Hal Ostrow:

The amount of data that's stored online doubles every couple of years.

Jeff Large:

Meet Hal Ostrow, an attorney and shareholder at Rhodes McKee.

Hal Ostrow:

And businesses have lots of data, primarily other people's and other businesses' data. A lot of what we're doing now is what they can do with that information and what they can't do with that information.

Jeff Large:

Today on Conversations With a Business Attorney, Hal and I are discussing the massive topic of information technology, cybersecurity, and privacy. I'm your host and fellow business owner, Jeff Large. Hal and I wasted no time jumping into this topic and this episode will be great for you if you're interested in a couple key things, how privacy laws vary based on your geographical location and how they affect your business. The importance of having agreements in place in order to cover things like this, especially when you're working with other clients or collaborating with creatives and what to have in place for when you inevitably get hacked. Yes, I hope you don't, but just in case, it's still really helpful information. But to begin, Hal and I start with the topic of personal data and how businesses are allowed to use it.

Hal Ostrow:

What is personal data? A good baseline definition of personal data is if you have information about somebody else that can be used to identify that somebody else, name, address, email address, something like that. Most states that have laws on this would consider that to be personal data. With the realm of federal law, there isn't yet a national standard, but there are a number of different laws, rules and regs. HIPAA is most frequently talked about. FERPA for education records and some others, and they generally use that same definition, that if a bit of information can be used to identify an individual, it's personal data. And then when you get into religious beliefs, sexual orientation, who's married to whom, things like that that many people would consider to be really private. A number of states consider that and the EU considers that to be what's called sensitive personal information or sensitive personal data. And so there's an even stricter standard on what businesses can and can't do with that level of information.

Jeff Large:

Okay. Like in terms of who has the data, what if I am using a third party service, what if I have an email provider that's the thing that maybe I'm getting the email but it's all that information stored on their platform. Or if I'm using say a third party payment gateway and it's not technically in my own database or on my own server, but on theirs, am I still liable for that?

Hal Ostrow:

That's a great question and like so many questions that people ask attorneys, the answer is it depends. You need to worry about making sure that your vendors are taking appropriate safeguards with information that you are obtaining in their processing.

Jeff Large:

So I can be liable for my third party vendor that I'm using?

Hal Ostrow:

Potentially. You want to make sure that you've got an attorney who's read your agreement with that vendor and then that vendor's agreement with the end user to make sure that if that vendor does something that it shouldn't or doesn't do something that it should and the consumer comes after you or asserts a claim against you that the vendor would indemnify you.

Jeff Large:

Okay. All right. That's interesting. The other piece that you started talking about is the variations almost, of these laws because it sounds like some of the laws change based from state to state based on nation or even country to country.

Hal Ostrow:

Correct.

Jeff Large:

How do I begin to even think about that as a business owner or what aspects matter to me the most?

Hal Ostrow:

Sure. So the first thing that I generally advise a client to think through is where do your users live? If you don't have X number of users in California and you're probably not going to in the next year or two, and I always try and be a little bit forward-thinking, so not just where do they live today, but where are you planning on doing business and where might your users be living in the next year or two. If you don't have 100,000 users or users with 25,000 different devices or something like that, in let's just say California or Connecticut, and I'm choosing two states that currently have privacy laws, then you don't necessarily have to worry about complying with those. But there's a caveat to that.

Apple and Google are now requiring anybody submitting an app to the App Store or the Play Store to have privacy policies that really go beyond what current state law requires. So one, you've got to think about where your users are, and two, you've got to think about what platform you're using and what you need to do to comply with that platform's requirements.

Jeff Large:

Okay. So we're setting the stage of some of the things that we need to be concerned about. What does all of this practically mean for a business owner? Do I need to have specific documents in place to safeguard me? We've said privacy a couple of times now. I know a lot of people are familiar with websites normally will have terms of service and then the privacy policy available. What do I need to actually do to begin decreasing my liability or safeguard myself against some of these things that we're talking about?

