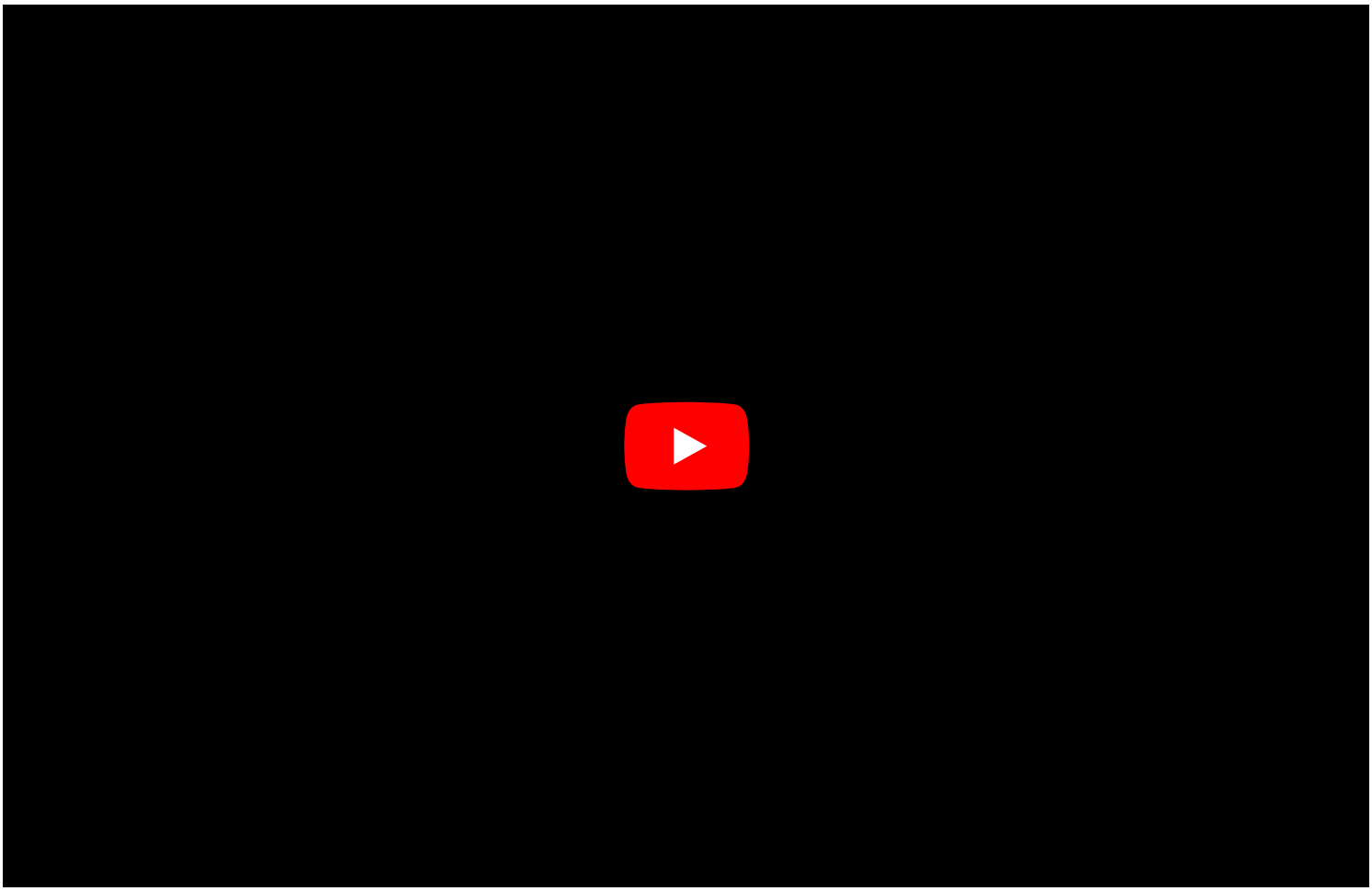
CARLTON FIELDS

CF on Cyber: Cybersecurity Due Diligence in M&A Deals Under the CCPA and GDPR

February 20, 2019



Sophisticated due diligence in corporate mergers and acquisitions has long included an assessment of the cybersecurity posture and privacy protocols of the target company. But the new California Consumer Privacy Act (CCPA) and the European Union's General Data Privacy Regulation (GDPR)

