Speaker 1: Welcome to the trade secret law evolution podcast, where we give you comprehensive summaries and takeaways on the latest developments and trends in trade secret law. We want you to stay current and ahead of the curve when it comes to protecting your company's most valuable assets. I'm your host Jordan Grotzinger.

Speaker 2: Welcome everybody to episode 33, uh, the trade secret law [00:00:30] evolution podcast. As our listeners know the purpose of this podcast, uh, is to keep you current at a high level on trade secret law. And that's why in every episode or almost every episode, we discuss the latest cases, uh, and, and specifically the evolution of the law and important developments today, we're going to do something a little different instead of discussing cases, we're going to discuss a key element of trade secret cases [00:01:00] that is not thoroughly addressed in the law, but is an essential, uh, subject that you see often, if not in every case these days. And that is forensic investigations, which is something that is often necessary, whether you're on the plaintiff or defense side. And these days, of course, most trade secret theft happens electronically. So if you're a plaintiff, you need to figure out [00:01:30] what happened and what was taken. And if you're a defendant, you presumably want the truth, uh, which may be suggest that there wasn't trade secrets theft. So with that, I'd like to introduce our guest, Jim Vaughn of, uh, I discovery solutions. Uh, he is the managing director and a leading forensic investigator in this space. Welcome, Jim.

Speaker 3: Thank you, Jordan. Thank you. Thank you.

Speaker 2: And you know, since it's 2021, and we do everything remotely, [00:02:00] you will hear the occasional being of a text or email, uh, and there's nothing we could do about it. So bear with me. So, Jim, uh, can you tell us briefly how you help clients in the context of trade secret investigations?

Speaker 3: Sure. And I love the fact that you led off with whether you're the plaintiff or the defendant, because, uh, the, the process is generally the same, you know, and you're, you're looking at different things and you want to, uh, you know, you want [00:02:30] to understand, like you said, you want to get to the truth. And so whether you're analyzing devices or looking at enterprise systems are looking at audit logs, their side plaintiff or defendant, those that will help you make some determinations on what type of, uh, risk there was and what may have occurred. And that's what I generally do that and testify about these types of issues on behalf of, uh, parties, whether the plaintiff, the defendant, and I do a lot of the, uh, forensic neutral [00:03:00] in between stuff for both parties.

Speaker 2: When we talked earlier, you mentioned taking a holistic view of, uh, the data or devices you're examining. Can you explain what you mean

Speaker 3: By that? Sure. So in terms of a holistic view, what I mean is, uh, for example, I know that if you think about how we've evolved over time, you know, I started doing this, uh, 20 years ago [00:03:30] and, uh, yes, Palm pilots were very popular back then in a very long time. That's right. We used to have to keep them charged up in the evidence room. Otherwise you wouldn't be able to get any data off, but, you know, as we evolved, you

know, today, I mean, you still have your laptops and you still have your desktops and you still have your, uh, what you call file servers, your network locations. And those are, uh, now they, they sometimes are still referred to [00:04:00] as the traditional data sources, but as we've evolved, there's, there's a lot of other cloud-based systems and there's collaboration systems and there's auditing trails. And of course with COVID now everybody's working remotely and working from home. And so there's a lot of things that you can think about in terms of a holistic view around, uh, these trade secret investigations. And that's generally what I mean by that is let's, let's think of take a look at everything in the big picture.

Speaker 2: In other words, [00:04:30] you know, it's not, it's not just a, uh, a hard drive and an iPhone anymore.

Speaker 3: That's right. It's funny, you mentioned the iPhone. I mean, we're going to probably talk about that a little bit later, but even on the, uh, the iPhones and the Samsungs and the mobile devices with all the, uh, the BYO D or, you know, bring your own device, that becomes, uh, an issue in and of itself for a lot of companies nowadays. So

Speaker 2: It sounds like one of the first important factors to consider again, uh, [00:05:00] w regardless of the side that you're on, if you want to map out what happened, whether for purposes of prosecuting or defending a case, you first need to identify the universe of devices and data to review, which could include, you know, as you mentioned, not just the hard drive in the phones, but cloud systems and, and presumably things like, uh, ephemeral chat systems, which we can talk about as well.

