Barclay Damon Live Presents *Cyber Sip*™
Season 3, Episode 8: "Compliance and Competition: Building Trust With Your Privacy Program" With Jodi Daniels

Host: **Kevin Szczepanski**, Barclay Damon

[Kevin Szczepanski]: Everyone, welcome back to *Cyber Sip*. It is a beautiful day here in Western New York. The sun is not out, but it's fairly bright. It's a *Simpsons* sky... and it is made even better by our guest. Jodi Daniels is the founder and CEO of Red Clover Advisors, a privacy consultancy firm. We're going to talk about what a "privacy consultancy" is later. She's a certified information privacy professional and has more than 25 years. Okay. If I mention more than 25 years?

[Jodi Daniels]: I know that makes me a little old now, just saying.

[Kevin]: I know. Well, I mean, what... I'm reading from your bio, so I can't get in trouble for it... a great deal of experience in not only privacy, but the related fields of marketing, strategy, and finance across a wide variety of sectors from startups to Fortune 500s. Currently, Jodi is an outsourced privacy officer for various companies. She advocates for privacy as a fundamental human right. Maybe we'll get to some of that later today. She is also a prominent national keynote speaker and cohost of the highly acclaimed She Said Privacy/He Said Security podcast, which she hosts with one of our guests, her and her husband, not necessarily in order of importance. I think the point with her husband, Justin Daniels, and most interesting to me, she is, with Justin, coauthor of the book *Data Reimagined: Building Trust One Byte at a Time*. Jodi, welcome. I'm so excited that you are with us here on Cyber Sip.

[Jodi]: Well, thank you for having me. And hello, and I am glad to be here.

[Kevin]: How many podcasts are you a guest on as opposed to a cohost?

[Jodi]: It's a really great question. It kind of goes in waves. So I have to be honest, I have absolutely no idea. I love talking. As a kid I talked nonstop and my family—I drove them crazy. Now it works out really well because I love to talk. I found a good topic to talk about.

[Kevin]: Yes, you have a great voice for it. And I was a bit of a weirdo as a kid. I loved to talk. I use one of my parent's snack trays and I don't know that anyone under the age of 40 knows what those are, but I put my cousins—We lived in the same house. I put my cousins' Donny and Marie microphone set and record player on the snack tray. And I played radio station for hours at a time. And it was a small house. I'm not sure people really liked it, but I liked it. So here I am. But you in our audience didn't need to hear that. So let's jump right in. I want to ask you first question. When did you get started in privacy and why? What was it that drew you to privacy?

[Jodi]: It's sort of in the second half of my career, and I was working at Cox Enterprises who actually had made an acquisition for an ad targeting company. It was an ad tech company at the time. And then one of the subsidiaries, AutoTrader.com, wanted to leverage that technology. So long story. I went over to AutoTrader, helped build this targeted network, and I essentially stalked you for cars. So you're welcome. And again, at the time, there was no regulation and there was no self-regulation either. Well, that's when self-regulation

started to come around. It was the IAB, the Interactive Advertising Bureau, who said, you know what? We need some self-regulation. Ironically, to prevent government legislation. And it kind of worked for about 10 years. And actually, let me correct myself. It is not only the IAB. It was seven different online advertising organizations and advertising organizations that got together to kind of form this industrywide self-regulation. And then IAB said to be a member, you have to comply. Well, were a member we wanted to comply. As a result, that was me figuring out what is this thing and what do I have to do with it. If anyone pays attention, there's a little blue triangle on the Internet. It's called ad choices. That's actually where that came from. Oh, that is my start into privacy. From there. Did that for a while. Was looking for something new. Convinced our company they needed someone full time in data privacy. And that was before there were really any laws like we have today. I mean, there were existing laws. The Federal Trade Commission has always been here with their "Unfair and Deceptive Privacy" principles and act. But I didn't we didn't have CCP. We didn't have all these other laws. Well, I convinced them that they should ask me to do that. And so that was my start into privacy. And then from there, I built the privacy program for three years at Cox Automotive. I left when we had about 23 different brands that I was responsible for from B2B and B2C that I ended up going to Bank of America, really mature, highly regulated industry, learned a tremendous amount in the financial services space and what a mature program in a regulated environment also looks like. Then I decided I was going to break away from corporate and start my own privacy consultancy, and I did that to help companies who are confused and complex and don't understand this whole privacy universe. And we help make it simple for them.