Hal Ostrow:

Oh, that's a great question. So it used to be that privacy policy would be a couple of paragraphs and it's still the thing that people scroll through and say, "Yeah, sure, I agree with it," and

probably haven't read it. One of the trends both with the EUs GDPR regulation and state privacy laws explain that-

Jeff Large:

Because that's a big thing.

Hal Ostrow:

Well, let's set that aside and come back to it for a minute.

Jeff Large:

Okay. All right. Sounds good.

Hal Ostrow:

But one of the trends is clarity. And so not only do you have a right to delete your information and a right to correct your information and a right to access your information, but you as a consumer according to a lot of these laws, have a right to know what exactly a business is doing with your information in a clear, concise way. What that means is that these policies have actually gotten longer and not shorter because if a business has to explain to you in a clear concise way what exactly it's doing with your information, it takes a little bit more space to do it. Because every business does something a little bit different with other people's information or with personal data, you can't really or really shouldn't, just copy and paste something that you found online, half of which probably isn't going to be applicable to your business.

So yeah, privacy policy is a good jumping off point, but that policy really, we can't just write something that says Business A does X, Y, and Z with your information. We really need to make sure that we're capturing what exactly the business is doing with your information, whether it's selling it, and by the way, selling doesn't just have to be for cash or for money. It can be bartering, it could be trading your information for other people's information. So if a business receives something of value, that's considered selling it. So we really need to know what the business is doing with your information and making sure that there's a mechanism in place for you either to opt in to allow that or opt out to prevent it.

Jeff Large:

There are so many different aspects of privacy. You are bound to see many of these things and these variables overlap one another. Another important one is the general data protection regulation or commonly known as GDPR.

Hal Ostrow:

Now, you asked about the EUs GDPRA. A couple years ago, you probably started seeing these popups every time you went to a site. This site uses cookies or this site uses tracking pixels or something like that and allow some, allow all that's because the EU passed an EU wide regulation called the GDPR that really gets into what businesses can and can't do with personal information including tracking you as you go from site to site. And so because most websites can be accessed not just in the EU but also around the world, we here in the US started seeing a lot of these popups asking us to grant permission for that website to track us as we're there. The EU is very strict about this. If you have just a couple handful of users in the EU, then you've got to comply with GDPR.

Jeff Large:

Yeah. So to clarify, for me, I have a bit of background in web development and so I saw a lot of my marketing and web development friends panicking around the deadline for that and just of, we've been using the acronym, but the general data protection regulation is what we're discussing here, what are the practical implications of that for a US user? Because I know somebody could think like, oh, I don't have anybody in the EU, but to me on the other end of this, it feels like that's impossible to not have somebody interacting with you on the EU. So it's like-

Hal Ostrow:

But where we get into it more or we've gotten into it more lately and yes, you're right. All of my web developer clients were, panicking is a very family friendly word for how they were around the time that GDPR took effect. Now what we're really getting into is flow of information or data flow from the EU to the US. So if a business is gathering information in the EU but storing that information in the US, it's in flux right now in terms of whether or not more US companies according to the EU, can actually comply with the GDPR's requirements. And so we're really analyzing the flow of information, how it's getting from the EU to the US, what's being done with it once it gets to the US, and making sure that it actually does comply with GDPR. So really, any business that has users in the EU or could have users in the EU and is gathering information in the EU or even here, gathering information here or somewhere else on an EU resident has to comply with GDPR.

Jeff Large:

Okay, so let me clarify a couple maybe more things. This is other stuff that's just come to mind when users are submitting information via a form or email or that's sort of the stereotypical thing. But then there's also other types of interactions where they might be vendor friends or something where you are going back and forth via email and there's a lot of personal information. The other thing that comes to mind for me even to what you just said is I know say for example our business, the website host is based in the EU, so I'm assuming servers or things are there, but the primary focus or become our primary target audience is here in the US and so does that open up a different type of can of worms, like when you have this cross information going back and forth?

