CARLTON FIELDS

The CCPA for the Land Title Industry: CCPA Resources and Compliance Tips

January 29, 2020

Join Elizabeth Reilly from Fidelity National Financial and 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 available tools and practical tips for companies as they work to comply with the CCPA. 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 part three of our series with the American Land Title Association about the California Consumer Privacy Act for land title industry. Thank you to ALTA, for getting us all together here to record the podcast. We've got a great team here answering real questions from real ALTA members. We've got the usual crew with us. Liz Riley, compliance and regulatory counsel with Fidelity National Financial in Jacksonville, Florida. We've got Joe Swanson. He's the practice group leader for Cyber and Privacy at Carlton Fields with me here in Tampa, Florida. We've got Steve Blickensderfer, a CIPP and a privacy attorney with Carlton Fields out of the Miami, Florida office. And, finally me, Jack Clabby, a former federal cyber prosecutor and a cyber and privacy attorney at Carlton Fields in Tampa. And, our usual disclaimer: this podcast is for education purposes only. We do not have attorney-client privileges with our listeners and we are not providing legal advice here. We do try to give you some practical answers to things, but it really is important for you to do your own research on this, and hopefully use this podcast as a guide, as you plan for compliance. Liz Riley is here and she does work at Fidelity, but she's here on her own, speaking for herself and not on behalf of the company that she works for and represents. Alright, so we have some great mailbag questions for this one. You recall in the first part of the podcast series we gave an overview of the CCPA, talked about what is a "business," we talked about how it might apply, the CCPA might apply to you as a player in the title insurance or the title industry. In segment two, we got into the definition of service providers and contrasted those with covered businesses and third parties. We also talked about the definition of sale, which is a little broader than most people might think under the CCPA In this, which is part three of the podcast series, we're going to talk about resources that are available to you as an industry member of the land title industry. We're also going to look at some internal and external tools and resources that you might have at your company and within sort of your networking group. And finally, we're going to talk about some practical compliance tips for companies that are struggling with how to fit CCPA compliance into their overall governance, whether they might be a business, a service provider, or a third party. So, let's get right into it. Alright. Let's talk about resources. Question eleven I assure you is not a plant from any of the people who are participating here. Is there a resource page where I can get information and practical advice about the CCPA over the course of the coming year as it is implemented? Liz, are there any that you know of, maybe associated with ALTA? **Elizabeth Riley:** There are in fact, Jack. Yes, ALTA does have a great resource page, fairly new. I think we spun it up, you know, earlier in the fall. That it provides a lot of data privacy and specifically CCPA resources. It's the ALTA.org/business-tools/dataprivacy.cfm or you can just navigate from the ALTA home page by clicking on the Business Tools link. I would be remiss not to mention that several of the great resources on that page have been authored by the folks on this podcast and are worth checking out.