[Kevin]: So there was a time when the industry, quite rightly or at least astutely thought, if we self-regulate, we will be able to put off the onslaught of federal and state governmental regulation. That obviously was not successful long term, because today we have precisely that. So thinking about Red Clover Advisors, let's talk about it. You are now founder and CEO of this privacy consultancy. What is a privacy consultancy and why should people be thinking about coming to Red Clover or organizations like yours?

[Jodi]: We help companies comply with data privacy laws, and we help companies build trust with their customers. At the core, we're helping companies figure out which laws apply to them and what that means. There's a long list of laws and long list of requirements. We look at your business and match up which laws apply, and then if there is no law, what do you do? For example, I live in Georgia. I have no privacy rights at a statewide level. There's no Georgia privacy law then cares about me. Well, what do you do as a company with people like me? Do you include me? Do you exclude me? So what we're doing is we're helping companies with all the actual privacy operations that they have to do. Think about a privacy notice. People are used to those cookie banners that they see on the Internet. That's the outward facing pieces. Those are like a window dressing. We help companies get all that right and then we go inward. What's the company actually doing with the data? What is it collecting? How is it using it? Should it collect it? Should it not.

[Kevin]: Right.

[Jodi]: There's can and can't. And should and shouldn't. And we're helping companies with all of that at a really kind of basic fundamental level. And anyone who is processing data, personal information, needs to think about privacy. Depending on the size of your company, the kind of data you're processing and who your customers are—and where your customers are and the size of your company—might warrant the level of requirements that you have to address. And having a guide to help you along the way and make it as simple as possible and make sure you're doing what is applicable for you and not just copying what you see someone else doing is really important. And that is what we do at Red Clover.

[Kevin]: So let's say I'm one of those companies and I'm in the state of New York and I do business in New York, but I also do business in ten other states, some of which are among the dozen or so with state privacy laws, some of which are not. And I come to you and I say, so I'm putting you on the spot. Sorry about that. I come to you and I say, you know, Jodi, here's the thing. We do not have anything in place. I... a couple of years ago I went on Amazon or another big company's website. I downloaded their privacy policy. I kind of configured

it so that we had something. But beyond that, we don't have any written policies and procedures. Where do you start with a company like that? How do you start to work through a strategy for compliance across these multiple states?

[Jodi]: We call those a "privacy program assessment." And if you think about any other part of your business, there's likely been some type of assessment or strategy in that area. Same kind of activity. Our privacy program assessment is going to look at first your company, your customers, and which laws might apply. We might find one, two, three, 10, however many more. That's going to be our starting point. Then we're going to understand what you're actually doing, the kind of data you're processing, meaning collecting, using, storing, and sharing. That's processing. We're going to understand all of that and start applying and mapping it to the different requirements. Based on the requirement there's going to be you're doing a great job or you're not, and you get a big red gap from that. We're going to come up with here's what the recommendation is, and then we're going to prioritize, because as much as everyone wants to do the right thing, right away, you literally can't actually do them all, most likely all at the exact same time. So we're going to outline... we believe this is what's most important because of your business and the kind of data you have and what your needs and what your gap is and create what that plan and roadmap would look like. You have to start with understanding the technical requirements, and then you have to understand what your company is actually doing with the data. From there you can create a plan.

[Kevin]: And do you have does Red Clover have both of those capabilities? In other words, you have the technical capability, and you also have that policy and procedure, legal capability. So you're bringing that to bear all at once?

[Jodi]: We do. Now, as a consulting firm, we are not a law firm. And what I would say from a privacy point of view, many people are really accustomed to HR consulting and HR attorneys or employment attorneys. In my belief, the privacy space is very similar, and there's room for both. HR professionals need to know the HR laws. And then there's also a place for employment attorneys. Well in the privacy universe, that's us. We need to know the privacy laws. We do have some attorneys on our team, but they're not practicing in the spirit of a practicing attorney. We all understand the laws and what those requirements are and help create that plan. And then we actually can help you do the work. You might need a policy or a process or a training documenting the actual data you have flowing through the company. Doing a risk assessment on some high-risk process that you have, or based on the kind of data... we can do all of that. And then in doing them evaluate, this was a really high risk and privacy, like many other areas, has a lot of gray. So sometimes there's a gray area where legal counsel might be involved, and we work alongside and with them often in a variety of different ways. I encourage anyone listening kind of think about that relationship between that in the HR universe. It's really similar in the privacy space, and we can absolutely help with those tactics like you were just describing.