Hal Ostrow:

No. That's such a great question and it may. And I would never assume that the server resides or is in the EU necessarily, particularly with redundancy. So we're going to have some information that may be stored in the EU and some information that hopefully is stored somewhere other than in the EU just for redundancy's sake. And then you've got to comply with both jurisdictions. What's really nuanced, it's really complicated and I hate to go back to this answer, but it really just depends. I think the best thing that a business owner can do would be to really take a deep dive into this with their attorney and probably with their data vendors and say, "Okay, what are we gathering? Where's it being gathered? Where's it being stored and what do we need to be doing to comply with all these laws, rules and regulations?"

Jeff Large:

When would you recommend with the... Because it's like so many of these things I can tell you from the conversations that we've had throughout this series, all of it almost feels like do it all at

once. Do it in the beginning. But I know for us, when I think back to our beginning, I didn't have that funds to go through with a bunch of different attorneys and figure out all these different things that these operating agreements I need to have in place and my privacy agreements and all this. So when practically speaking, in your opinion, is a good time to actually address this issue?

Hal Ostrow:

My general advice on that is it always costs less to do it proactively than reactively. Always. If you're doing it reactively, you're responding to somebody making a claim against you most likely, or responding to circumstances that are beyond your control. But if you do it proactively, you spend a little bit of money on the front end, you save a lot of money on the backend. So if your business is starting out, I would certainly budget some for legal and compliance and ask your attorney, "Okay, what's a fair budget for this? How much time is this going to take? What's a budget for this?" And so when you're doing your business plan, you can include that in it.

Jeff Large:

Now, another thing that is in the same vein, so we've been talking about maybe some of the liabilities, how it works, a couple of the practical implications that we can take or actions that we can take in order to address it. Another piece of this that you mentioned that is interesting to me is this idea of data ownership. What kinds of information are being transacted and who actually owns it? Is it you? Is it me? Is it something else?

Hal Ostrow:

Yeah, so that's another great question. You've clearly done your homework around this. So I'll give you a couple of different instances.

Jeff Large:

Yeah, give me scenarios and stories.

Hal Ostrow:

So here's one that just coincidentally, I was talking through with somebody last week. More and more universities are tracking student athletes' metrics, not just on Apple watches or other devices, but they have other wearable things where they're tracking all kinds of metrics and they're tracking sleep and they're tracking nutrition and they're tracking how hard a baseball player's hitting a ball, what the trajectory is, what the launch angle is for pitching, how fast it is and all kinds of different things. Is that the student athlete's data? Is that the university's data or is that the wearable manufacturer's data? And really, at the end of the day, because it's part of their educational record and FERPA, the federal statute governing educational records is so broad, it really is the student athletes data. But universities don't necessarily want to give it to them because one, they can try and leverage it for increased NIL and get more money that way, but also because it can be taken out of context and they can be using it for things that it shouldn't necessarily be used for or wasn't intended for.

Jeff Large:

Who's to say that though? This might be a weird tangent, but who's to say that it shouldn't be used for that if it's the student's data?

Hal Ostrow:

Well, that's exactly right.

Jeff Large:

Okay.

Hal Ostrow:

Yeah. The University's playing Big Brother and deciding, we don't necessarily want to let you compare your data with somebody else's, but at the end of the day, if the student asks for it, because of FERPA, because it's part of their educational record, if the student athlete asks for it, it's theirs. The university has to give it to them. Let's just say that the client hires you to develop a website. You are not going to create it from scratch. Just like a lot of the agreements that we do here are not going to be necessarily from scratch. It's not a particularly well-kept secret that we have concepts that we use over and over again. You have code that you use over and over again. If I hire you to do something for me and I pay for it and you give us a deliverable, is everything in that deliverable ours or is it ours just for that specific purpose of website? Are we going to go through and reverse engineer it and take outlines of code and say, "Oh my gosh, this is the greatest code in the world. We can resell this."

