CARLTON FIELDS

CF on Cyber: Key Takeaways from the California AG's Proposed CCPA Regulations

CYBERSECURITY AND PRIVACY | TECHNOLOGY | OCTOBER 15, 2019


John E. Clabby


Joseph W. Swanson


Steven Blickensderfer

On October 11, 2019, the California AG published its long-awaited proposed regulations to implement the CCPA. This podcast describes a few key points from those draft regulations, including as they relate to online privacy notices, verifying consumer requests, and financial incentive offerings. The full text of the notice of proposed rulemaking, the regulations, and the initial statement of reasons is worth reading in full.

Transcript:

Jack Clabby: Welcome to CF on Cyber. Thanks everyone for joining us today. We're going to talk about highlights of the California attorney general's proposed CCPA regulations. We've got with us the usual suspects. We've got Joe Swanson from the Tampa office who leads the cyber security and privacy practice group. Joe, welcome. We also have Steve Blickensderfer from the Miami office who is all things privacy and breach response. So, thanks guys for joining us today.

Before we really get started on what is in these regs, Steve, maybe you could give us some background on what these things are.

Steve Blickensderfer: Sure. Thanks, Jack. So, the California Consumer Privacy Act passed in June of 2018, and it included a provision that authorized and required the attorney general to issue regulations. So, what we effectively have here as of October 11th, 2019 are the proposed regulations that the California attorney general is issuing with respect to the implementation of the CCPA. So, now when you're thinking, "What do I need? What does the CCPA require?" not only are you required to look at the CCPA language itself, but also these regulations.

And just a quick side note, the CCPA goes into effect on January 1st 2020 and the attorney general will not begin

enforcement until July of 2020. Regardless, it is important and the notice that accompanies the proposed regulations made clear that businesses are expected to at least start demonstrating or be in compliance by January 1st.

Jack Clabby: Alright. And Joe, what are the next steps here? We have these published regulations, but they're in draft form, essentially. What happens next?

Joe Swanson: Sure. Thanks, Jack. The next step is the attorney general's going to receive written comments from interested parties. Those are due by December 6th of this year. The attorney general's also going hold public hearings in four California cities over the span of three or four days in early December. And, you know, at some point after that the attorney general will take those comments in and publish final regulations.

Jack Clabby: Alright. Thanks, Joe, and thanks, Steve. Let's get to some of these highlights. So, we looked at these over the weekend. We got them I think late Thursday night. They were technically published on Friday the 11th. But, we looked at them, you know, in their entirety and there's going to be more that gets unpacked as we talk to our clients over the next few weeks about them. But, we're going to have some of our initial reactions here. One of the things that I noticed at the outset, right, was there's a real focus on how the notices and the information that are required by the CCPA shall be provided by a business to the customers in a manner that is "easily understood." Now, we all know how we should write with clarity. Privacy policies, opt-out notices should be written with clarity. But, there were two things I noted that I thought are going to be important that might seem like minor points, but for companies that are complying, I think they're important.

First, in, you know, consumer notices, right, the right to, the notice at collection, the notice of the right to opt-out, there's particular language in these regs that says these notices must be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sales announcements. Alright. What does that mean in practice? Well, for a lot of businesses that are doing multi-lingual business, for example if they have add circulars or websites in Spanish, they need to have their notices of the right to opt-out and similar notices in the Spanish language. So, again, now that is going to be clear in the regs, if they go into effect, that you need to have this multi-lingual approach.

The second is just a reminder that these notices must also be accessible to customers with disabilities. A number of our clients and customers who have significant web operations know about compliance with the Americans with Disabilities Act about website accessibility and there've been a lot of lawsuits in the past few years about website accessibility. So, the teams that are working on CCPA compliance should make sure that they're connected, again, simply with a team working on ADA compliance so that there's some understanding of accessibility here.

Steve, we've talked a lot with our clients about verifications. We got a lot of client questions about this. What's going on in these regs about verifications as to who is in fact making certain requests?