[Kevin]: I think that's a great point, Jodi. I think a lot of us... we're concerned about cost and efficiency, of course, but we just some of us may just not know how the process works. So I would encourage everyone to do exactly what you did. You may want a privacy consultancy. You also may need to bring a lawyer on to your team. You may need a forensic vendor on your team. You may need to coordinate with data security lawyers and with HR lawyers. So I think—is it? I should ask you, it's almost like building an internal team and a relationship between that internal team and your outside privacy consultancy to make sure you're covering all the bases.

[Jodi]: Absolutely. Teams... to accomplish anything you need a collection of resources and they don't always have to be internal, and you just want the experts that are appropriate for your organization. We don't cover contracts; we don't cover the cybersecurity and data breaches. And if you were to think about any type of data breach response, you're going to have a variety of different experts. A lot of those people aren't always internal. They might some of them might be. You might hire from the outside as needed. In the privacy

space it's going to be very similar. You're going to want to have the right people in the seat to help you with whatever obligation is identified for your privacy program.

[Kevin]: So thinking in terms of time, Jodi, let's say from the from the time I first talked to you about my business to the time when we're beginning implementation, either a privacy policy or a more robust plan, a set of policies and procedures. Is this something that an organization can bring to the fore in a week or two, or is it a longer process? I suppose it depends on what needs to be done, but I guess I want to give our guests a sense of how involved and how long of a process this is. It's not something we can do overnight...

[Jodi]: It is not, nor in a week. That would be really lovely. I mean, maybe if it's the smallest change ever possible and you can do that that quickly. Generally speaking, this is a multi-month to multi-year process depending on the size of the organization and the complexity of the data. I have seen some really large organizations have some really simple data, and it's not only about size of company, it's honestly about the complexity of the organization and the kind of data that they process. For some it might be simple and it's a few month activity. For others, it really can be a multi-year, phased approach, much like any security changes that someone might need to take. You typically... maybe there's a really easy fix overnight. Often it's a phased approach.

[Kevin]: Right? And on the security side, I can offer an example. We... we're involved with a client right now and we're putting together an incident response plan for a publicly traded financial institution and for a variety of reasons, we've had to fast track that. But that process from the kickoff date to creating a draft for consideration within the company is a 4-to-6-week process, and then we're going to retool it before we finalize it. So we're looking at a fast-track process that's going to take probably two to three months. So for anyone that's thinking, you know, can you just send me over a privacy policy that we can review, that's... you can do that. But if anything ever goes wrong and someone takes a look at that policy, you may not be able to answer every question as best you otherwise could.

[Jodi]: Absolutely. I completely agree.

[Kevin]: So... let me ask this question because clients will ask this question as well. I'm curious your thoughts. So if I have... I've come to you and I say, look, I made up a privacy policy based on the one I found on Amazon's website. I don't have any other written policies and procedures. Can you just give us an overview, Jodi? What is it going to look like at this business after the first phase or phases of the privacy program are implemented? What sort of written policies are we going to see in that company that we didn't see when the company first came to us?

[Jodi]: Well, we're going to want an external website privacy policy that matches what your business does and not a copy of somebody else's. Depending on the company, there could be more than one. For example, I spoke with a company this morning and they have a technology product, so they have one privacy policy for the tech product and a different privacy policy for the website. Then if you have any employees that are in jurisdictions that also have privacy obligations (hint, hint, California and in Europe and the U.K.), they need their own special privacy notice, too. Sometimes people have an applicant privacy notice if it's not already embedded in the website one. There's pros and cons to having it connected and separate. Then we need internal policies. We should have an internal privacy policy. And much like security policies, sometimes these are all wrapped in one or separate. It kind of just depends on your company right? These types of internal policies to cover the rules of how we're going to process internal data. They also should cover how often we're going to review our data. We call that a data inventory. Or how often we're going to look at privacy impact assessments, what our plan is for managing privacy rights requests, how we're going to do vendor reviews. So these are all the different parts of a privacy program, and you need a policy and how you will actually address those requirements in your company.

