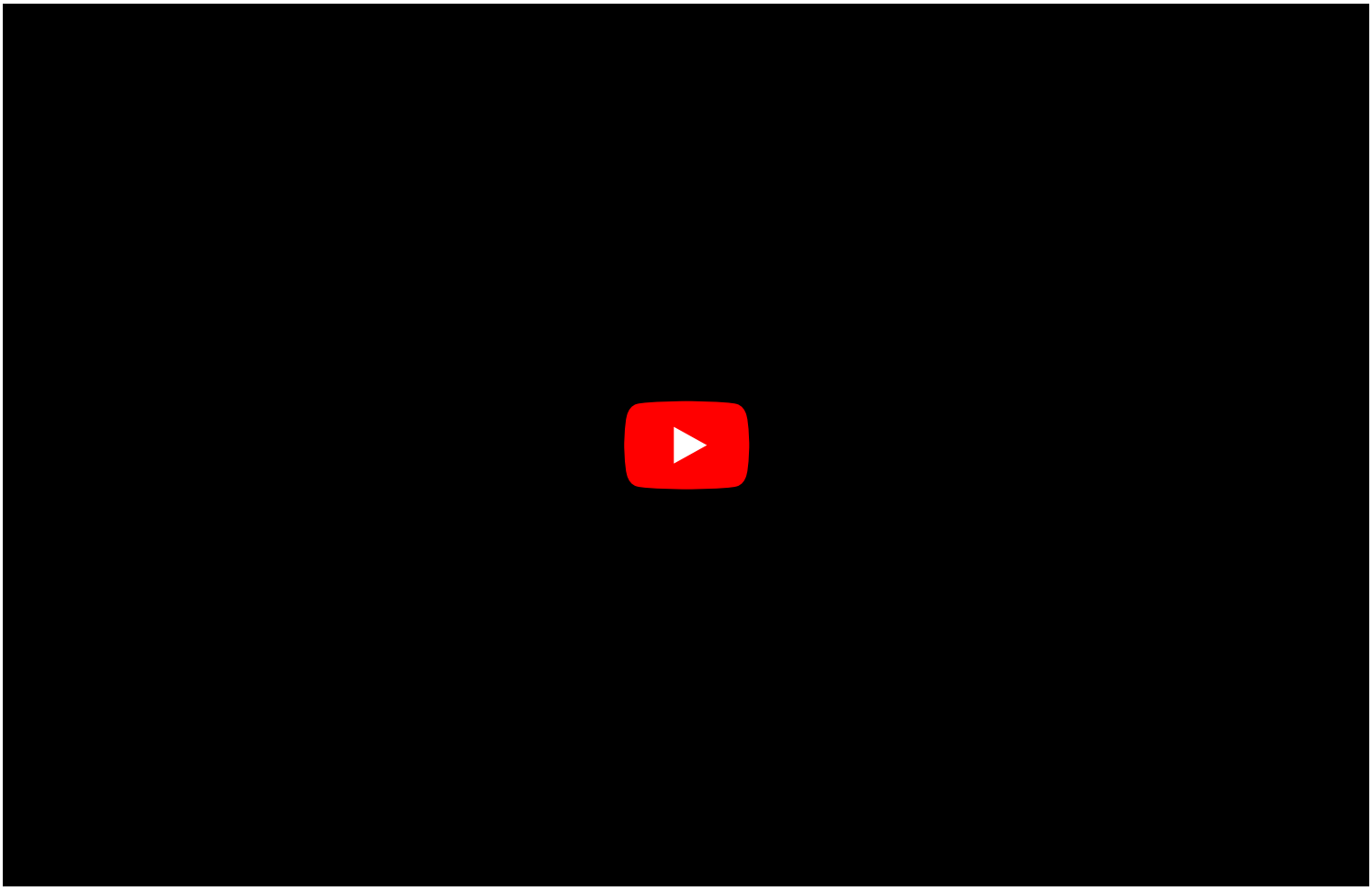
CARLTON FIELDS

# The CCPA for the Land Title Industry: Practical Compliance With CCPA and New Privacy Laws

February 06, 2020



With the introduction of the CCPA in January 2020, many other U.S. states have also begun to consider their own proposed data privacy legislation. In this podcast, Elizabeth Reilly from Fidelity