Presumably in your services agreement with us, with your customer, there's something in there saying you can use what I'm giving you for the purpose for which it was intended and not for any other purpose. And you can't go through an reverse engineer and decompile it and take scrape lines of code out of it and resell those lines of code. I'm licensing it to you really for that specific purpose, but I'm not giving it to you to use for anything in the world that you want to use it for.

Jeff Large:

That's definitely fascinating because you see it like I said, even for me in our development days, you would have aspects of that where sometimes aspects of it would be custom. It would be specifically built for that person or whoever the client you're working with. Sometimes, if you're using an open source type platform like a WordPress or something along those lines, or even Shopify or whatever it is, there's just generic code that's available to everybody and it's not like the client all of a sudden gets exclusive rights over that piece. And then even in the same way for say what our company's doing now with these podcasts and everything, it's like we'll have templates that we follow with different styles of show notes. It's pretty well accepted to anybody who listens to podcasts that there's pretty standard formats people will follow. But what about in the situations where maybe a contract doesn't exist? Say you and I, this wasn't more a formal agreement, but you and I were just sitting down for an interview and you're coming on my personal show, we don't sign anything. What does that look like?

Hal Ostrow:

I would advise creative professionals to call me or call another attorney and have an agreement defining what you can and can't do with that content.

Jeff Large:

So it sounds like when we're collaborating with other people, should we always have an agreement in place?

Hal Ostrow:

If you can, you should.

Jeff Large:

But if I'm going to push back a little bit, do you feel like that's realistic?

Hal Ostrow:

I'd go back to you really ought to have an agreement in place, and so many disputes arise. I've got one right now that's in litigation where a business hired a creative professional to do something for that business. There wasn't an agreement in place, and here we are several years and several hundred thousand dollars later and they're fighting over who gets what because there wasn't an agreement in place at the beginning of the relationship.

Jeff Large:

When you say who gets, what type of things are being fought over right now?

Hal Ostrow:

Revenue and content. So content on the website and revenue over the product that was sold or that is being sold on the website. I go back to, it's always easier and less expensive to have these agreements in place at the beginning of a relationship than after the relationship goes sideways.

Jeff Large:

Yeah. Of course.

Hal Ostrow:

And if you're going to use somebody else's, whether it's their likeness, whether it's their opinion, whether it's their presence on your podcast, but somebody else's something, you really ought to have parameters of that, even if it's not a formal contract, even if it's just an email. Though, I don't advise that. But even if it's just an email or something that you can look back on later and say, "Okay, I agreed to do X, Y, and Z for A, B and C. And that means you get to use X, Y and Z and that's it. And you've got to pay A, B and C, and that's it. Nothing more, nothing less. And if it's outside of that, then it's not really subject to that agreement then you really ought not be using it."

So privacy policy is when you're collecting other people's information, what they're giving you permission to do with their information. What we're talking about now is more of a services agreement. If I'm hiring you to do a project, what are you doing? What are you getting for it? What am I getting? What's the deliverable that I'm getting? What am I paying for? And what are you selling to me and what are you licensing to me?

Jeff Large:

Now given Hal's already explained this, but to recap, when it comes to privacy, you need to have an understanding of what you are collecting, how you are collecting it, and how you are using it. When possible have agreements in place. Now, another aspect of informational technology is properly understanding a terms of use agreement.

Hal Ostrow:

You go to most websites. You talked about the privacy policy. I think we've talked quite a bit about a privacy policy, but we haven't really talked about the terms of use. And that is, what as a user, you can do on this website and really what you can't do? For website hosts, for companies that have websites, if you've got users interacting on them, not just browsing them and looking at what's on your website, but actually being able to post things on your website, then you want to have some content standards so that if somebody posts something-

Jeff Large:

Postings being anywhere. Like submitting an article to forums to all of that.