Steve Blickensderfer: Sure. So, real quick background on verifications, and the regulations make this very clear. So, the verification process is essentially requiring businesses that are responding to CCPA requests to verify that the person making the request is the person, that's the person whose personal information the business has so that when they respond and give the particular data sets or, you know, execute a deletion action, they are responding to the right person and it's not some fraudulent actor who's going and posing as someone else. That's the verification that we're talking about.

What these regulations make very clear and is what impressed upon me was to remind businesses that the verification obligation doesn't apply to the opt-out of selling personal information, and selling is very broadly used in the CCPA as the regulator makes note in the notice of proposed regulations. So, the verification is required for the request to know about the personal information the business collects, discloses, and sells and also applies to the right to the request to delete that personal information. It does not apply, as I said earlier, to the request to opt-out. So just to keep that in mind.

But, here are some top four things I took away from the verification discussion that is in the regulations. This is Article IV in particular, and the first one is, use what you have. If you're a business, you have personal information. Don't go out and start collecting additional personal information to verify that the user is who they're saying they are. If you have name, address, email address, and maybe another data set use a combination of that information to verify the personal information, to verify the person and don't go creating more personal information unless you have to.

Second, check against, and what these regulations are helpful for is that they do answer, well what, how do I verify? What does that mean? And so the regulations make clear that for a standard request to access or delete, you're looking for reasonable degree of certainty. And what does that mean? Well, as a baseline, it means checking against two pieces of personal information. That's your address, email, and then if you want to go above and beyond, something else beyond that.

The more sensitive the data - and this is the third point - the more sensitive the data, the more stringent the verification process has to be. And for that, the regs are requiring a reasonably high degree of certainty. And what does that mean? Well, helpfully we know that means three pieces of personal information. So, you can see there's a scale depending on how sensitive the data is, the more stringent the verification process will have to be.

And the fourth and final point that I wanted to make sure we make know is that if a business has a password protected account, which a lot of them do with the consumer, you can verify through that existing authentication process. So, businesses could and should look to see what's the process for verifying users already. Does that satisfy what the regulations are discussing with essentially checking against two pieces of information? That may be enough. You might not need to do anything new other than just making sure it works and it's integrated with this new verification process.

Jack Clabby: Alright. Well, thank you for that summary of sort of the highlights of Article IV. Joe, let's talk now about Article VI of these new regs, which is probably another bucket where we've had a lot of questions from our clients on financial incentives and what those mean.

Joe Swanson: Sure. Article VI is about nondiscrimination and one of the core tenants of the CCPA is that a business cannot treat a consumer differently because he or she is exercised a right afforded to them by the CCPA. It can, however, offer different service levels and other treatment for their consumers if that difference in price or service is reasonably related to the value of the consumer's data. And so, a good chunk of these proposed regulations addresses that issue. What does it mean to be reasonably related to the value of the consumer's data so that you're not discriminating if you are offering different service levels or prices.

And really, the key takeaway from this section is, your practice cannot be reactive or punitive. Think of it in sort of a traditional tort and, but-for test. That's really what these regulations illustrate.

And so in Article VI they provide a couple of examples that are worth looking at in terms of trying to understand what would be OK in the AG's estimation. You know, one example, fairly straightforward, is if a retail store offers discounted prices to consumers who sign up to be on their mailing list and that consumer can continue to receive discounted prices even after they've made a request to know or to delete their data, then the differing price level is not discriminatory. Those examples are worth looking at.

And in 999.337 there's also a list of all the different ways in which a business could calculate that difference in value of the data and I think, you know, stay out of the crosshairs of the attorney general. And there's eight examples of how you would go about calculating that value of the data. For example, it could be the marginal value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data. So, take a look at those examples. But, again, the key is make sure your practices are not punitive or reactive.

Jack Clabby: Thanks, Joe! And I think now that we've talked about verifications and we've talked about these financial incentive offerings we're going to hit a couple other things that kind of jumped out to us apart from those two dynamics where we've been getting a lot of questions.