National Financial joins Carlton Fields' attorneys Jack Clabby, Joe Swanson, and Steve Blickensderfer as they answer real questions from real members of the American Land Title Association on compliance in the current data privacy framework and the future of privacy legislation. Part 1: Who Does the CCPA Apply To?
Part 2: Service Providers and Sale of Data Under CCPA
Part 3: CCPA Resources and Compliance Tips
Part 4: Practical Compliance With CCPA and New Privacy Laws Originally published in American Land Title Association's Data Privacy CCPA Resources.

# Transcript:

**Jack Clabby:** Welcome. This is Jack Clabby from Carlton Fields and we are back with the fourth part and the final part of our series for the American Land Title Association about the California Consumer Privacy Act. We're gearing this towards the Land Title Industry and we want to thank ALTA for the opportunity to get this group of sort of CCPA, lawyers and thinkers together to answer real questions from real ALTA members. As is usual we have with us Liz Riley who is a compliance and regulatory council with Fidelity National Financial in Jacksonville, Florida. We've got Joe Swanson here with me in Tampa, Florida, he's the practice group leader for Cyber and Privacy at Carlton Fields. We've got Steve Blickensderfer who is an attorney with Carlton Fields out of our Miami office and he's in Miami recording. He is a CCP, CIPP rather, and a privacy attorney. And you've got me, Jack Clabby, a former federal cyber prosecutor and a cyber-security and privacy attorney out of the Tampa office of Carlton Fields. So our usual disclaimer: this not legal advice we're offering this podcast for education purposes only. We don't have attorney-client privileges with our listeners and it's a lot of nuance that we might be missing even with these written questions we got from ALTA members. Liz is also here on her own and does not speak on behalf of her employer, her client Fidelity. Alright, so we've got some great mailbag questions for this one looking forward to getting into it just a quick review. In the first part of the podcast series we gave an overview of the CCPA. We talked about what is a covered business under the statue, we talked about whether it might apply to you depending on how you touch California and what role you play in Land Title and residential real estate transactions. In the second part we talked about some really important definitions under the CCPA. What is a service provider, what is a third party and importantly what is a sale under the CCPA? Which has a definition that is little bit different from how we might normally think of that term. In part three of the four part series we went over some resources that are available to you to help you to determine if you need to comply with the CCPA and if so what you should do. We also listed and kind of talked about internal and external tools and resources as well as some tips for practical compliance depending on where you fall as a covered business, a third party, or a service provider. In this the fourth and last part of the podcast series really going to do a little bit more and additional practical compliance with the CCPA and then we're going to talk about what other states might be doing. Whether you are or are not covered by the CCPA there are 49 other states that are thinking through how they are going to approach privacy for their consumers. And it's creating this kind of expectation of a, of a patchwork of what might be potentially different privacy rules that we'll

