THE PERFORMANCE REVIEW PODCAST

Greenberg Traurig

Episode 15

Guest: Lauren Green, Barry's Bootcamp

Philip Person (00:29):

Welcome back, listeners. We have an esteemed guest here, friend of the firm. We're going to call her the incomparable Lauren Green. She's internal counsel at Barry's Bootcamp. It's going to be a fun episode. We're going to be talking about employee privacy. We're so excited about it, that we're going to do it in a two-part series for all our excited listeners. But before we do that, let's talk about Lauren. Lauren, tell us about your practice.

Lauren Green (01:02):

Sure. So, thank you so much for having me. I'm excited to be here. For those that don't know, or haven't heard of Barry's, we are a global boutique fitness brand with studios all over the world. Currently, we have about 40 international studios, which are franchised. I believe the count right now is 45 corporately owned studios within the US.

Lauren Green (01:26):

And then within our studios, we typically have fuel bars where we sell all sorts of shakes, and we have our own clothing line too, where we do very cool collaborations with companies like Nike and Lululemon. I manage all things legal. It varies from franchise to corporate governance, music licensing, contract review, and people in cultures. If I reference people in culture, that's our HR department. PNC, which includes client and employee cyber security initiatives and privacy issues.

Philip Person (02:04):

It sounds like you do everything at Barry's but be an instructor.

Lauren Green (02:09):

Yeah, basically. I think that's right. I know. We've grown very quickly in the last few years and I am a legal department of one, so GT has been just wonderful to work with. Certainly a big help in a lot of different areas for Barry's.

Ryan Bykerk (03:40):

Okay. All well, Phillip just took the words right out of my mouth. Lauren, you do have just an insane, very broad practice. You cover really the waterfront of things over there at Barry's. Today, as Philip mentioned, we're going to be talking about employee privacy.

Ryan Bykerk (03:58):

Among the thousands of other things that you do, how does California Privacy Law impact you on a day to day basis? And maybe what percentage of your role is focused on dealing with privacy?

Lauren Green (04:16):

Privacy is an important piece of what I do. The majority, or the largest amount of studios we have in one state is in California. That's where we were founded. That's where our first studio was launched, and so we have a lot of employees in California. At Barry's, we're fond of saying that we are a fit fam. That means that one of our core values is that we treat our employees with the utmost respect and fairness, which in turn helps build up trust within our company.

Lauren Green (04:49):

Currently, we have just over 1,100 employees across the organization. We take it very seriously that we have a responsibility to those employees, as I'm sure that many of them, if not all want to be assured that their private information is kept confidential. This employee privacy universe includes things such as resumes and background checks to on the job privacy and data collection, storage or dissemination. Our responsibility as an employer is to ensure we have a system in place to protect this employee information. And of course, we're always making sure we're on top of being compliant with all the applicable privacy laws, which are changing all the time.

Philip Person (05:38):

Since today is part one of a two-part series on employee privacy, let's start off by discussing the general concepts about employee privacy. And since we're in California, we have to talk about the California Consumer Privacy Act, which is to be superseded by the California Privacy Rights Act. Let's keep up with our acronyms. We have the CCPA, and then we have the CPRA. We can also talk about what employers can do to comply with the CCPA and the CPRA and some general best practices.

Ryan Bykerk (06:16):

Right. And then in part two, so just a little plug for the next one. In part two, we're going to be discussing some of the more general privacy laws, but again, for today, we're going to focus on CCPA and the CPRA, which [inaudible 00:06:31] at some point during this recording.

Ryan Bykerk (06:33):

Lauren, can you kind of take us through some of the basics on employee privacy and tell us about those two alphabet soups, the CCPA and the CPRA?

Lauren Green (06:42):

Yes, absolutely. We'll try to keep them straight, but privacy rights generally arise from various sources, actually. We can look at the California Constitution, the US Constitution, HIPAA among others. And it's worth noting that unlike in the US Constitution, where there is no express right to privacy, which interestingly enough, I'm sure we're all hearing about these days.

Lauren Green (07:11):

It's only implied, but in California, the right to privacy is expressly stated in the constitution. So, the difference can lead to different outcomes if one is able to prove a privacy violation, but after the EU passed the General Data Protection Regulation, which a lot of people know as the GDPR, California was

the first state to come out with its own privacy law, and that was the CCPA. That became effective January 1 of 2020.

Philip Person (07:44):

Not too surprising that California was the first to come out with the privacy statute.

Lauren Green (07:49):

Right.

Philip Person (07:49):

But that's a CCPA, but there's already the CPRA. What can you tell us about the CPRA?

