to participate in what we can call the show's third annual CCPA episode. I'm looking forward to the fourth annual already.

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, YouTube and Spotify.

To learn more about Akin Gump and the firm's work in, and thinking on, cybersecurity, privacy and data protection matters, search for “cybersecurity” on the Experience or Insights & News sections on akingump.com, take a moment to read in Natasha, Michelle's and Lauren's bios on the site, visit our *AG Data Dive* blog for insights and analysis on all matters related to cybersecurity and privacy, and, finally, visit our LinkedIn page, as I mentioned, or akingump.com to get your own copy of the 2021 *CCPA Litigation Annual Report*.

Until next time.