[Kevin]: So if I were to summarize, I would say it's not overnight, it's not one and done. And although it doesn't have to take forever, I think if you're an organization that is fairly young when it comes to thinking about and implementing privacy policies and procedures, it's probably going to take more work than you might expect. But at the end of the day, you are going to be... your data will be protected, your customers, your employees will be protected. And what happens if you don't do that, Jodi, have you ever had... can you share with us a story? You've had a client come to you after an incident, perhaps where they have been, they're part of an investigation by some regulatory authority. Can you just give us a sense of what happens if you don't take the kind of holistic, step by step approach to privacy that you and I are talking about now?

[Jodi]: Well, then you scramble. And what should take a thoughtful, timely approach is now having to be done in a really time-crunched environment. It might not be accurate, it might not be thorough. That's from a regulatory perspective. I would love to add that what I see a lot, especially in a B2B environment, is companies not being able to close a sale because they don't have the privacy program buttoned up the way their customers are expecting them to. And customers, especially larger customers, are very savvy and have very high expectations. And I am seeing much more pressure from those companies downward sort of in that vendor cycle. And now those companies have to really start building their privacy program and be able to show here's what here's what I'm doing, and answer those questionnaires that I'm sure everyone listening here loves, accurately.

[Kevin]: So let's jump to that. Let's suppose I'm a small company, I'm a vendor. I happen to work for large companies. I work for some large, publicly traded companies who may be subject to FCC requirements. Gramm-Leach-Bliley... A whole set of federal and state privacy laws and regulations. But I might come to you and say, well, Jodi, I'm just a small business. Why? ...I shouldn't have to worry about the same laws that Amazon or IBM or the bank on the corner has to worry about. Do I? I'm not a publicly traded company. So what's your response to some to a company like that?

[Jodi]: I get that one all the time. There's a few. The first is if you are operating globally, globally, they tend not to have thresholds and they don't care if you are private, nonprofit, public or have more than one customer. You just need one to have to be in scope for many of the global laws. In the United States, we tend to take a kind of softer approach and we put some floors and thresholds in for companies in all different fields. And as a small business owner I'm sometimes really grateful for that. However, in the privacy space, the companies don't necessarily take that approach. Many small companies want to work with the large companies and large companies don't say, you know, you're small, it's okay, you don't need to comply with any of my approved significant vendor processes. We'll make an exception. That doesn't happen. Which means all the small companies who want to work with the big companies have to comply because that is their process. I will also offer that depending on the size of your company, it's not always revenue driven. In fact, most of these laws are not revenue driven. Some are. California has the revenue threshold or the number of records being processed and many companies fall in because of the revenue. But you can also be a smaller company with just a lot of records because of the nature of your business and as a result might find yourself in scope because of the record threshold. Again, public... if you are a small private company trying to do business with the big public company, the big public company is not going to make an exception for you. And you have to play by those rules.

[Kevin]: Right. And thinking of it from their standpoint, if I'm a compliance officer at a publicly traded company, I have to comply with an array of federal, state, and sometimes international privacy laws. And I'm responsible if something goes wrong. So if my company is going to hire you, a small vendor who's not regulated, and you're not in compliance, if something goes wrong, I'm responsible for that. I'm responsible to the consumer, I'm responsible to my shareholders, responsible to my boss. So it's not that these... the big bad company wants to force you to comply. It's they have to comply either directly or indirectly through the vendors that they use.

[Jodi]: Absolutely. The example I always give to try and get people to understand this is imagine you go to a really small local health care provider and it's a one- or two-person shop. They... you expect when you walk in for them to take your privacy and HIPAA obligations equally to a larger physician, practice or hospital. You don't walk in and say, you know what, you're small. That's okay. You can do anything you want. Here's all my files and stuff and you don't need any protections. No one walks in and has that expectation.

[Kevin]: No.