Lauren Green (07:57):

Right. So, in the November 2020 election, before the CCPA was even a year old, the people of California voted on the CPRA, which is an addendum to the CCPA. So, that law will become fully effective January 1 of 2023. But, everyone should be aware that it does have a one year lookback period, meaning that employers should be complying with it effective January 1 of 2022. So they are hopefully already aware of that and have been compliant with it since the beginning of the year.

Ryan Bykerk (08:33):

Right. Exactly. And if not, a public service announcement.

Lauren Green (08:36):

Yeah.

Ryan Bykerk (08:36):

Let's [inaudible 00:08:37]. So, since the CPRA is more or less an overlay of the CCPA, it probably makes some of the most sense to just start with the CCPA and then cover the CPRA and how it modifies it. So, maybe let's start with the CCPA.

Lauren Green (08:56):

Sure. So, the CCPA protects both consumers and employees. The CCPA applies to for-profit employers that collect personal information from California employees. If their business or their parent or sub-company falls into one of three specific categories. So number one, if the employer is making over $25 million in annual gross revenue. Or, number two, if they buy, receive, or sell personal information of 50,000 or more California consumers, households, or devices. Or, number three, if the for-profit employer derives 50% or more of its annual revenue from selling California residents' personal information.

Ryan Bykerk (09:52):

Okay. So this regulation, you've mentioned the term personal information a few times here, and that's obviously the focus of the CCPA is... Can you... What qualifies as personal information?

Lauren Green (10:09):

Sure. So what the CCPA would say is considered personal information would be, name, social security, driver's license number, email address, financial information. But even things like biometric information, records of products purchased, internet browsing history, fingerprints. So it's pretty broad. But you should be aware too, that per the CPRA text, personal information would not include publicly available information.

Philip Person (10:48):

Interesting. So what rights does the CCPA give to employees?

Lauren Green (10:56):

So, employers should be aware that employees can ask that employers delete or not sell their personal information. But an employer would be allowed to keep the information needed while the employee is employed. And if it's required for internal business reasons. For things such as, complying with a subpoena or defending legal claims.

Ryan Bykerk (11:22):

So can employees opt out of the sale of their information? Just like we can opt out as consumers? Or is there a line drawn there?

Lauren Green (11:31):

No. They absolutely can opt out. An employer should keep this in mind if they sell or disclose information to third parties, or a contract with service providers, if those contracts involve the disclosure of personal information.

Philip Person (11:46):

I honestly don't know how much my personal information is worth. Probably not much, but that's good to know. What is considered a third party under the CCPA? And what is a service provider?

Lauren Green (12:01):

Right. So we need to understand that distinction. So, under the CCPA, a third party is an entity to which a business would sell or disclose personal information for money or valuable consideration. On the other hand, a service provider would be something like your payroll company. And these are excluded from the CCPA's definition of third party. But, there's a qualifier, so in order to qualify as a service provider, the employer must have a written contract with that service provider, or else they could be considered a third party.

Lauren Green (12:38):

So, particularly, the contract with the service provider must include an agreement that the service provider won't use, keep, or disclose any personal information other than what's stated in the contract with the business or employer.

Ryan Bykerk (12:56):

Okay. So, we've covered a lot of this, and in Phillip's question, that's got me thinking about, what is my information worth? And probably not. And what even is out there? But anyway, I won't derail us with

that, although I have to tell you, my mind is spinning. So, Lauren, what does all that mean, practically speaking, as it relates to these third parties and how that works?

Lauren Green (13:21):

Well, okay. So as I mentioned, employees can opt out of this. So that means that if you are a covered business, you need to be able to track those opt-out requests from individuals and have a process in place to ensure their wishes are respected. Employers need to obtain consent from employees to share their personal information, and have these systems in place to track whether consent has been given, and then consult those records regularly, in order to stay out of trouble. You just don't want something falling through the cracks, because I'm sure we'll get to kind of the consequences of that coming up here.

Philip Person (14:04):

And we get calls all the time saying, "What if I don't comply with this law? Phillip, Ryan, what does that mean?" I've always wanted to ask the question. So, what if the employer does not comply with the CCPA? So I wanted to ask you, Lauren.

Lauren Green (14:20):

Yeah. So that's a good question. A California employee could bring a private lawsuit under the CCPA for a data breach. If the personal information was stolen because the employer didn't maintain reasonable security procedures and practice. In order to sue, the personal information stolen must have been non-encrypted, and non-redacted, and must have included the employee's first name or first initial and last name, along with any of this following information. So it would also have to include their social security number, or driver's license number, or some other personal ID number, financial information combined with an access code or password, medical or health insurance information, fingerprint or other biometric data. And then, the attorney general also has the write to assess penalties for violations.

