Barclay Damon Live Presents *Cyber Sip*™
Episode 42: "'California Emissions': Is the CCPA a Bellwether for the Rest of Us?," With Michelle Merola

Speakers: **Kevin Szczepanski**, Barclay Damon,
and **Michelle Merola,** Hodgson Russ

[Kevin Szczepanski]: Hey, everyone, this is a *Barclay Damon Live* broadcast of the *Cyber Sip*. Practical talk about cybersecurity. I'm your host, Kevin Szczepanski. Let's talk.

[Kevin]: We are back again with Michelle Merola, associate general counsel of Hodgson Russ and leader of that firm's Cybersecurity & Privacy Practice. Thanks again for coming back to talk to us, Michelle.

[Michelle Merola]: Happy to be here.

[Kevin]: So today we're going to talk about California, and I'm just going to start with a silly observation that I think makes sense today. So when I was a kid, I used to watch "The Price Is Right," and on "The Price Is Right," they would give away cars. And when Johnny Olsen described the car, he would always say "with California emissions." And I never knew what that meant. So later I figured out what that meant was California has some of the strongest or onerous, depending on your perspective, emissions standards in the country. And if this vehicle has California emissions standards met, then, you know you can drive it anywhere. So I feel like we're coming into a new era of California "emissions," except it's in the privacy realm. So with that as an odd backdrop, we have recently [seen] amendments to the California Consumer Privacy Act in the form of the California Privacy Rights Act. There's been a lot of talk about these changes, Michelle. What do you make of them? Can you give us an overview and tell us whether and the extent to which they actually apply to us?

[Michelle]: Okay. I love your emissions analysis. I think it absolutely applies. California is a state that's very... it tends to be very consumer friendly and progressive in the way it approaches legal issues. And that is what has happened with its privacy law. California was the first state—we now have seven states, but California was the first of those to pass legislation that really focuses on privacy rights, the rights of individuals to protect their personal data. There are some cybersecurity components of the law, but it's really focused on letting consumers interact with businesses around how businesses use their personal data. So that went into effect. Hmm. Gosh, that must have been 2020? It went into effect and had a number of provisions about providing notice to consumers. So you have on your website how you as a business will use that information, allowing consumers to ask questions about how it will be used and to have some limitation around those uses. So it created a number of new administrative obligations for businesses. The rest of the country watched in awe, and I think, you know, sort of states have started to think about who we need to be following suit. But before many states even had a chance to follow suit, California felt it hadn't gone far enough. So the original act, as we call it, the CCPA, the California Consumer Privacy Act, then the legislators worked up a bunch of amendments to make it even stronger, and some would say more onerous for businesses. Those were the that's the California Privacy Rights Act that you referenced. We call that the CPRA. It's really just amending the CCPA. So just to keep it simple. We're still dealing with the CCPA, but when people refer to the CPRA, they're referring to the new requirements that actually went into effect as of January 2023. There were quite a few additional things which we can talk

about. One thing I want to point out to begin with is: although the law went into effect in the beginning of the year, you have until July before the enforcement will begin under that act.

[Kevin]: So a bit of a grace period.

[Michelle]: A bit of a grace period, which I think is needed because they introduced a number of concepts. They also introduced a new agency that's overseeing the enforcement. It's the California Privacy Protection Agency, just to keep, you know, the alphabet soup confusion moving forward.

[Kevin]: Right.

[Michelle]: I'd say some of the biggest changes is that the act has a new category of personal information. It's called "sensitive personal information." And it mimics a little bit what happened in Europe here, Europe has its own special category of data. The only difference is in California, they wanted to go big, go big or go home. And so what "sensitive personal information" is I think is much broader. And I I'm actually looking at a definition because it's so broad, but it includes "social security numbers, state ID cards, precise geo location, racial or ethnic origin, biometric information," and the list goes on. It also can include emails that you have, but not emails if you're the business communicating with the individual, but emails that you have in your sort of personal account that somebody might get access to. But so it creates this new category and it gives consumers the right to control that data more vigorously than others. You can, you know, you have to provide—in certain circumstances—the right to opt out of the use of your sensitive personal information. So that is one of the bigger ones. Yeah.