see over the next year to five years. And lastly we'll do some speculating on the future of privacy legislation in those states including at the Federal level. So we're really excited to wrap up the podcast series with some practical advice and some predictions. Let's get into it. Alright question sixteen asks about data mapping. How detailed does the data mapping need to be, high level or just enough to know what it is, where it is, how it's handled and stored? Alright so, how detailed does the data mapping need to be, high level or just enough to know what it is? Where it is? How it's handled and stored? Alright, so we can give some tips on, on data mapping. We've seen a fair number or these and again the, the people who do the data mapping its smaller organizations, it's typically an in house team, a combination of business folks and IT professionals on the back end. Because it's both looking at inputs and outputs of, of information but then also tracking how they move through the systems. If you can afford it and you are one of these companies that is going to have a lot do with the CCPA because you touch California and have a high volume. Hire an outside vendor preferably through counsel to help you with this because this data mapping is significant and these outside vendors have templates that can make it a lot easier. And make it more defensible if you ever are called to account for what you did to track your data there are some smaller companies that can help with this that we've worked with and they can do it on a flat or a fixed fee. If you're not in a position to hire one of the larger vendors who've been doing these even the smaller vendors have pretty good templates now where they can walk you through a good exercise to track your data. And again by, by sort of outsourcing it you help insulate yourself from accusations that you are not sufficiently detailed in your data mapping. You know the purpose of it is as the questioner wrote, you know, to see, you know, what you have but it's also to see if you were to get a request to delete, if you were to get a request to know the categories of information that are held or if you, got a data portability request could you in fact comply with it? Could you go through your own systems and track based on a household or based on an individual's request, what data you have? And then, could you deliver it in a form that's usable to the consumer? Could you evaluate whether there are exceptions to the exercise of their right to delete for example? Right so it's, it was two things, it's not just what the questioner sort of asked it's, it's not just finding out where it is and where it came from, but also, you know, as a practical matter could you do the things you're saying that you're going to do in your privacy notice when someone starts asking you to do those things. The data mapping as a practical effect apart from compliance it also helps you figure out if you're holding a bunch of data that you don't need to be hold. That you don't need to hold that is. Why are you holding data in a way that's accessible to even employees, if you don't need to be holding it? Why are you holding multiple copies of data, when only one would be sufficient? Should you be encrypting the data that you're holding, as opposed to keeping it in unencrypted form, even within your systems? But again, the overall goal here is to see what you have and to determine whether and in what way you would respond to a consumer exercising her rights under the statue. The more you are in California, and the more money you produce from California, the more detailed your mapping should be. The outcome of this thing, you know, at the low end, and the quicker the engagement is sometimes is just a conversation with the person doing the data mapping. But, as you can move higher up the time spend chain, it really, when they're done well, they're very useful documents. They're privilege

documents if they're done well, shows the data flows, shows the responsible departments and the third parties and it can be used by other parts of the organization as needed, to design sort of the response systems to CCPA Right Exercise request. And, it can also be used by your security personnel to determine ways to decrease the potential attach surface for bad guys, who are looking to do harm and get data from your companies.

1. The seventeenth, question seventeen in our mailbag: How do I return data to my customers if they're asking for it? How do I return data to my customers if they're asking for it? Steve what do you think here?

**Steve Blickensderfer:** So, the propose regulations that just issued a few weeks ago help a lot with this. With respect to what's the process for responding to a right to know or a right to have access to the particular pieces of personal information. First and foremost, it's important to realize that, just as it is important the business is secure in its data handling practices. It's also important that when it gives the information back to the consumer, that it have reasonable security measures when transmitting the personal information to the customer. So, if the customer has a secured portal, through which they go online and they see their account. One option would be to develop a system through that online account process to deliver the information that should be delivered pursuant to the request to know back to the consumer to give the customers their data back. Another way, if an online account isn't feasible is to deliver it securely through perhaps a secure email transmission. Or, you know, this is where again we start to diverge in terms of we do not know enough yet. And, we're still waiting to see, but delivery through mail is an option. Delivery through, perhaps, on a thumb drive if it's offered in a secure way, again it's going to depend on the context, the type of data and how it's reasonably stored by the business. **Jack Clabby:** This is, you know, this is one side of the CCPA that I think has not been fully thought through, even after the regs. And, I think, you know, Steven, we talk about this a lot, but Liz we've talked about this too. It's, it's one where it's creating this mandate to deliver information to consumers but doesn't layout, puts all the burden in, and frankly, you know, potentially liability on the companies responding to it in good faith. You know, but if a customer says 'give me all the data you have on me,' and I print it out. And, let's say it's the equivalent of four phone books, you know, do I mail that to their house? Or FedEx that to their house? And, here we are now putting in the stream of commerce an entire, several phone books worth of personal information. You know, I think what we're going to see here is a consensus around the encrypted digital device probably being the best way to deliver it. That is for those consumers who don't have a secure account already set up with the company. You can't make them set up the secure account and that makes sense. Fair, you don't want them to have to have a longer relationship with you then it needs to be. But, you know, in the mind-run cases, they say I think for the most part we're going to be delivering this information through that customer secured account that already exist. And if they're a one off, it's probably going to be some form of encrypted digital media **Steve Blickensderfer:** And that's another reason you might want to use an outside vendor, because they might be able to help you with that process as well. **Jack Clabby:** And this would be something I think as the REGs develop, it would be good to see. There's been, you know, other parts of the CCPA that REGs that have been