Jack Clabby: Thank you, Liz. Joe, well, you've got folks who, you know, this is an area where the title industry is different from the rest of the country. Right? There is this idea, the Gramm-Leach-Bliley exception under the privacy rule is sort of a game changer. You know, and it's just, there's no guidance whatsoever from California about what to do, but there are pretty good resources out there that can help you answer some of the threshold questions. Joe, what's another one that you do a lot of work on? **Joe Swanson:** The firm, Carlton Fields, has a CCPA toolkit. If you google Carlton Fields CCPA toolkit I think you'll come across it or you can get it on our website as well. And it's intended to help businesses answer some of the questions we've been talking about on this podcast, and in particular the threshold questions about whether or not the CCPA applies to a business. There are a series of questions that the toolkit or app will ask that are designed to get to the bottom of that issue. And then if it is applicable or looks to be applicable, it also asks a number of questions about the kinds of things you need to be thinking about to get compliant privacy notices, data sharing practices, that sort of thing. And it ends with a written report that that organization then has from their time spent with the app. **Jack Clabby:** Thanks, Joe. You know, another thing too is when January 1st hits there's going to be a lot, a lot - right? - hundreds if not thousands of new privacy policies that are going to hit there. And my guess is that about 30 days later you're going to see a lot of people's privacy policies be edited once all these things that had been worked on in secret finally get out there. For participants in residential home closings that touch California, another idea is when that happens, go look at the lender's web pages, the lenders that you work with on an ongoing basis. Go look at the real estate brokers' webpages who you work with on an ongoing basis and see what they're saying. See what they're doing, see what they're saying about the CCPA and see if it aligns with your expectations about what's going to happen in your own practice. Steve, you've got some other good resources I know that you check pretty regularly for CCPA. **Steve Blickensderfer:** Those are all great resources. I agree with you in checking other people's websites. I would also add the IAPP's website's a great resource: iapp.org. And also for the not-so-faint-at-heart, I would go to the California AG's website. Check out, you know, go straight to the source and see what they're saying about it. I suspect we're going to see some actual helpful, you know, interpretations on some things, or advice, maybe. Oag.ca.gov/privacy - that's the current website - oag.ca.gov/privacy. **Jack Clabby:** Alright. So we've got, let's recap it. We've got the ALTA's privacy resources page which is really going to be, has been updated and will continue to be updated. We've got the Carlton Fields CCPA toolkit which has the interactive sort of widget there. We've got your lender's privacy policies as of January 1st. We've got your real estate, agent, real estate brokers, and realtor websites who you work with on an ongoing basis to check out what they're saying and they're doing. We've got the IAPP's website. And then we've got the California AG's website and the disclosures that they're going to make and guidance they're going to make under the public disclosures rules and their sort of other obligations and helpful ways to get the message out to the industry. Alright. Twelfth question here, little bit different from resource page, or passive resource pages, but: What tools should I be leveraging in order to comply with the CCPA? So, what tools are there out that may be existing or that might be out there that folks can use to comply with the CCPA? Joe, what do you think? **Joe Swanson:** Yeah, organizations can think of this in kind of two buckets, both internal resources as well as external. I'll

start with the internal. First, and this is going to be driven, you know, largely by the size of the organization's sophistication, what kind of departments it has that may have a hand in helping with CCPA compliance. So, not all of these will be applicable to any given organization but certainly your IT group, your information security group, your website team, risk management to the extent that that's a standalone function, the general counsel's office, privacy officer if there is one in the organization or privacy office, and then the marketing because they're probably going to have a pretty good handle on some of these data flows that are going to be critical to the kinds of questions that we've been talking about. So that's internal. External, you know, if you're working with outside counsel they can be helpful in assessing whether the CCPA applies. If it does apply, they can help draft the notices that would go on your website and otherwise where there's collection of personal information. And also, outside counsel can hire, to the extent they're necessary, other third parties, you know, to help with forensic work, data mapping. That work would arguably be protected by the attorney-client privilege if outside counsel has retained them. And I mentioned those third parties. They can be instrumental in doing the data mapping that's critical to understanding where your data is and what you do with it, doing a gap assessment relative to the CCPA's requirements, providing a 1-800 number that can help to accept customer requests for information about the personal information that that organization holds on them, and outsourcing the verifications so that when after January 1st consumers start asking for deletion or asking for copies of their information these third party firms can help verify that the person making the request is in fact a California resident and the person they purport to be. **Jack Clabby:** Yeah. So that's the internal people, the external people. There's some technology and software that is available, I think, to help. You know, it hasn't really been tested much. Some of it really cut its teeth in connection with the GDPR's request for access and request for data portability, and it's not, you know, round peg square hole or apples and oranges. Right? It's a little bit closer than that. But, the software that did help stand up the GDPR is available for at least larger companies who are getting compliant with the CCPA. Some examples of those are authentication and verification software systems or third party resources that service software systems, automating responses to customer requests. Right? OneTrust is an example. No affiliation with the, but they're sort of the household name for this verification and automation service. There's a number of other sort of software and service companies and companies that do computer programming and software engineering that can help work on your backend systems if you're a larger organization or if you're based in California and you know you're going to have a lot of requests on this. I mean, we have, we've talked to a number of clients about one of the features of the CCPA which is the statutory damages. Right? So if there's data breach under the CCPA, a plaintiff could bring a case without having to show actual damages. There's a statutory damages and it's a couple of hundred dollars, it's a range of a couple hundred dollars. Folks have said, "Look, Jack. I get it. Right? There's going to be more lawsuits here, but I'm already being fined because each one of these things is going to cost me $500, $1,000 to respond to each time." So if you do the math with your organization and you anticipate getting 100, 1,000, 10,000 potential requests, as you climb up that request likelihood ladder, looking at these outside solutions for verification and for automating responses becomes more sound. Also, if you are buying data from anyone - right? - or if you are