Hal Ostrow:

Particularly forums. If a user's going to be able to post something to a website, you want to be able to police it. And if somebody points out to you that it's offensive or if you just happen to see on your own that it's offensive and you really want to be able to delete it and to maybe block that user if need be. And the best way to, again, this goes back to a recurring theme in this podcast, prevention. You want to have clear unambiguous standards at the outset and not just do this in reaction to something but out the outset so that you can remove that content.

Jeff Large:

That makes sense. I feel like maybe if we transition a little bit. So we've been talking a lot about the collection, the use, the legal aspects around collecting data. What about cybersecurity? What do I need to be thinking about as a business owner in that realm?

Hal Ostrow:

So I think most cybersecurity experts, whether they're IT vendors or law enforcement officials will tell you at this point, it's more a matter of when you're going to be hacked than if you're going to be hacked. So from a business perspective, from an information security perspective, you want to have policies in place governing how your employees and others access your corporate information. Odds are, it's not just your business's information, but again, it's other users that you're doing business with, you're going to have a lot of their information.

So you're going to have pretty comprehensive policies in place in terms of what your employees can do with your information. Websites that they can and can't go to. How when they step away from their computer, just something as basic as when you step away from a computer, lock your computer, so somebody else can't access it. If you're accessing corporate data from offsite, being safe about that. It means what you can and can't do or should and shouldn't do with mobile devices, with public wifi networks, things like that. So you want to have pretty comprehensive policies in place that make it less likely that you're going to be hacked. And then you want to have a policy in place for, and again, it's a recurring theme here, prevention, but you want to have a policy in place for what happens when you are hacked. And a cyber response policy.

Jeff Large:

These policies, are you saying that they're just strictly policies? These are the practices that we use as a business, or are these things that are say, written into contracts when you hire an employee or things along those lines?

Hal Ostrow:

Both. No, great question. And I think the appropriate answer there is both. So some of them are best practices, things that all employees should aspire to do. If I had my choice, employers would require employees to adhere to these, but practically speaking, we know that that doesn't happen 100% of the time. And then they're often in company handbooks. They're often in contracts, and then a lot of businesses will have mobile device policies. So if a company's giving you a phone to use, this is what you can do with it, this is what you can't do with it. If a company's giving you an iPad or something like their tablet to use, this is what you can do with it. This is what you can't do with it. And if you're using your own device, and really the pandemic, I think, changed a lot of these policies dramatically, right? Because people had to use their own devices to access corporate information, what you can do with it, what you can't do with it, making sure that to the extent possible, it's not a shared computer.

If you're working from home and you've got one computer for three, four, five people at home, you want to make sure if you can, that your kids aren't going to be able to access corporate information.

Jeff Large:

I feel like that did shake up things a ton, especially when you look at massive units like call centers when they got moved to home or especially the financial sector. We saw that second hand with a lot of things that were going on of businesses all of a sudden in the position of how in the world do we maintain the same level of security when all of our workforce is working remotely?

Hal Ostrow:

Right. No, exactly. And even thinking through professional services, whether it's legal services, accounting, things like that, where we've got very strict rules governing what happens if and when other people overhear our conversations. We had to make sure that when we're talking to clients and we want to maintain attorney-client privilege, there's nobody around who can overhear it. Go somewhere in your house where other people can't overhear that conversation.

Jeff Large:

That's fascinating. It's like a lot of the people are wondering like, oh, it's not going to happen to me, but it's like, no, it probably will. What is a cyber attack? For somebody that might not know, we jumped into it quickly, but just at a base level, what does that even mean to get hacked or to have a cyber attack?

Hal Ostrow:

It means somebody somewhere is accessing information that doesn't belong to them, that they shouldn't be accessing. Right? And it could be anything from somebody reading other people's email, to somebody tracking what you're typing on your keyboard, to somebody targeting a high level exec to get information that can then be exploited to damage a business, to ransomware, right? Shutting down a corporate network and saying, "If you don't pay me whatever, and it's now in crypto, this information's either going to be deleted or worse yet, used to then move on to another target."