the focus of the initial noticing comment. But, I think how it gets delivered is something that is a practical matter. You know, there's answers to it but it would be nice if the, you know, if the AG just said what you had to do. That way it's easier for companies to qualify what it is and they'd be less worried about sending it, you know, again, these phones books through the mail. It's never a good REG if it requires someone to print something out and put it in the mail. I'm just going to lay that out there. I don't think that's politically controversial. The, alright question eighteen: Does deleting data requested by my customer satisfy the CCPA or do I need to show proof or evidence of deletion? Alright so, does deleting data, you know, the customer, consumer sends you a data deletion request, you've asked them twice, because now you have to ask them. You get the initial piece, then you have to get them to confirm one more time. And you verified it accurately that it's them. Now, you've done it. You've gone ahead and you've deleted it, what's the next play? Alright, so the answer to that is you do have to report to them that you have deleted it but there's no requirement in the rule or in the statute of the proposed REGs that you have to show them the proof that you did it. OK, and proof that you did it is probably pretty challenging even to do. Particularly, for sophisticated computer systems, right? What companies who are covered must do is retain a record that showed "how the business responded to those said request." So, you got to have a record, and you got to hold it for 24 months. That shows how you responded to the consumer. Alright, that can be in a ticket or a log form, so it doesn't really need to be too sophisticated. You know, the guess here is like all regulatory paperwork, try to decide if the outset, how are you going to keep those records and then just do the same thing each time. Periodically check it against best, you know, best practices or reasonable commercial practices, and then change it and syndicate to your team and to everyone who is doing it as part of your training for them, how it's supposed to be done. Alright, so, you do need to, when you do delete the information, you do need to tell the consumer you have deleted it, and you need to save a record of what you've told them, but you don't need to somehow save a record of what you did. If you can do it, you probably should, but there's no requirement in the statue or in the proposed REGs about that. Alright, so now we're going to switch it over to, thanks Jack, thanks team for talking about California. I don't think I'm covered and I'm not a service provider for any entities there. What's going on in other states? Is CCPA going to become the standard of care for the rest of the country? Alright, so question nineteen tees this up: How many states currently, or are expected in the next year to require data mapping of personal information as part of privacy coverage? Alright, so it's hard to say exactly which of these bills pending requires data mapping but we can talk about what states have CCPA light or CCPA heavy bills that are pending or maybe likely to be passed. There are about a dozen states that are playing around with the idea of CCPA. Some more likely in the near term then others. Nevada (pronounced as Ne-Vay-Da), am I saying that right Steve? Nevada? **Steve Blickensderfer:** I think its Nevada (correctly pronounced as Ne-vah-da). **Jack Clabby:** Nevada, right. **Steve Blickensderfer:** [*laughs*] **Jack Clabby:** That's what, we say that state a lot but I always get it wrong the way I say it. So, Nevada. Nevada is probably the closest. I mean, they have a right to opt out of this sale that's existing right now as we sit here today. Nevada has a right to opt out of sale information. So, if you're there or if you touch that state, that's worth looking into. New York has a robust cyber security and privacy regime for companies that are regulated by the Insurance and