have raised the stakes for compliance, particularly for target companies that process or collect personal information or otherwise earn a living from consumer data. In this podcast, cybersecurity attorneys Jack Clabby and Joe Swanson and M&A attorney Jackie Swigler offer their top five inquiries for cyber due diligence in this enhanced landscape. The discussion is of use both to those looking to invest in or acquire companies subject to the CCPA or the GDPR and to such companies or owners who are preparing for a sale or strategic partner. After a helpful overview of the applicable regulations and their impact generally, the podcast turns to a discussion of the top five tips beginning at around the 7:00 minute mark.

Transcript:

Jack: Welcome to CF on Cyber. We have a topic today that came out of conversations with some of our clients and friends about what impact the new California privacy statute is going to have on investments that private equity and other entities might be making in businesses that process or collect consumer data, and we thought through some of our talking points for that and said, you know what, this would be a good podcast. We have Jackie Swigler here, who is an M&A and corporate transactions attorney in our Tampa office. She works with companies that are both up for sale and companies that are making investments or purchases so Jackie, thank you for joining us on the podcast today. And as always, we've got Joe Swanson who's the head of our national cybersecurity and data privacy practice and me, Jack Clabby, a shareholder here in the Tampa office of Carlton Fields. So let's get into it. Joe, we've been on a couple of these phone calls where our friends or our clients are asking us about not just compliance with the new California data protection statute but if they're looking at making an investment or acquiring a company that processes data, how it affects them. What's happening here in this cyber due diligence space?

Joe: Thanks, Jack. So the cyber due diligence space has really picked up and it's due in part, I think, to some mega breaches that have hit the news over the last couple of years and what that has meant for a couple of M&A deals – most notably, the Yahoo and Verizon merger that had a significant data breach occur in the midst of it and it resulted in a significant decrease in the price. And then more recently, the Marriott data breach, which as it turns out spanned the period of time during which they were conducting due diligence for the Starwood acquisition. So that's why there's a lot of attention in this space and it's not just on M&A deals. We have been called quite frequently in recent months to assist our partners, for example, in negotiating reps and warranties for a commercial lease or other types of transactional documents that the parties to those deals now want assurances that their cyber house is in order.

Jack: Alright, so one of the lawyers who calls us from time to time to help out is here. Jackie, can you tell us a little bit about, let's put aside the GDPR and the special problems from the California Consumer Privacy Act, what is usual in cyber due diligence?

Jackie: Right. So in cyber due diligence you would want to know what laws and regulations are applicable to the company that you're investigating. If you're buying a company then it would be the target company or if you are putting your company up for sale, ideally you are looking into these kinds of questions before you go through the process of putting up your company for sale. So you would want to know the laws and regulations that are applicable and how the company is doing in terms of complying with those laws and regulations. And in order to do that, you would want to look at, for example, policies that are in place whether they are privacy policies, terms of use for online operations or policies just internally for employees to be operating under. A lot of companies have vendor contracts that they outsource to third parties to help them with the compliance. So you would want to know what vendor contracts they have and if they're complying with their vendor contracts and how they're using third parties to help them with their compliance. You would want to know if there have been any incidents related to cyber and data security and data protection, large incidents but also small incidents where they're having troubles with people complying with their policies. Insurance coverage is an important part of this as well, whether the company has proper insurance coverage to cover for any sort of these breaches.

Jack: Joe, could you talk to us about why the GDPR and the CCPA have changed this a bit.