One is section 999.326 which talks kind of simply about this concept of authorized agents, that is a consumer who authorizes someone else. Right? Maybe it's an attorney, maybe it's a business, or maybe it's one of these third party apps to go out there and submit request to know or request to delete on their behalf. We've seen this in the GDPR concept that the automation of this has caused a lot of questions and head scratching. There's some guidance, probably not as much as we would've have liked to have seen, about how to handle these automated requests. But what the reg does allow, right, is if a company gets an authorized agent's request, right, they can require, the business can require that the consumer (1) provide the authorized agent written permission, right, so they can essentially, I think, the reading of this is that the authorized agent would have to surrender or show to the company this written permission from the consumer to the authorized agent; and that the consumer would verify their own entity directly with the business. And so, yes, there is an authorized agent and the concept is allowed in the CCPA, but the company can still demand to interface with the consumer and verify their own identity. And my guess is this might get smoothed out more in the comment period because there is a real concern about these third party apps and services generating almost like an automated flood of requests. So, the AG gets it. There's been some guidance. I'd like to maybe see that guidance flushed out a little bit more.

Another one which, again, the theme we've talked about in a few of these podcasts is, you know, what has California co-opted or taken over or required on a website? This was a little surprising. So, in subsection 315 in discussion of request to

opt-out under (a), the regs appear to require, again, as we expected, two or more methods. But it specifies that it has to be a "interactive web form." Alright. What that means is a company can't just rely on, I guess, an email and the hotline. It's got to actually create on its website one of these interactive html web forms or some other form to take in the information to trigger the request to opt-out. So, you know, again, this is conscription of a company's web designers, additional costs in making the choice for the California or the CCPA facing business about what it has to do.

So, Steve, another sort of word we've seen a lot in these regs, or phrase, has been this idea of a two-step, this two-step concept. Can you help us understand what that is in these regs?

Steve Blickensderfer: Sure. And we see in several places in the regulations where the regulator, the attorney general is looking for a clear delineation between the consumer's request to elect a right versus the actual execution of it, and that's effectively what this two-step process is all about.

And so the first, we see this in one spot with the request to delete personal information. In the first step the consumer submits the request. The business then confirms receipt of it within ten days. And the second step is the consumer separately confirming the choice to delete. And I envision that this came from a motivation to make sure that consumers are not accidentally and permanently deleting their personal information where they didn't intend it. So, in order to prepare or to avoid that, to put on businesses the burden of creating essentially a divide between electing to execute the request and then actually carrying it out.

We see this similar two-step process for opting in to the sale of personal information. Now, this happens after a consumer has elected to opt-out of the sale of personal information. So when that happens, and there's an opt-in to consent to the sale of personal information, the first step is the consumer makes the request and then a separate confirmation of their choice.

And then we also see that again for the consent required for collecting and processing personal information of consumers under the age of 18 which happens by the parent or guardian in step one. That consumer's parent or guardian clearly opts-in, and then the second step there's a confirmation of it.

Jack Clabby: Thanks. And I think the two-step for consumers might be consumers under 13, I think.

Steve Blickensderfer: Yeah, no. That's the consumers under13 for the minors provision.

Jack Clabby: Alright. So one other question we've been getting a fair amount of is OK for companies that engage in direct marketing, when they've signed up a customer they sometimes will say, look, refer a friend. We can give you a benefit if you refer a friend or they just ask for it. Hey, do you know anybody else? If you like our product, is there someone else you want to recommend to receive our product? So, we've called that concept the refer a friend. We were kind of hoping there was going to be some guidance in here about that. I think like a magic eye picture, you can see what you want on these regs.

But, there does appear to be some guidance in section 305(d) which does talk about if a business does not collect directly from consumers, it doesn't need to provide this notice at collection. It's almost logical, right? If I'm not collecting from a consumer, I don't need to give them any notice. I might acquire it from some third party source or I might buy a list of some sort. And there's other things that will trigger, but I don't need to do the notice at the point of collection. If that happens, right, I can hold that data that is of a California consumer but not someone who I have collected from.

But, before I can sell it, rather before the company can sell it, they need to do something. Right? There are two options: one is they can go back to the source, you know, the person who sold them or provided them or referred them that consumer's data and confirm with that person that the consumer whose data you're ultimately holding has received the correct notices. Or, alternatively, you know, because you're holding a consumer's data, you can go directly to them and before you sell it, again with that broad definition of sale, you provide them with the notice of the right to opt-out. So what this would seem to do is let companies use a refer a friend program to collect information on consumers, but then before they actually go ahead and sell, and again with that broad meaning, they should reach back out to those new consumers, or reach out for the first instance and give them the right to opt-out.