[Kevin]: Go ahead, Michelle.

[Michelle]: There are the other two ones that I wanted to mention. Are you also before there were, you know, there was talk under the CCPA that this would include business-to-business communications and personal information that might be exchanged in that context, but it never went into effect. They kept postponing its implementation. It is now in effect. So as of January 2023, personal data that gets exchanged in the business-to-business context is also covered by this law, and that is something that folks weren't accustomed to thinking about. Employee information is also covered, but that was covered before.

[Kevin]: Right? And a couple of the new features I wanted to ask you about as well, Michelle, there are two that weren't covered in the original CCPA, one is the right to correct information and the other is the right to direct a business to limit the use and disclosure of that sensitive PII category. So those are those fall under the category of what you just described. We're not just tweaking at the edges. We're making some substantive changes to the act.

[Michelle]: No. And so it's created administrative obstacles for businesses. The right to correct just means you have to offer that right to the consumers, not only your customers, but people interacting with your website, which that creates additional nuances so that you just need to include in your privacy policy, which needs to be available at the point that you collect any personal information from a consumer. So if it's your customer, if you have, you know—in our field because we're lawyers, we have engagement letters, so you need to make sure you've pointed them to those rights at that point when you start communicating with them about an engagement. But when it's a website, you need to have that privacy policy available on the landing page of your website so that they can read that their rights, which include this right to correct to ask a business, hello, show me what information you have and by the way, you've incorrectly characterized this piece of my personal information. But the sensitive personal information that's a little trickier. That really requires what you're seeing now on a lot of websites is banners when you reach the website page explaining California rights and they'll explain that you have the right to opt out of the use of your sensitive personal information.

[Kevin]: Right.

[Michelle]: And that's and we're dealing with it so far.

[Kevin]: And another way, at least as I read it, the act has expanded is it's moved beyond the mere ability of a consumer to control or limit the sale of consumer information. Now, as the act is revised, the consumer has the ability to control the sharing of information, even if it's not sold with other third parties. And that's an expansion as well.

[Michelle]: It is. But what happened was, under the CCPA, there was confusion about what they meant by the term "sale." So they had this concept that you could not sell, but then through some of their guidance material and then the regulations, it appeared to us, to the folks trying to follow what's going on, that their concept of "sale" was broader. To me, selling is giving data in exchange for money...and that does happen in a lot of marketing contexts, but they seem to be suggesting that selling was also when you're using some form of targeted advertising. So you have a marketing provider who takes in information about the device being used and follows the movements of a consumer across the Internet, realizes they like Stuart Weitzman shoes and sends them directly information about those items that they have evidence that the consumer likes. So there was that confusion is "sales" selling or not? And with the CPRA they cleared it up. Now when they say "share," now share is to me a different has a different meaning to clarify that share to them is targeted advertising and sale is exchanged for money. So that is one of the things that has changed. You do need to allow people to opt out of targeted advertising, which they're calling sharing.

[Kevin]: So the high points, as I see the act, if you had to summarize it, the act requires businesses to give notice to consumers as to what they have and how they're using it. And with that disclosure comes the consumer's right to limit use in a variety of ways.

[Michelle]: Right.

[Kevin]: So in order to know whether we have to comply, we have to know how far the tentacles of the CCPA reach. So tell us about that, Michelle. How do we know, as businesses, particularly those sitting outside California, whether the act applies in any way to us?

[Michelle]: Right. So there are some complicated thresholds which I can walk anyone through if they're interested. But it really comes down to... the reach of this act, you know, it goes beyond the borders of California. There's no question. For example, my law firm has decided that we have to comply with the act. There is both...unlike the other state laws, there's both a dollar threshold, I believe it's $250 million in gross revenue. And then so if you hit that threshold and then you meet one of their other criteria, which is, basically handling the personal information of more than I believe it's 100,000 consumers, which includes website traffic, right? Or if you sell information of a certain number of consumers or if you do business—and that's the one sort of the big catch-all. So what does it mean to do business in California? It's a very, very broad concept and it pretty much means if you have a customer in that state, you're doing business. And so you need to see if you hit the dollar threshold and then you have to comply. You're complying with respect to the California consumers that you work with, but it still requires putting in place this, you know, this rubric of administrative procedures so that you're compliant. And obviously, if you have employees in California, you also need to comply. But my clients are often surprised to learn they might need to because they say, well, I just have one or two people that we sometimes do business with, and that's not the end of the analysis.