[Jodi]: You have the same one regardless of the size. In the United States, we tend to put these thresholds here to help just from a compliance burden. But again, that doesn't mean that the end result is any less concern or focus or care and the actual privacy and security of that data.

[Kevin]: Right. You could be a small company, a relatively small vendor, but if you're handling millions of pieces of data, you pose an extraordinary risk that is in no way connected to the revenue that you generate from your work. So I think a lot of businesses think, well, we only do $2 million or $5 million in business. Why do we have to comply, and it's not necessarily tied to revenue can be tied to the quantum... the nature or quantity of data that you have as well.

[Jodi]: Exactly.

[Kevin]: So we're coming close. We've got a few minutes left and I want to ask you about your book. So here it is. I know Kyla is going to put it up. It is data reimagined building trust one bite at a time. Why... you're so busy. Why did you and Justin write this book?

[Jodi]: Well, we just thought we needed to add to our kind of crazy plan. Well, the real answer is we find ourselves talking all the time, just like we are here today. Why does it matter? Why should you comply? What are the obligations? Why is this good for me? And we wanted to find a way...Not everyone likes to listen to a podcast. Not everyone wants to attend different conferences or read 4,000 blogs that all add up to the same idea. So we codified it into a book for a business professional. It is very much a story-driven approach. It is not a super, detailed technical book. It is meant for the business professional to understand, just like what we were talking about today. We walk through all the different components of a privacy and security program and why it matters to the company. There are some rules, here are some of the basics of the rules. Here's why you should comply. Your customers care. We've talked about that a lot here today. Your customers care. And ultimately, in our mind, it has to do with trust because your customers and prospects are making decisions every day. Should they continue to work with you. That could be B2B or B2C, and they are making that decision based on the goods and services. Here's all the features and experiences that are being offered, and in that process they're giving data to the company. They want to trust that the company is going to deliver on the good or service and exchange of promise and also not worry about their data. We firmly believe it's not just about fines and regulations. That's really helpful. And the time of this recording, we have 17 states that have passed and actually 17 and a half—there's another state, Minnesota just passed the Senate literally while we're talking. Not the House yet, but we're getting close to the magic 18. So fines and regulations are helpful. They encourage some companies who don't like to violate fines, and most companies want to do the right thing and be good stewards. In our eyes, it's really about doing the right thing. It is building trust with customers, whether it's B2B or B2C, because you have to or because we want to. And we feel right now there's still an opportunity to make it be a competitive advantage because not everyone is doing the right thing. But if you are, then you should emphasize that. We have seen it shorten sales cycles. We've seen it help alleviate any objections that your potential customers might have again, B2C or B2B, And again, our philosophy was this story just needed to be told to the business people at all different parts of the organization. So it's not just for privacy person or legal person or a security person. Then we have found that they like it a lot because then they're able to bring it to the others in their organization and it's explained in a

way that's fun and interesting. We've had people read it on the weekend and really like it, so we really did try and make it a compelling read using stories and real, real stories that are, you know, obfuscated so that we've protected the innocent.

[Kevin]: And, you know. Right. You know, I did a little micro about the book. I love it so much and a little... I'll let our audience in on a little secret: us cyber lawyers, Cyber 1.0 was we told you what we thought you should do and we used fear to get you to comply. If you don't do this, someone's going to hack into your system. You're going to be out of business. You're going to have to spend a lot of money getting back up online. And people didn't like that. Understandably, the reaction was, you know, that's kind of an immature way to approach it. We don't need to be persuaded by fear. So then we switched to a combination of things. Cyber 2.0 was, well, if you don't do this, you're going to have...you're going to face regulatory fines and penalties, as you mentioned, Jodi, and that didn't work really well either. And I think you have seized on the most important reason to do this. And if I may, I'm just going to read... I want to get your reaction on the other side. I want to read a passage from your book. This is from page... part one, page 20 of the book Data Reimagined. It says "Companies that successfully reimagine data as a medium for strengthening their relationship with customers will first earn our trust and then ask the right questions to encourage us to willingly share more of our data with them. These organizations will then safeguard that data, use it for our benefit, be transparent about that use, deepening their customer relationships by delivering tailored messages that create value for us and a powerful competitive advantage for them." I know you mentioned it earlier, but I wanted to use that as a setup. What's your best pitch for how data privacy can create a competitive advantage out in today's marketplace?