Alright. Joe, we've had a lot of questions about security measures, right, because the CCPA does require in some instances the transmittal of data on a consumer to that consumer. Is there any help in these regs about that concept?

Joe Swanson: Well, I don't know if I would call it help, but there's certainly some discussion about it in these regulations. And this aspect of the draft regulations is particularly challenging. So, we're talking here about how a business responds to a request from a consumer to know what data that business has on the consumer. And in the draft regulation, we're talking

here about section 313. It requires reasonable security measures. So, as business shall use reasonable security measures when transmitting personal information to the consumer. That phrase is not defined. That's a phrase that our listeners will be familiar with in that other aspects of the CCPA talk about reasonable security measures. There's a private right of action for a data breach caused by an absence of reasonable security measures. Does the use of reasonable security measures here mean the same thing as it does over there? If so, it's not defined in that other provision under the CCPA. So I think we need to keep our eye on this and, you know, practically speaking, think about, you know, how will this work if the consumer requests the information be returned by mail as the CCPA appears to authorize.

Staying in that same section, there is also language that says a business in responding to a request to know shall not at any time disclose a consumer's social security number, driver's license number, or a handful of other highly sensitive personal information. Well, you know, it's not clear from these draft regulations. Does that mean the business cannot disclose the information to the consumer him or herself, or does it mean to a third party? It's not clear how far that prohibition extends. And I imagine that there will be a fair amount of comment on this in the next six to eight weeks. You know, perhaps you can transmit it so long as it's redacted. We'll have to see what emerges in the back and forth now before these are finalized.

Jack Clabby: Alright. So, I think, Steve and Joe, those are the highlights of what we saw in actually reading the regs. Right? And, again, that comes from our conversations with folks who are struggling or are planning to comply with the CCPA as the sort of hot topics that we're on the lookout for.

Steve, I mean, this notice of proposed rulemaking, though, contains a lot of other nuggets about what's going to happen in California. Can you help us understand what the highlights of those are?

Steve Blickensderfer: Sure. So, with the notice of proposed rulemaking we have this analysis and assessment and basically the impact that the CCPA has on the state of California, including the AG's own office. And the notice gives us some basically a peek behind the curtain so to speak and tells us that the AG's office will be hiring 23 new full time positions and expert consultants to assist the office with implementing and enforcing the CCPA. Whether that will be enough in addition to the staff that they already have, you know, time will tell. But, already the AG is ramping up and preparing for, you know, having a larger staff to assist it with implementing and enforcing the CCPA. And I know that there have been actions. In particular, a recent new filing or new proposed legislation in California to create, like, a separate privacy enforcer that's more specific than just the AG's office. So, we'll see what happens in the future, but it's already resulting in increased staff at the AG's office.

In addition, these assessments, they tell us, and this is what justifies the AG's actions, that's why it's in the notice. It says that the AG's office estimates the cost of compliance of the CCPA over the next ten years will be $0.5 billion to $16.5 billion over the next ten years. That's an incredibly broad range, almost to the point where it's, like, hard to guess or it is a guess. It's speculation as to what the impact will be. And I don't know if that even includes the cost of class actions and litigation related to data breaches or just generally regarding rights conferred and created under the CCPA.

And another interesting stat: the AG's office and the report on which it relies - it says that the estimated cost of small businesses to implement the CCPA is $25,000 and then $1,500 annually to maintain. I am not sure if that's accurate for small businesses or not, it seems a little low. The estimate for larger businesses is $75,000 to implement and $2,500 annually to maintain. Again, those numbers seem a little low. But, who knows if this process will be automated in the near future. You know, privacy tech is fast becoming a thing. So, you know, we'll have to see if those estimates pan out to be true.

Jack Clabby: Thanks so much, Steve.

Joe Swanson: Thanks so much, Steve and Jack. And just wrapping it up here, we encourage our listeners to check out these regulations, the notice of proposed rulemaking and the initial statement of reasons, all of which are available on the attorney general's website. Thanks, everyone.