[Kevin]: Right? So the lesson is, if you're a business with any ties to California, you want to talk to your legal team internally and consult outside privacy counsel to determine whether you are subject to the CCPA. Because if you're not, Michelle, as of now, I think limited, if any, private right of action on the part of consumers. But this new regulatory agency that the amendment's created is going to be empowered as of July to start going after businesses. And while there may be a grace period, as we've seen in other states,

by and large, we're starting to see regulators in New York, for example, and in other places, they're taking an aggressive approach. And while they may not want to make an example of businesses, they're going to need to show that they're enforcing the act. So at some point the regulator is going to get active and that could pose a problem for people that don't comply.

[Michelle]: Yeah, and in California in particular, they've already started at least the obligations that existed under the CCPA. They've already started enforcing those. There was a really huge settlement from the... it was the state AG's office at the time. But with Sephora it's gotten a lot of press and, you know, a lot of critical response. And I think the [CPRA], it will be no exception. I think they're gearing up, they're setting their priority list and they'll be they will be auditing and then following up with enforcement actions.

[Kevin]: So before we sat down today, you had raised this question. I want to put it to you now: Is the CCPA the bellwether for privacy law in the other 49 states and across the country? So bellwether obviously implies that it's not... it may not literally be applicable, but as we talked about just a few minutes ago, it could well be applicable. But even if it isn't, Michelle, is it a bellwether for the rest of the country? What should we be thinking about right now?

[Michelle]: Yeah, I think that it is. But of course, it depends on a whole host of factors. What we're seeing across the country is basically three tiers of legislative approaches. So California's taking the most consumer-friendly approach. So the most obligations and the most enforcement action, you know, we're already seeing the trend with California, and that makes sense when you think about the politics of that state. I believe there will be other states, especially the state that you and I are sitting in at the moment, New York, that will follow suit and perhaps even there's some indication it could be even more onerous. But you've got that tier of legislation and I think you can expect to see other states that follow suit. You do have two other tiers. That's the good news. And right now, Colorado, Connecticut, Virginia, and I believe Indiana are sort of sitting in the middle. They have legislation that is, you know, provides a number of consumer rights, but it's not quite as aggressive as California. And you see, when each of these acts pass, they're very similar, you know, phrases and terms and the acts are very similar. I think there will be a number of states that follow that middle of the line approach. You do also have a couple of states so far, Utah and Iowa, that have taken a more business-friendly approach and they leave out some of the most onerous obligations. So, you know, there's no prior consent required to collect personal information. There's no discussion of targeted advertising, and there's some other things that are much easier to comply with. And I think there will be states that take that approach, too. And I think it will largely turn on the politics of the state. So you can probably, knowing your state, sort of imagine where it's headed. But I do think we will see legislation across the country and California certainly, I think, set the high-water mark. And some of those concepts will show up in all of this legislation.

[Kevin]: But yeah, so if you're sitting here, I'm sitting here thinking if I'm an organization of any size and I'm listening to you, Michelle, talk about the, you know, upwards of ten, maybe a dozen states, with more on the way I should be thinking, the more states there are enacting privacy laws, the more likely it is that I may have contact with a state, I may have a client, I may have customers, consumers in a state that has a privacy law in place. And if I do, I've got to be thinking about coming into compliance fairly quickly or else I'm risking regulatory investigation, I'm risking costs that I may be able to avoid if I take a more proactive approach.

[Michelle]: I think, you, unfortunately, if you're a multistate business, really need to sit down. I think sooner rather than later and look at what the reach of each of these statutes is. The good news is California's the only one that's as broad as it is. The rest of the states, for the most part, say you have to at least interact with about 100,000 consumers in the state, you know, through the collection of personal information or the sale. So it's going to be more in those states looking to see, do I really do business there, not do I have one customer? But if you do, like I said, just a few moments ago, the obligations vary from state to state, and you're going to have to decide what approach you're going to take. I mean, I think most people will end up adopting the most onerous of the obligations, just so you have a uniform approach, but you don't have to do

that. And you will, though, however, have to let the consumers in the various jurisdictions know what their particular rights are. So I think you're going to start seeing privacy policies that say, if you're from California, click here and lead you to a notice specific to those residents.