[Jodi]: Well, I have two. From a B2B? Well, really, it doesn't have to be B2B. If people are looking to buy your product or service and they're literally looking at all the products and all the different features that are here, privacy is... it could be a very important one. Are you in the financial space? Are you in the health space? Are you going to monitor all my data? I was looking at a video tool the other day. Well, what's the big concern from a video tool? Are my videos being shared and stored? I have really private information. What's going to happen with that? Well, they have an entire section that answers all the questions that someone would have. Are... is my data secure? Are you going to use it for any other purpose? Who else can have access to it? They appreciate and figured out. What is the big concern of a video tool? It's not only how quickly I can edit and do all kinds of fancy things. It's Oh my gosh, you have really sensitive data. How are you making sure that I'm going to feel safe and comfortable there? And they made that a prominent piece of their feature set. So that is one I think, in another one. So the first part of that passage that you read, oftentimes people want to have a lot of data as quickly as possible. Marketers love collecting everything they can right away. And I think as we move into an era that's all about personalization and more and more data, well, how are you asking those questions in a way that I'm going to feel comfortable about it? And often they just go on in. Anyone listening ever answered, I don't want to answer that question. Yeah, why did you answer it? Because you didn't trust what they're going to do with that information, right? The exact reason, if you start slow and build up, it's kind of like building a friendship or any relationship. You typically start slow, get to know each other, and then I give you a little bit more, and I give you a little bit more. And ultimately, okay, you're not going to misuse it. I feel comfortable telling you more about my life and what my concerns are and what I could use your help on. That is how you build a relationship. Asking me right away for 20 different things that you don't actually need right away. I'm not going to give you accurate data. I'm going to give you inaccurate data, if you force me to answer those questions and don't give me my... I don't want the answers. You get bad data. Now, I got a bunch of people making decisions on bad data. And instead, if you put privacy into the pieces and you think about what's the right user experience, what's the customer journey, how am I using this data? That's the idea of "reimagine" how we're actually using the data.

[Kevin]: So what I'm hearing you say is two things come to mind. One, trust is a two-way street. It's not just the consumer or the customer trusting the business with his/her/its data. It's the business being able to trust

the accuracy of the data by creating that opportunity that's safe zone for the transfer of the data. And the other thing I was thinking, and I guess we're near the end of our time, so we'll close here. The other thing that occurred to me was that privacy is not just a legal compliance issue, it's a market opportunity issue.

[Jodi]: I agree a gabillion percent, because so many people look at it as a compliance activity and you ask, what do I do? I said, I help companies comply with privacy laws and I help them build trust with customers. You do have to comply with privacy laws just like you have to comply with a long list of other laws. Most companies don't walk around and say, I don't like that law. I'm not going to comply. The same is going to be true here. However, the level to which companies are complying with the law and again, what do you do with Jodi? I don't really have a lot of laws. You have to deal with me because I'm in Georgia and I don't have any. How do you treat my data? That's all about building trust with customers 100,000% is: what's the relationship that you're going to have with me now, the people you have laws with you. The same applies. You should still get trust with them too. And that is why it is in my mind, a combination—comply with what you're supposed to be doing. But just because you can, because the law says it's okay, then you have to ask well should I? And how should I disclose it? And you might say it's okay to bury it. I disclosed in a privacy notice, but maybe if you pull it out in the feature set, that's the opportunity. That's what's going to distinguish you in earning more sales. That's what's going to be able to help build trust with customers ultimately and make you special and different and unique.

[Kevin]: On that compelling note, we're going to leave it there. Jodi Daniels, founder and CEO of Red Clover Advisors, a privacy consultancy, cohost of the She Said Privacy/He Said Security podcast and very busy entrepreneur on a Friday, which is when we're recording really appreciate you taking some time to sit down with us on Cyber Sip.

[Jodi]: It is my pleasure. Thank you.

[Kevin]: Oh. Thank you, Jodi. Hope we can talk again and until then, in our next episode, we're back soon and take care.

[Kevin]: The *Cyber Sip* podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share, and continue to listen.