Joe: Sure. Jackie talked about looking at applicable laws and regulations, and increasingly for businesses that is the GDPR and will be the CCPA. The GDPR took effect in May of last year; the CCPA was passed last year and will take effect in January of this coming year. And each of them imposes significant obligations on organizations around the world. They have extra-territorial reach and for that reason a number of our clients are interested in how they apply and what their impact might be on these types of deals.

Jack: Alright. So these privacy issues that are raised by the GDPR and the California Consumer Privacy Act, the CCPA, am I getting that right?

Joe: You are.

Jack: Alright. They're particularly acute when the company that's being put up for sale or contemplating a merger or investment is a business that earns its revenue from the collection and the processing of personal data, right? So the average retail company has its own risks from consumer lawsuits, for example, but a company whose business is buying, selling, processing or earns revenue from the buying, selling or processing of that data, has special considerations and could essentially be wiped out if the wrong calls are made under compliance with these statutes. We have top five hits that we want to talk about today. So let's get through these top five suggested inquiries from parties to transactions or M&A deals that might involve these kinds of companies. Joe, could you walk us through the first of these inquiries.

Joe: Sure, the first inquiry would be just basically where does the data come from? And by that I mean, how much of a target company's business model relies on data that is collected from public sources versus data that is purchased from other data aggregators versus data that's collected from the consumers directly.

Jackie: And where the data comes from matters. That's one of the key establishing questions in your due diligence investigation. As a deal lawyer on either side of the transaction, knowing the answer to these questions helps me locate the right vendor contracts that I mentioned earlier, to see how the rest has shifted. It also helps me understand what specialized cyber advice I might need and to advise my client whether it should invest in that specialized cyber advice.

Jack: Right, and that's because the GDPR and the CCPA do a lot more than state data breach notification.

Joe: They do. They govern how organizations collect, store and use data and what those organizations promise and disclose to the individuals. These would be their use of data and their rights and that's what has made it such a paradigm shift.

Jack: So that's why you want to start these specialized inquiries with where is this data coming from? It might be treated differently, or the incident might be treated differently under the regulations depending on what originates that data. And it also flows through to the questions that are followed. The second inquiry is how is that data used for each individual? And critical here is this idea of profiles. Does the company set up profiles for individual people to track that person across time, across their spending habits or across other behavior, and then does the company segregate the data within that individual profile by where it came from? The answers to these questions, I think, can help the potential investor in the target company know, again, where the cascading risk arises.

Joe: Profiles are really a double-edged sword on the one hand. You know, the downside of them is that if a company keeps profiles, that may trigger a number of reporting and compliance obligations if GDPR and CCPA come into play. On the other hand, the good news is that if the company is keeping profiles it's more likely to be able to comply with a customer request to surrender, delete or transfer data, all of which at a high level are the rights that are conferred by the GDPR, the CCPA and surely in what will be other statutes like them and active in the coming months. So the bottom line is, if all of this information is one place and the company has a good handle on that, they have a higher regulatory risk profile but their ability to comply is going to be that much greater.

Jack: And there's a big difference between companies that track consumer data in individual files in individual folders essentially for those consumers, and those that simply are aggregators that separate that consumer data from identifying whose it is. So our first inquiry then is *where* does the data come from, our second is *how* is the data used for each individual and our third inquiry is, *what* is

in the privacy policies that the target entity has in place? And are the things that the entity says it's doing in the privacy policy in fact being done? Alright, so if a company is collecting data from the individuals directly, what does it tell those individuals and how does it inform them of what it's collecting, why it's collecting it and what their rights are with respect to that data? And can the potential investor, maybe the private equity firm or the larger company, can they get copies of those privacy policies? Are they readily available? And critical to this is getting the privacy policies that actually exist at the point of collection.

Jackie: Like any due diligence, the target company's willingness to share the information tells us as much, if not more, than the actual information itself. Willingness or ability. This is why when we're helping companies sell themselves, ideally we would spend a little bit of time helping them clean up their contracts in their books and records. We'll often suggest changes to the privacy policies and their procedures if data collection and processing is integral to the company value.