Financial Services Regulator in New York. OK? So, that's the New York DFS. And, that's been stood up for a little while now and it's a pretty robust regime. I wouldn't say it's an alternative to California's regime but it does focus more on accountability in corporate governance then it focuses on giving consumers particular rights. So, California is sort of maybe an alternative or a different way of proceeding and again it's specific to those entities that are regulated by the New York DFS. So, if you're a title insurance company and you are regulated or certified by the New York DFS, you're familiar with that regime and what it does. And, then there's, you know, and again there's probably 10-15 other states that have CCPA like bills that were either proposed, pending or somewhere along the bill becomes the law passage way. Washington has one. Texas has one. Massachusetts has an existing fairly robust cyber security law but there is a CCPA clone that I think is still pending there. Hawaii has a broad CCPA clone, without a juridical limit, but again that's pending. Maryland has one as well. North Dakota has been giving some thought to it, although, I don't know, you know, how much that's going to impact the listeners but, you know, it's hard to predict from the size of the state how much impact it'll have. Because we've seen before in insurance regulations when, you know, a state that doesn't have a lot of impact, you know, as a percentage of the countries work in that area can just come up with a great idea and it gets accepted in state houses across the country. So, it's possible that what's happening in North Dakota could be transported down. And sort of industry participants should still follow it. The biggest question we probably get on this is, is there going to be a federal law? That's either going to pram the CCPA or that is going to otherwise, give us some color on it. And I think most large industry players want it, but I don't see a sign that it's going to happen anytime soon. What do you think Steve? **Steve Blickensderfer:** Yeah, the rumor is that we're probably going to get a federal bill. Maybe sooner than expected. But one that will not preempt stricter privacy laws. So to the extent that CCPA is a tougher law and it is more privacy friendly then it will not preempt those types of laws...which is actually pretty common. With California privacy loss. They tend to set the standard. You'll find a federal equivalent later that most of the time doesn't preempt California standards. And, then California still maintains the standard. And, just another note on the state stuff. Florida we saw a, what you mainly find here, you'll find amendments to the breach notification statues that expand the meaning of personally identifiable information in a particular state. So, Florida has one of those type statutes, so maybe we'll see an expansion to that statute, or maybe we'll see something like California: a standalone privacy bill. That's another option. So these just take various - they look different. Right? They're different types of laws and how they're introduced, they all vary. The Nevada one you mentioned, that's actually an amendment to the Nevada online privacy law that only three states have including California. So it just depends on the state's particular privacy regime. But from a federal standpoint, I think we can expect one federal law but one that will not preempt state stricter privacy laws. **Jack Clabby:** Yup. So that for the folks listening, I don't know if that's the worst of both worlds or the best of both worlds. Right? I think the hope was that a federal privacy law would just resolve what the standard was for multi-state businesses. So, as we often conclude on topics like this, write your congressman. **Steve Blickensderfer:** All the time. **Jack Clabby:** Alright. Question number twenty: How many states require, by title or de facto, a responsible data privacy or security officer? Sometimes we call that a DPO