selling data to people, talk to those counter-parties. They may have solutions because they have every incentive to keep those relationships in place, and they may have already done vetting on those that you can piggyback on. Lastly, you know, there's a few other people that you should probably talk to about preparing for the CCPA if you are a covered business and anticipate a large volume. Talk to your insurance broker. Talk to your company's insurance broker about the risks and what they're advising their customers and clients to do. And talk to your insurance carrier if you have a direct relationship with your carrier. Now, the insurance brokers and the carriers are probably concerned more in the first end about the consequences for the data breach itself. But they've also done quite a bit of thinking about compliance and then they have some discounts or low-cost resources that they can push you in. Again, before you go out and make huge investments if you haven't already done it - right? - if you're listening to this and you are a huge company facing the CCPA, you're probably already on top of this. If listening to this you think, "I have a bigger CCPA problem than I realized," again, you have a little bit of cushion with the enforcement delay. But, now is the time to start and, you know, talk to folks who you have good relationships with and trade data on before you go outside and start paying a lot for new resources. Alright, let's shift over to some other practical compliance tips because we got some questions on those, too. Question thirteen - we actually thought about skipping question thirteen because it was unlucky, but we just, you know, it's not a matter of luck with the CCPA. It's matter of being prepared, so we just kind of went for it. What are some practical preparatory steps for CCPA or other forthcoming similar state laws? So, what are some practical prep steps, Joe, to get people started? **Joe Swanson:** Sure. I think part of it is just a paradigm shift for a lot of organizations in the United States to shift from a notice and a focus on data breaches and preparation and responding to data breaches to actual rights associated with privacy. And those privacy oriented rights are not supplanting the data breach, because that's also part of the CCPA. There's a private right of action for data breaches, like you just said, Jack. But in addition to that there's also this new era of privacy rights that has existed outside the United States for a long time, you see Europe and the GDPR, but is coming to our shores and coming here in a big way. So, getting ready for it requires a lot more than just preparing for data breaches. So, some practical tips in getting ready: (1) we talked about this already but it's worth mentioning again and that is data mapping. You really can't prepare for the CCPA or what are likely to be a raft of other laws like it in 2020 without knowing where your data is, who you share it with, and what else you do with it. Then work on three CCPA documents: a California privacy notice, a notice a collection that informs Californians of the categories of data that you collect and the reasons for it, and also an employee notice. Again, the employee coverage under the CCPA is fairly limited for this first year, but there is still a notice that needs to go with it. Another document to have handy is the incident response guide. Most companies should have that already for dealing with breaches, but because that's also a component of the CCPA you're going to want to have an incident response guide which is the playbook the organization would use in the event of a cyber-security incident or breach. Review your vendor relationships, gather your contracts, prepare the addenda that contain the terms we've talked about on this podcast, and consider do you have an accountable person in your organization who has enough authority. That person needs both to be successful, authority and accountability.

And that could be, depending on the organization, a SISO, a privacy officer, a lawyer, or someone else. Just make sure that he or she is both accountable and has authority in order to be successful. **Jack Clabby:** Yeah, and, you know, when you're doing these tasks for the title industry, I mean, some practical tips that we've seen be successful, particularly if you're a smaller organization and you're going to be subject to the CCPA, you know, look at a typical closing. Look at a typical closing and look at each piece of California personal information that was collected during that closing or that was used at the closing and trace it back to where it came from. And if you can trace back, you know, it's a closed universe of documents that everyone listening to us is pretty familiar with. Check each document. Where did you get it from and what was the contract by which you acquired it? And if you didn't acquire it pursuant to a contract and you collected it directly, you may be a business and you want to look at what it was that you said or need to say at the point of collection. The second way of doing a data mapping is to look at each and every marketing piece that you send out if you're marketing directly to consumers. If you're marketing to a consumer, you need to know how did I get this person's name? How did I get their phone number? How did I get their address? How did I get their email address? If you can't answer those questions, you got to get to the bottom of it. Right? So, I think those are two ideas for data mapping is, taking a real property closing and look at each document and trace it back to its source. And then second - right? - look at each piece of marketing you've done in the last three months, four months and try to figure out how you figured it out. Lastly, you know, if you're covered by GLB, as many people listening are, the privacy rule, you know, look at your GLB documents because you may be doing a lot of this already. The rights to opt out are different there, but you may have already have a system in place that works fine for the right to opt out for GLB that you could piggyback for some of your CCPA work. Alright, let's look at our fourteenth question. Are there any proactive steps I should take as a third party service provider to meet CCPA obligations or duties passed on by the client? Alright. So this is someone who is a third party service provider already and, you know, what are the proactive steps that they should take? Steve? **Steve Blickensderfer:** Step 1, I would figure out if you are a third party or a service provider and how that differs from your capacity as a business. So, we already talked about the [*inaudible*] answer. If you're a business what you could do. I'll stress the importance of figuring out your capacity. Are you a service provider? Do you want to be? Are you a third party? Because there could be benefits to wanting to be a third party. But, most important, you know, if you figured it out and you want to be a service provider, which is really what I think this question is getting at, look at the contract that you have in place with your businesses that you're doing business with and that you're providing services for. See if it has the required language that you need under the CCPA, which isn't much but it's kind of like magic language we're going to see start being added to contracts. Next I would, repeat, doing the data mapping. As a service provider it's equally important to do data mapping as it is when you're a business because you want to know what information you have coming in. If you're handling that data as a service provider versus a business your obligations change. And it's also important to know what you're doing with data and where it's going. And, you know, also think about the other things that you have to think about as a service provider. Typically in these agreements for data processing we are seeing obligations and requirements for auditing, for