Joe: And I would add one other thing to this discussion and that is if collection of the data is done through a proxy-vendor or some third party, it's important to consider what review does the target company do for those point of collection disclosures and does the vendor, the third party, comply with those disclosures strictly, because liability here for the target company is not just what it promises to do about its consumers or its employees and information it collects about those individuals but also what these third parties are promising on their behalf with regard to collection, storage and processing of data that could ultimately cause problems for the target company.

Jack: A lot of the work that companies are doing now in the run-up to the California statute is cleaning up their privacy policies for exactly this purpose. And Jackie, you were saying, if a company is getting ready for a sale, it's a pretty easy thing for a company to do to rewrite the policy – the hard part is determining whether the company is actually doing the things it's promising in the policy.

Jackie: Yes.

Jack: And inquiry four is based around the new requirements of the statute we see in California that may be adopted in other states. Inquiry four is, can an individual actually see his or her data and can they delete it? So if a particular individual has requested to the company, "I want to see all my personal data that you have on me and if I don't like what you have, I want you to destroy it," can the company comply with this? And if so, how quickly and how completely can they comply? This at the heart of the GDPR's right to be forgotten which we've talked about on other podcasts, and also part of what's essential to the CCPA's structure, right? Can the company destroy all data on an individual on demand and if not, why not? That's the question that I would want to know if I was planning on making an investment. And if they can't do it, that's not fatal while we're in this run-up period, but how soon can the company get its compliance structures in place and what resources would it need from me and my investment firm in order to get there?

Jackie: Right, and that will certainly be one of the stumbling blocks to compliance with the GDPR and the CCPA – how can the target company comply with a consumer's request to see, delete and transfer all of the data on that individual.

Joe: So that brings us to the fifth of the inquiries that we wanted to cover today and that is, what is in the vendor contracts and are they being followed? Will the target company allow you to review all contracts or just a few example contracts that it has in place with its third parties from which it receives personal data, for which it holds personal data, or to which the company transfers personal data either for processing or storage?

Jack: And Joe, that's particularly true about those profiles that we were talking about a moment ago, right?

Joe: Yes.

Jack: Is the target company selling its profiles? It's making these profiles but does it actually profit from the fact that the data is segregated by individuals? If that's the case, then all sorts of risk arises and the due diligence needs to dig in a little bit more.

Joe: That's right.

Jackie: Right. And what we really want to know when we see these contracts is how they spread the risk of data security and compliance. What are the companies promising to each other as far as legal compliance is concerned? Separately, if the target company has made a number of commitments in these contracts, is it actually following them? Does it have the ability to track what its employees are doing? And are the employees following the commitments that are being made?

Joe: The bottom line here within this inquiry is that it's important to know how many vendors there are, where they are located, and do they do business in Europe or in particular United States jurisdictions such as California that would pose a heightened risk because of the CCPA. Frankly, California is probably not going to be the only statute, or the only state with a law like it, and so any target company should have its house in order so to speak with a view to these issues.

Jack: Alright, so in sum, there are these five inquiries that we use in connection with M&A due diligence as to cybersecurity and privacy that takes into account the GDPR and the new California statute. First, where does the personal data come from? Second, how is that personal data used by the company to support revenue, that is, how does the money get made by the use of this personal data? Third, what are the privacy policies and is the company following them? Fourth, can an individual see the data that the company has on her and successfully request its deletion? And fifth,

and finally, what is in these vendor contracts and are they being followed by the target company and its vendors?

Jackie: And remember, it's a cliché, but a hard compliance environment is an opportunity for competitive advantage. For a company that's preparing for sale and particularly one that believes it has significant growth ahead, compliance with these emerging privacy standards will be immediately apparent and it will stand out in the sale process.

Joe: Thanks for joining us and special thanks to Jack and Jackie. Thanks to everyone for listening and we hope you'll join us again soon.

Presented By

John E. Clabby

Related Practices

Cybersecurity and Privacy
Technology
Mergers and Acquisitions

Related Industries

Technology