[Kevin]: No, I think that's right. And I think that's going to be potentially confusing to businesses who are trying to comply, and I think that's why it's so important. We touched on it earlier. You want to sit down with your in-house privacy team. You may well want to consult an outside privacy professional to make sure that you've covered all the bases and you have literally mapped your own in-house policies and procedures to the laws of the states for which you need to comply. So we've got a couple of minutes left. I want to take a little detour and ask you about biometric privacy laws. I've been involved with litigation recently. I don't know if you've seen it, but we know that it's... Illinois has BIPA, which is, I think, the leading biometric privacy law in the country, starting to hear and see some efforts on the part of other states to enact their own biometric privacy laws. Where do you see this going? And do you think that other states will necessarily be as aggressive in their approach as the state of Illinois?

[Michelle]: I think the same thing is going to happen that we're seeing in the privacy arena. And I think, Kevin, honestly, you're more versed in this than I am. But my experience is... I've heard, you know, a number of states that are looking at this, and they will adopt an approach that fits within their comfort level, that Illinois will be...it will be the high-water mark for these types of legislations. And the other states are going to follow suit, you know, but there will be tiered levels. I do think every state just, you know, this is just going to lag in terms of implementation and timing, just like privacy. I think we'll get all those privacy laws in place and then we'll be looking at the biometric data as the next sort of subset of ...it's personal data as well that you're going to have to deal with on a state-by-state basis. Because I don't, you know, I haven't seen anything compelling at the federal level to understand, you know, I do not believe and maybe, you know, that it's addressed in the ADPPA [Note: American Data Privacy and Protection Act]. I think we're going to have to wait and see, you know, where the federal legislators go in that arena as well.

[Kevin]: No, I agree. And I think it cuts both ways because on one hand, I'm not convinced that biometrics are as sensitive as someone's sexual orientation, personal...content of personal emails, union membership, and so forth. On the other hand, I think you're absolutely right. I think we are going to see an expansion of these biometric privacy laws. Illinois is the high-water mark. I think that the law in Illinois, BIPA, has had several unintended consequences if you're on the business side, if you're on the tort lawyers' side, I think those consequences were intended. And so I think we're going to see states grappling with the question, you know, should there be automatic damages, or should a party have to prove damages? Should there be a private right of action or should it be limited to government enforcement? And is there going to be an opportunity to cure? I mean, BIPA is an extraordinarily harsh law. And so we will hopefully see some states trying to make improvements on it, hopefully beginning with Illinois. But we haven't seen those efforts yet. So thank you for your take on that.

[Michelle]: Absolutely.

[Kevin]: I think that certainly I think we have to be very careful as organizations to keep our eye on the looming biometric privacy laws across the country.

[Michelle]: I think that's right. And I don't know if you've had this experience, but we have talked to legislators in the privacy arena who've asked for feedback. If, you know, there are folks out there with feedback, I think they're interested in hearing it, the legislators.

[Kevin]: Yeah, I think they are, too. I think they want to make the right decision and I think, you know, overstate. I think most people who look at what's going on in Illinois right now and the effects of that law are concerned that it's gone too far. I think the Illinois Supreme Court is concerned that it's gone too far, but in its

decisions upholding the act, it has been constrained to say this is the text of the statute. And if there are to be changes, the legislature needs to take the lead.

[Michelle]: Yep.

[Kevin]: Well, thank you.

[Michelle]: Yeah, it is interesting.

[Kevin]: And on that note, we will close for now. It's been so great talking to you again. Thank you for coming back and talking about the CCPA and what it means for the rest of us.

[Michelle]: Absolutely. Thank you, Kevin.

[Kevin]: Michelle Merola of Hodgson Russ, thank you so much for joining us. We hope to have you back on another episode sometime and we hope to have all of you back for another episode of Cyber Sip.

[Kevin]: The *Cyber Sip* podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share, and continue to listen.

Thanks for listening.