example. The person who's giving you data has a right to audit you and audit your systems. Have you thought about what that looks like, have you agreed to it in contracts, are you prepared to? Those are the things I'd be thinking about if I was a service provider. **Jack Clabby:** Thanks, Steve. Alright, question fifteen: I use platforms and systems that are provided by a third party. How do I make sure that my customer's data are safe and aren't being sold? Alright, so this is, again, this is sort of the flip side of the question we just answered. This is, you know, you are a business or you're a service provider and the service provider itself uses service providers. But, you're a business that interacts with service providers. What do you need to do to make sure that the data that's being held by the service providers is safe? Alright, well, it's the flip side of what Steve just talked about. Look at your contracts with those platforms and systems. You know, they may be terms of use if you're using a really big provider of those services rather than a negotiated bilateral contract. But there's still, it's something you can look at and it should have something in there that talks about data. Do you have the magic language that turns them into a service provider? But as a practical matter when you're thinking about their security, you know, have you retained or do you have auditing rights? That is, do they send you a report or an attestation on the security of their systems? Do they send you a report or an attestation on their compliance with data security or data privacy laws? What is the contract or your course of dealing say about their compliance with data privacy laws? You know, there is magic language for what is going to be a service provider, but the industry, until we sort of start seeing more and more of these after January 1st, there's not exactly a script. We know what it needs to get at and it's evolving, but you really need to talk about that restriction on the use of data. Steve, what else is going on here? **Steve Blickensderfer:** Well, if you're giving data and there's no further restrict on its use, that could be a problem for both parties involved because that creates an obligation on the business to provide notice about selling of data and also provides restrictions on the entity receiving the information because then they can no longer share it with other entities without that being a sale. So, a party receives data, is not a service provider, can't sell it unless they check with the person first with respect to how it was received, if they received the appropriate notice from the consumer and so on. So, just additional considerations to think about. **Jack Clabby:** There's a lot of overlap between the lawyers and the vendors who are advising on the CCPA and that subset of Americans who are really interested in novelty t-shirts. Right? So there's a pretty big overlap between those two groups. And, Steve, we've been seeing some t-shirts that say "I am not a - " what is it? "I am a service provider." That's it. **Steve Blickensderfer:** "All my vendors are service providers." **Jack Clabby:** Yeah, that's it. "All my vendors are service providers." You know, I think of, you know, if we talk to ten clients or ten companies that we work with, each of them starts out with a conversation, "Well, I don't sell any data, so that part's not going to apply to me and I don't need to worry about that." And then, you know, out of each of those ten conversations probably three of them end up being sellers when you get to the bottom of what it is. But, yeah. "All my vendors are service providers." Give some thought to that. Right? Because if you're relying on the service provider exception to a disclosure of what would otherwise be a sale and you don't have a Do Not Sell button and you don't list the right to opt out in your privacy notice, you know, you could be at

some risk. So there's different decisions that you have to make, how you categorize the folks to whom you transfer data is probably at the top of your list of what's most critical.

Presented By

John E. Clabby

Related Practices

Cybersecurity and Privacy
Technology

Related Industries

Technology