

Alastair Mactaggart's Privacy Perspective: Past, Present and Where We're Headed

After leading the charge to enact the California Consumer Privacy Act (CCPA) and changing the landscape of data privacy in the United States, **Alastair Mactaggart**, Board Chair and Founder of the privacy rights group Californians for Consumer Privacy, spearheaded the movement to pass the California Privacy Rights Act (CPRA).

Like the CCPA, the CPRA has monumental implications on how businesses operate in the United States, especially in the ad tech ecosystem, and builds on the unprecedented data rights and protections that the CCPA gave to California consumers.

The following is an excerpt from a Fireside Chat discussion between **Alastair Mactaggart (AM)** and Davis+Gilbert partner **Richard Eisert (RE)** on what to expect once CPRA comes into effect on January 1, 2023, and the issues that the CPRA is meant to address:

RE: **The CCPA just came into effect [at the beginning of 2020]. Why CPRA now?**

AM: I was surprised in 2019 when the industry mounted a full scale assault, from my perspective, on the CCPA, right after it had just passed in 2018. It struck me we were going to need something more robust in terms of defending the law from the inevitable attacks. It was a good opportunity to strengthen the law, and in terms of bringing it up to world class standards, make it more GDPR centric. That was the goal, and I think we've done that.

RE: **A number of changes in the CPRA appear to address the ad tech industry, and what is now defined as cross context behavioral advertising. What does the new distinction between sharing and selling in the CPRA say about the concept of sales under the CCPA, and what does that new distinction mean for cross context behavioral advertising going forward?**

AM: I think that the language in the CCPA is clear, and I think the intent is clear. I was really surprised to see a thread developing among some attorneys saying, "don't worry about 'sell,' because that means exchange for valuable consideration," and essentially, "we can 'share,' and it'll all be OK." Even though I don't think the CCPA is ambiguous,

if some people are saying it is ambiguous, let's make sure we close that out. It is now crystal-clear, when it comes to sharing consumer information for cross context behavioral advertising, that the law gives consumers the right to opt out.

RE: **The CPRA seems to effectively remove service provider status and the benefits of more limited responsibilities that service providers have for entities that are facilitating cross context behavioral advertising. Can you give us some background on the intent of that change?**

AM: I think it's all just an intent to try to reinforce and clarify that, under the CPRA, you are either a business, a service provider or contractor, or a third party. Service providers and contractors are basically very similar. In both cases, you're allowed to transfer information for a business purpose, but that purpose cannot be behavioral advertising for an opted out consumer.

The problem is that sometimes you want information to be sold or shared. Credit card fraud detection is a good example. In many cases, there *is* a sale taking place, because the fraud detection outfit is making money off the transaction, and so is the business by completing the sale to you. That's a good kind of sale. Then there's the kind where the consumer says, "No, I don't want to be tracked from site to site."

The CCPA included language saying that [for non-third parties] consumer information can't be disclosed outside of the direct business relationship between the business and the entity. That's now in the CPRA for service providers and contractors. We cleared it up.

RE: In your view, can businesses engage in cross-context behavioral advertising in a way that is both pro-privacy in accordance with the CPRA and will work in a going-forward basis, or do you think, essentially, that's going out the window?

AM: If you go to a music-sharing service and, all of a sudden, it's like 500 other companies you've never heard of are now going to share your information, and also use that as a portal to watch what you do on your phone as long as you have the other app open, most people say, "I don't like that." I think it really depends on the relationship of the business with the consumer. You can imagine lots of things in the future, because the law is pretty flexible. It allows any number of arrangements that are voluntary.

Also, in terms of behavioral advertising, remember that this law is not nearly as draconian as a law could be, in the sense that the first-party data the business has can be used in any way that the business wants with that consumer. If you have a relationship with the consumer, you should be able to use that.

RE: Intentional interactions are carved out of sales or sharing of personal information. Let's say there's a disclosure to the user that the business is providing the user's personal information to a third party. The user then clicks on a consent box, kind of GDPR-like. Would that be considered an intentional interaction that somehow exempts it from being sharing or a sale?

AM: At this point, I'm just a citizen. The regulations are going to come out for the new law [this year], and I hope that they will deal with your question. But I would just keep on coming back to the language [of the CPRA]— now it is pretty clear that cramming a consent down someone's throat is not "intentionally interacting."

RE: Why was the cure period for violations not included in the CPRA?

AM: If you look at the FTC model, which is notice and cure, it's been frustrating in some cases that you almost have to have a consent decree and then have that violated. Essentially, 30-day notice and cure is a "fix it" ticket. We went to a speeding ticket where if you are caught speeding, you're liable. I think it's a better enforcement model.

It's really important to also notice that [Cal. Civ. Code 1798.199.45], has language saying that the [California

Privacy Protection Agency] is empowered to look at the business's behavior. Was it intentional? Are they trying to fix it? Did they come forward and disclose it? I'd suggest one of the Agency's primary tasks has got to be education.

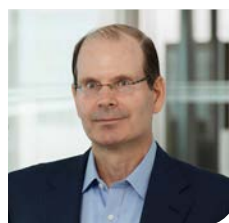
RE: Regarding the private cause of action in the CPRA, it doesn't seem very different from the CCPA — any insight as to whether there was an intention to do anything there or is it pretty much staying as it is?

AM: Look, I understand both sides. I understand the businesses who think this is just a "stick up" thing. I understand the advocates who think an under resourced agency won't be able to keep up. What I will say is that I'm not nearly as negative about the prospect for effective regulation [from the Agency].

The other thing, which I don't think gets a lot of attention, is that because exclusive enforcement is removed in this law — under the CCPA, it was exclusively reserved to the Attorney General — now the Agency can enforce it. The AG can also step in. Under the Unfair Competition Law, any district attorney or city attorney for the four biggest cities in California can also prosecute a violation. If a company thinks, "oh, we're just going to ignore the law," it's probably not a wise course of action.

RE: How do you think the Virginia law compares to the CPRA?

AM: It's not nearly as strong in terms of security, and it allows unfettered pseudonymous tracking. Sales are specifically designated as for monetary consideration, so you can share information, especially pseudonymous information. It's kind of business-as-usual for tracking.



Richard S. Eisert

Partner/Co-Chair
Advertising + Marketing
reisert@dgllaw.com

Richard's practice sits squarely at the crossroads of technology, advertising and marketing, e-commerce... [more](#)



Zachary N. Klein

Associate
zklein@dgllaw.com

For agencies, startups and global brands struggling with the evolving legal landscape surrounding... [more](#)