Jeff Large:

As my conversation with Hal continued on this whole world of hacking and cybersecurity, he brought up an interesting term that I haven't heard before. Cyber hygiene. This basically means that you are making sure your users, your employees, et cetera, are not clicking on links or accessing sites that they shouldn't be, that could allow someone to hack you or them. Here, he explained some tips and warnings on how to improve your company's cyber hygiene.

Hal Ostrow:

IT infrastructure, and a lot of companies now are doing a couple different things. One is, they're really annoying and they're really effective and necessary. The header of every email it says, "This comes from outside of your organization, be careful about clicking links," and data tells us that that really helps cut down on the number of times that employees will click on links in emails that they shouldn't. Another thing is training and not necessarily naming and shaming people who aren't doing well with the training, but helping people to really understand, yeah, this is going to happen here and I need to be really careful about the sites that I go to and the links that I click and emails.

Jeff Large:

All right. What about maybe more broadly speaking, just because I know this is a huge part of your specialty, what questions do you feel like you're getting asked the most?

Hal Ostrow:

Sure. No, great question. One of the things that we're trying to be proactive about now is really tracking the changes in state privacy laws. It's changing all the time, even between the beginning of the year and now, a couple more states passed data privacy law and we're tracking national data privacy law coming through Congress that hopefully knock on wood here, will get passed. I don't say that necessarily, hopefully because I have some vested interest in it, but because it'll make it a lot easier for my clients to not have so many inconsistent standards to comply with. But more often than not, it's okay, what do I have to comply with? And going back to one of the first things we talked about, how in the world do I make sense of these conflicting statutes?

Jeff Large:

Yeah. That's to me even where my head goes as business owner where it's like, I don't understand how this isn't just an endless investment with the way that things change. I would assume the attorney would know, but are there things that I can do to be more all encompassing? Are there things that I can do to just address the issues in a way that I don't have to keep going back to my privacy thing and changing it or my terms and changing it?

Hal Ostrow:

Good question. What our advice generally is, is to pick the strictest possible standard that you might have to comply with and make sure you comply with that. And if you comply with that, then odds are, you're complying with lesser standards in other states. And really before, we're thinking about where your users are, where they're going to be, how many you're going to have in each jurisdiction, and what is the strictest possible standard that you can do to comply with that jurisdiction's data privacy. And then really to go back and double check and make sure that it's not inconsistent with another jurisdictions.

Jeff Large:

Like I've already mentioned, this is a massive topic with lots of intricacies. So I asked Hal what he recommended that business owners think about before they have a conversation about it with their attorneys, and he gave a solid answer centered on your businesses' responsibility.

Hal Ostrow:

The policy isn't just what we publish on your website. The policy is really getting to know what you are doing, advising you on what you should and shouldn't be doing, and making sure that we have a policy that describes that to people taking a look at your website or interacting with you so that it's not just that, yeah, we're going to scroll through that, we're not going to read it. But if somebody actually does pay attention to it and read it, they will know what exactly it is that you're doing and what your responsibilities are and what their responsibilities are.

Jeff Large:

A lot of this comes back to obviously addressing some of those baseline things that we said with just how is data collected, how is it used? But it feels like clarity is just a huge piece of this whole thing. Clarity and then especially... Maybe clarity more for the user's sake. And then it sounds like, like you said, even just giving yourself a standard, whether it's the "strictest standard" or something to just begin working off of. I think when we get to this point, it feels a little less daunting to me when you explain it that way.

Hal Ostrow:

I think so. And one of the common threads through the more recent legislation on this, whether it's GDPR, whether it's California or some of the other states that are passing legislation, is not just right to know what a business knows about you and what a business does with what it knows about you, but really, a right to have that broken down into the clearest, most concise possible way.

Jeff Large:

Are there any stores that come to mind? You mentioned the one about it getting messy and the two parties arguing over data. Are there any other good illustrations you can think of? Is there anything that's come up where your client was proactive and it saved them a lot of headache?