under sort of the other regimes that we talk about. You know, California doesn't really require this. I think by default for many organizations it's going to be the person who fields the general questions that have to, sort of, at the end of the California privacy notice it's essentially required that there be a way of getting in touch with the company, not to necessarily exercise your rights, because that can go in another part of the privacy notice, but a way of getting in touch with the company to ask questions about their privacy conduct and their privacy policies and procedures. I think it's going to be whoever the companies tend to list for that is going to be your accountable person. But, yeah. There's not a lot of general laws in each state that require it. If you are one of these companies that is regulated or licensed by the New York DFS, then yes, you know, you do need to have an accountable executive. That may be the model, at least from regulated industries, that has sort of worked. So the New York DFS requires a SISO or the equivalent of it. That could be the precursor, I think, for a DPO more readily. If you're GDPR covered already, if you're a big player and you're in Europe - right? - if you're GDPR covered, you know, you need a DPO. Right? You need somebody, at least in Europe, to kind of have that function. If you're covered by GLB, as many title companies are, Right? The Gramm-Leach-Bliley Acts, the privacy rule, and the safeguards rules, you know, requires the designation of an employee who coordinates the information security program. You know, there were some proposals that have been kicking around about changing that to I think an exact SISO title, but either way you've got a person who's in charge of your regime under GLB. It should probably be the same person for the CCPA just in terms of making it easier to do. But again, you know, all told, even if a state law doesn't particularly require it, it's a good idea to have one just from the perspective of information security, let alone sort of the privacy obligations and tracking them. Alright, so question twenty-one: What's the expected main focus of the new data privacy laws on the books and coming in the next year. Alright, so when the new laws that are out there, what are the focusing on? You know, again, I think we're seeing CCPA light, CCPA heavy, or CCPA clone models. But, they're really going to focus away from notice of breach events - we've really built that out - to some form of notice of use of the data plus rights being given to the consumer to access, delete, or take that data and port it somewhere else. So, again, we're moving from a regime that's defined by access to, by bad guys, of data and then notice to the consumers at that point to one that requires companies to think about privacy as a set of rights that are possessed by the consumers whose data they're touching. **Steve Blickensderfer:** I think we're going to see in terms of trends. Recall, California has long had an online privacy law. CalOPPA is what it's called for short. And we're used to seeing online privacy notices that explain the privacy notice of the particular website. Cookies and things like that. I think what we're going to see as the new CCPA does is expand the online privacy notice that we find on websites to encompass more than just the business's online data collection activities. It's going to include their offline data collection activities and their use activities. So, I think we're going to see more in terms of notice about what the business is doing and depending on how active the attorney general is in saying what is and what is not sufficient notice, you know, it may be pretty helpful notice about what a company is collecting about a consumer. **Jack Clabby:** Yeah, I wouldn't be surprised too if some model laws that came through, you know, took the approach that Massachusetts and Gramm-Leach has where essentially requiring a company to write down what it

does about its security practices. Right? So that's the WISP, the Written Information Security Plan. That's separate and apart, too, from privacy issues necessarily, but this idea that I'm going to take a piece of paper and I'm going to write down here's the data I have, here's how I protect it, and here's why I protect it that way, and here are the people who are sort of in charge of that data. I think that a WISP model, W-I-S-P, is something that we're going to see more of in what's coming next, particularly after the CCPA because the CCPA creates these rights. But, because it was sort of the legislative history of it happened rather suddenly, it focused on a lot of what customers would see when they interact with a business, but not too much on what a business can or should do to protect itself internally. So, I wouldn't be surprised if the next step even in California is something concrete like a WISP. **Steve Blickensderfer:** And we didn't really talk about this, although it was mentioned a little bit, private rights of action being caked into some of these laws. The proponents of the CCPA are actually have already introduced what's being colloquially termed the CCPA 2.0 which includes a private right of action for enforcing all parts of the CCPA. And so, and I failed to mention before, but the federal privacy legislation that is expected or at least has been recently passed around includes a private right of action for all or part of it. So, including provisions that allow for individuals to enforce the terms of these new laws is something that we can expect as well. **Jack Clabby:** Alright. Well, thanks, Steve. And that rounds it out. That was the mailbag. I think by answering those questions over the several parts of this discussion we were able to go from does the CCPA apply to me to if it doesn't apply to me directly as a business but I get personal information, what am I as a service provider or as a third party? And then we talked a little bit about what other states are doing and what the future of privacy and security regulation might look like in the US. We look forward to continuing the discussion among the panelists here and to future opportunities to talk to this audience. Thank you very much, everyone, for participating.

## Presented By

John E. Clabby

## Related Practices

Cybersecurity and Privacy
Technology

## Related Industries

Technology