Speaker 3: [00:05:30] Yeah, that's right. You think that, uh, when you, when you think of cloud systems, I'll think I'll just give a CRM system as an example, a contact resource manager, customer resource manager, um, you know, one example, Salesforce happens to be a pretty, pretty big one in the market. And I probably want to say that, uh, even if I may talk about specific systems or, or areas today, I'm not endorsing any particular products, you know, um, kind of, uh, I guess weird in that regard, I'm just giving advice [00:06:00] and ideas on things that I've seen over the years. So, but that's one example of a system where you may not have the data on premises, but there may be auditing logs and queries. You can run to get the information from those types of systems. So that may involve other things like, uh, you know, teams and slack and things that we'll talk about in terms of enterprise systems. But all of those things may be, uh, data that you may have, uh, custody or control of, but [00:06:30] not necessarily on a computer per se. Okay.

Speaker 2: So you're talking about other systems a company can be aware of, or have data on, uh, but not have actual custody over.

Speaker 3: Yeah, that's right. The was an example for Salesforce know, it's a, it's a cloud-based system where you may keep confidential information. In some cases, it may be considered trade secret dependent on your jurisdiction. [00:07:00] And so, you know, that type of information, I've seen many, a times where departing salespeople have been accused of running particular queries and downloading reports from the Salesforce

cloud system. And you, your only real, uh, evidence of that would come from getting the audit, the audit logs from the system, which become perishable after over time. So things like that is something you want to go and preserve so that they [00:07:30] don't disappear on you.

Speaker 2: And, and how does one do that?

Speaker 3: That's a great question. You know, it's funny. I actually was on a call with a client, uh, yesterday and, um, not surprisingly, they were complaining about, uh, productions. They had received from the other side, uh, because they're getting productions for multiple parties and they're all Salesforce exports, but they all look and feel different. I said, of course they do. And the reason for that is because, [00:08:00] you know, Salesforce being a database and the fact that you can set it up the way your organization wants to, you know, the, the output can look much different. So, you know, generally if you want to depends on what you really want to do, but for purposes of just, you know, showing what queries were being ran and things of that nature, you could export to an Excel file or a CSV, uh, which will kind of break the database per se, but it still gives you a report of what's going on.

Speaker 3: [00:08:30] But you know, other than that, too, you know, we, we have a lot of remote work going on these days, and I have cases where the folks will use their company computer, but then they'll also log in through something called VPN. I think mostly by now, everybody's at least have heard of the term VPN, which is virtual private network, right? And for a lot of companies, they require you to connect to your VPN before you can actually access the data. [00:09:00] But there are times when that gets overlooked. For example, somebody says, I didn't do this, or I didn't do that, but yet you go and you look at the VPN logs and it shows that the user's credentials was used and it was used from a particular IP address. And I'm sure a lot of people know that heard the term IP address, but just close.

Speaker 3: You don't technically know what that means. And how does that tie into something? IP address is think of the mail system, think of the actual mail [00:09:30] carrier, walking around house to house and drop off mail that in love that gets dropped in your mailbox as a unique address on that mail and IP address operates in the same fashion. It's an address ties back to a certain business or a certain residents that will help you prove that somebody did something from a particular physical location. So those logs are also perishable and should be grabbed as part of your investigation, if they're available and you, [00:10:00] and you believe that somebody was accessing via a VPN to do stuff.

Speaker 2: So if a company has a VPN, right, and you're right, many are using those, uh, particularly these days and the putative, uh, trade secret thief signs into the company network, through the VPN, you can look at who entered the VPN and when to [00:10:30] determine, you know, whether that person had access to the company's database.