Ryan Bykerk (15:21):

Okay. So that was the word I was waiting for, the penalties word. So, sounds like there are penalties, but what are they?

Lauren Green (15:27):

There are penalties. The statutory damages for data breaches can be up to $750 per employee, per incident, or actual damages, whichever is greater. The somewhat good news is that, employers do have 30 days to cure the breach. But I would say, the main takeaway is that employers should create and maintain security procedures and best practices for protecting employees' personal information. It's much easier to do that on the front-end then kind of scramble on the back-end when you have that just short period of time to try to cure in the event of a breach.

Philip Person (16:10):

We've been giving a lot of love to the CCPA. Let's now switch gears to the CPRA. We don't want it to feel left out. So what's new? What is different? What do California employers need to know?

Lauren Green (16:24):

So, as I stated earlier, the CPRA will be effective January 1 of 2023, but the caveat, again, is that there is that one-year look back period, where you would be expected to be compliant as of January 1 of this year, 2022.

Ryan Bykerk (16:45):

Oh, and one of the things I think that changes here is [inaudible 00:16:52]. Can you explain that a little bit?

Lauren Green (16:55):

Sure. The main changes to the entity coverage include... So there were the three pieces that qualified an employer under the CCPA, and they're mirrored in the CPRA, but there are some minor differences. So the first was over the 25 million in annual growth revenue. They've added language to clarify that is based on the preceding calendar year. Next, they increased the threshold requirement. So for businesses that buy, receive, or sell personal information, it was previously from 50,000. It's now 100,000 consumers or households. And they also removed the devices piece of that. And then the final... or the third caveat was the 50% or more of its annual revenue derived from selling or sharing now California residents' personal information, so it's not just selling. It's also sharing

Philip Person (18:03):

Sounds like the CPRA reduces the scope and impact on small businesses, yet somehow expands the protection to include sharing info as well, right?

Lauren Green (18:14):

Yeah, that's exactly right.

Ryan Bykerk (18:16):

All right. So, in addition to these changes over which entities, I suppose, are covered, what are some of the other changes that we can expect from the CPRA which, of course, we're all already complying with because it has a look back period, but what are those changes we can expect?

Lauren Green (18:33):

Right, I am sure we are all on top of that. So with regards to enforcement, they created the California Privacy Protection Agency specifically to enforce the CPRA. It's also noteworthy that implementing and maintaining reasonable security procedures and practices after a breach will not constitute a cure. And then, additionally, they addressed violations involving personal information of minors under the age of 16 years old. For those instances, they've increased the penalty to $7,500 per violation. And then, finally, the private right of action was broadened to cover breaches of email addresses in combination with a password or security question or security question and answer that would permit account access.

Philip Person (19:39):

You're giving us a lot of fun news here, Lauren. Thank you for that. But I want to ask you, what can you tell us about the expanded protections for the employees? I'm guessing that under the CPRA, the employees can opt out from the sharing and selling of their information. Is that right?

Lauren Green (19:59):

Yep, that is right. Some of the expanded protections include... They now protect selling and sharing personal information. Employees have the right to opt out from sharing info, not just selling. The employer must use reasonable efforts to correct information if an employee requests. That and the CPRA also created a category called Sensitive Personal Information. So, previously, the CCPA didn't define or treat any differently sensitive information. So now the CPRA does that, where the sensitive personal information employers are limited to using that information as only reasonably expected by consumers and employees.

Philip Person (21:02):

A lot of our audience members are GCs, HR folks, or just people who are wearing lots of different hats. So you may be the perfect person for this in your million job duties that you have to do. Can you tell us what can employers do to comply with the CCPA and CPRA, and what are some of the best practices?

Lauren Green (21:25):

Sure. So I've spent a lot of time thinking about that very question and so I hope people maybe have their notebooks out and can keep track of this and look back on it later, but-

Philip Person (21:41):

We're all taking notes.

Ryan Bykerk (21:43):

Everyone at home, get your notepad out right now.

Lauren Green (21:46):

Exactly, because here it comes. So they should be implementing reasonable security procedures and practices to protect personal information. That includes such as data, inventory, and mapping if possible. And I would highly recommend they designate a team that would be responsible for compliance and employee privacy inquiries. Another thing they can do is review corporate contracts and correctly classify service providers and contractors from third parties. And that means ensuring the corporate agreements are in compliance. If you'll remember, I spoke about making sure that any agreements with third parties expressly prohibit the sale or unauthorized use of employee information other than for specified purposes. Employers can also update and maintain employee privacy policies or notices. They should give notice to employees about what information they're collecting and how they're using it and then also making sure that they're accessible to employees with disabilities.