Hal Ostrow:

The better stories are the ones where they weren't proactive. Just that trying to untangle people from one another or businesses from one another. So a few years ago, agent from the FBI showed up at a client's door and scared them, and it turns out that client was itself a victim of a cyber intrusion.

Jeff Large:

What does cyber intrusion mean?

Hal Ostrow:

People who shouldn't have accessed that company's data access that company's data and were preparing to publish it in a pretty well-known tech journal.

Jeff Large:

Okay.

Hal Ostrow:

And there wasn't really anything that this client could have done better or differently necessarily. I guess I'm using this as a way of saying that a lot of times, law enforcement's going to get involved after the fact and let you know, and this is again, more of a when than an if. And out of that, we've developed a really good relationship with local, state and national law enforcement who deal with these things all the time. And I think that was the first time that we'd worked with the FBI on a cyber intrusion, but it certainly wasn't the last time that we've worked with the FBI on a cyber intrusion, both in terms of the FBI notifying us that our clients have been victims, but also, us having a really good resource that we're really grateful for to go to when we think that clients may have been victims.

Jeff Large:

That leads me to a separate question that I think is pretty pertinent. What should I look for as a business owner? It seems like to work with a law firm or an attorney who has that type of relationship seems like it would be very important. What would be some qualifications if I'm trying to seek out an attorney to help me with something like this, what would you suggest that they know?

Hal Ostrow:

Sure. So there are a few of us in town who have this now. It's called the CIPP/US certification, so Certified Information Privacy Professional US. So US is for here, E is for the EU. There are a few of us in town who have that certification, and what that means is, had to go back to school and study about this stuff and take a test that's pretty challenging. It's pretty all encompassing on state law, federal law to some extent, EU law. So I would make sure that the professional that you're working with has a pretty good baseline, and that's an objective way of determining whether or not that professional isn't just telling you they know what they're talking about, but that somebody else is actually determined that this professional knows what they're talking about.

Jeff Large:

What is the name of that certification again?

Hal Ostrow:

CIP, C-I-P-P, and then /US. So I know there are a few of us in Grand Rapids that have it. I would look to an objective standard of making sure that the person that you're working with knows what they're talking about. I have colleagues here who have certifications in other areas, mergers and acquisitions and that sort of thing, and I just think it's a very good objective way of saying, okay, somebody who knows what they're talking about has said that this person knows what they're talking about. So I would look to that.

I would in an interview, ask for examples of projects that a professional has worked on before. References are tough because so much of what we do is private. I have a lot of clients that don't necessarily want you to know that I'm working for them. I'd asked some of the questions you asked before, like okay, tell me how you've responded to this situation. Tell me how you've

responded to that situation. Have you dealt with hack or cyber intrusion? And have you worked with law enforcement? Have you worked with insurance companies? That sort of thing. And what have you learned from that? What have you done differently as a result of that experience?

Jeff Large:

Perfect. Is there any final advice you'd like to make our listener heard before we wrap up?

Hal Ostrow:

An ounce of prevention is worth its weight in gold. Don't enter into relationships without contracts. Don't enter into B2B relationships without contracts. Make sure that you've got at least a baseline understanding of what your rights are and responsibilities are and what your customers or clients' rights and responsibilities are.

Jeff Large:

Big thanks to Hal Ostrow for sharing his time and wisdom on today's show. If you have a need when it comes to privacy or cybersecurity, consider reaching out to Hal or one of his peers. You can learn more at rhodesmckee.com. That link will be in the show notes.

Conversations with a Business Attorney is a project of Rhodes McKee and is produced by Come Alive Creative. Thank you to Rachel Workman, Isador Niavez, Elaine Mohre, and everyone else who helped make this episode possible. I've been your host, Jeff Large. My final request, if this is something that you actually found helpful and you have somebody in your life who would benefit from it, please make sure you share it with them. Thank you.