Lauren Green (22:58):

Any notice must link to a privacy policy and include what employees' rights are. They should be open and tell employees if their personal information is being sold or disclosed to third parties for business purposes. And then make sure to give employees an easy option to opt out and communicate that process to them. If an employee so requests, they should delete information or an employer should delete the information on their server and any service provider server as well, making sure to correct inaccurate information as necessary. And then a few other points to consider is I would recommend against asking employees to waive their rights under the CCPA and making sure that you don't retaliate or discriminate against employees for exercising their CCPA rights. You maybe consider updating policies to include anti-discrimination or retaliation pertaining to the CCPA and the CPRA. And then, finally, I

would just say you should be consulting on a regular basis with council regarding compliance, particularly when it comes to selling and sharing information with third parties.

Philip Person (24:15):

I like that last point, consult with council. I like that.

Lauren Green (24:17):

Yeah, I'm sure you do.

Ryan Bykerk (24:20):

Yeah, just a reminder to listeners, you can now pause that, you can rewind it. I'm sure your hand is cramping from taking notes on that. That was fantastic, Lauren. Thank you. And, really, just tons of really good best practices. One of them, by the way, I should point out Lauren mentioned, maybe designate a team. If you can't designate a team, try and find somebody like Lauren who is a one person team, who's handling things like this. Fantastic. Thank you so much, Lauren. That's a ton to digest for part One of our Part Two series, and we're very excited to have you back for Part Two here shortly. So, as I'm sure you know because I know you listen to the Performance Review Podcast every single day just repeatedly, that's all you do is listen to our podcast, I know you're aware that we always ask for a crazy employment story from all of our guests at the end of any episode and we would like to do the same here. We are eager to hear a crazy employment story from you.

Lauren Green (25:19):

Sure. So, yeah, I saw this one coming and so the thing that came to mind was actually an incident that occurred to me very early on in my career. I was working for a company in their legal department and we had an employee. He was a very nice man, worked in our accounting department. It was a very small company and so it was a smaller accounting department. Everybody knew everybody. It was a small office. But as I was heading into the office one morning, I had another coworker send me a link to a news story, and I opened the link and the headline was something like "Accused embezzler stashes nearly $770,000 in cash behind the drywall of his house." As I'm reading it, I realized that this story is about this very nice man in our accounting department. And so this was something that he had done with a previous employer right before he started working for our company and I think he was our controller. So, I mean, okay, we find out this information and we know, all right, we're going to have to terminate this employee. And so this isn't that exciting of an employment law story necessarily because, first of all, he was almost surprised because the twist of this story is that when he was found out by his previous employer and confronted about it, he admitted it and returned every single penny that day. He had all of that cash hidden in the drywall of his house and did not spend one dime of it. He had just hoarded all of this. I honestly don't know what the plan was, but it stuck with me because you put all this effort into investing all this money and he did not spend a dime of this money. And he thought because he returned it all that, that would just be the end of it. "Why is there a problem?"

Ryan Bykerk (27:40):

Oh man.

Philip Person (27:42):

What was that supposed to be, retirement? I would have so many questions for this guy. What were you planning to do with it? Just sit on it.

Lauren Green (27:49):

I don't know. Honestly, I think what I recall the rumor was, I don't know if things were going great in his marriage, and so I think maybe he was prepping for, I don't know, him leaving, her leaving and he needed cash. I don't know, but I just found it fascinating that he just didn't even spend a dime. We had to terminate him and there was no drama. He was still very nice about it. It was very odd.

Philip Person (28:19):

Maybe he was so smart that he said, "Let's keep the money in the walls. We're going to go through the divorce proceeding. I get the house. You get everything else."

Lauren Green (28:26):

Yeah.

Philip Person (28:27):

Right?

Ryan Bykerk (28:29):

That's an interesting story.

Lauren Green (28:29):

I'm not sure how it was going to play out in his head.

Philip Person (28:31):

I don't know, but this is interesting.

Ryan Bykerk (28:34):

Wow.

Philip Person (28:34):

See, stories like that, stuff movies are made of.

Ryan Bykerk (28:37):

Yeah, that's fantastic.

Philip Person (28:39):

Yeah.

Ryan Bykerk (28:41):

I have so many questions, I don't even know where to go, but anyway.

Philip Person (28:43):

[inaudible 00:28:43].

Ryan Bykerk (28:43):

We'll leave it at that. Thank you. Thank you so much, Lauren.

Philip Person (28:47):

So, Lauren, thanks again for joining us. We hope that you can join us on Part Two of the Privacy Series. And for all our listeners, stay tuned, and if you have any questions, email us at performancereview@gtlaw.com. Shows how much I email ourselves. That's it, and we look forward to seeing you all on the next episode.