Speaker 3: Yes. The way I actually love the way you just described that Jordan, because it's important for the listeners to understand that there are, there may be multiple pieces of the puzzle. You have to get all of those pieces to finish completing your puzzle, right? So

the way you described it, which is these are logs, that show connection [00:11:00] points, but it may not show the actual exfiltration or transfer of the data itself. It's one piece of the puzzle. There may be a next level where you go, okay, we now show they were connected. So they can't say they weren't accessing the network at that time. So that that's a, that was a very good, uh, summary by you. I liked that. And then you would take into the next steps as far as what other logs might be available or what other forensic artifacts might be available [00:11:30] to show what they were doing after they made the VPN connection.

Speaker 3: The other thing too is I've had several cases where the historical information around VPN access, if available can be important because you, you may show, for example, if they're employed to say for two years, or what have you, on your first 18 months, the VP and activity is really only occurring during normal work hours, but then the last [00:12:00] few weeks or months, or what have you, uh, there was a lot of activity after hours or on the weekends that in and of itself doesn't quote prove anything, but it's definitely, again, it's a holistic view. It's a, it's a storybook you're putting together what was going on. So that, that could be important. I am, I really

Speaker 2: Liked the reference to the puzzle because it reminds me of a lot of trade secret cases that, uh, repeat the concept that proving trade [00:12:30] secret theft is often a function of circumstantial evidence. And in these cases, you, uh, frequently don't have a smoking gun or every single piece of the puzzle. But if you've got like you suggested connection points that are, uh, suspicious because all of a sudden, uh, whereas the, uh, putative defendant might've been working for months during work hours, all of a sudden the signing on at midnight on Saturday, that's suspicious, but it's one [00:13:00] piece of the puzzle. So you talked about finding these logs and identifying these connection points. How do you get the next piece of the puzzle, which is what did he or she do when, when he, or she connected, in other words, how do you get from, okay. They were on the network to what they did, because that also is obviously an important piece. Sure.

Speaker 3: Yeah. And of course, obviously, as we're talking about this, you know, every case may be unique and you may find different pieces of different puzzles [00:13:30] based on the way the organization is set up. Right? So even though we may be talking about one specific way to piece things together here today doesn't necessarily mean it will work for every single matter, but in this case, as an example next year, and you'd be okay, you see somebody connecting through the VPN now, what are they doing? And then, and then what you start to see, if you start to see that they have the ability now to move files from the network to the computer that they're using to make [00:14:00] the VPN connection. And so you start seeing those files being moved. Let's say as an example, if the, if the company has a DLP software in place or data loss prevention software in place, or they have other auditing, that's able to show files, being transferred back to the computer.

Speaker 3: That's a step of the puzzle as well. The next thing is, if it's being moved, for example, if it's being moved from the laptop to somewhere else, [00:14:30] I it's being exfiltrated, there's, there's a, there's a finite number of ways that can be done, right. That can be done through, uh, the easiest way, I guess, nowadays is plugging USB port in and copy

things over to the USB. And to your point earlier, Jordan, you know, there's not always a smoking gun or a quote log that you plug a USB and then you copy 10 files to it. And then you just pull the USB out. You may not have a log of those 10 files [00:15:00] being copied. You know, where I hope there's no, uh, that actors listening to this podcast because I'm going to give them a little cheat here. But if you, if you love, you know, if you normally, how people get caught is they put a thumb drive in and USB drive.

Speaker 3: They copy files over, but then they want to make sure the copy was successful. The logo, and they'll poke around in the folder or they'll click on a file and open it. They'll look at it and make sure it work. That's when we get them right there [00:15:30] is because that's what leaves the markers. It'll leave a little artifact there showing that, Hey, you browse this folder on this day, while USB device was plugged in, Hey, you opened this file this day from that USB things like that is how you start piecing all this together. And conversely, if, if none of this happened, then you're a defendant and you're only Denver happened. Then you start looking at all these holistically to show. There was no evidence of this, and there's no evidence of that. And there's no inference of this. There's no inference of that.

Speaker 2: When [00:16:00] you first mentioned identifying these logs and connection points through the VPN, I heard you suggest that this is something that should be done promptly. And I, I took from that, that, that the data could be a femoral or, or deleted. What, what is the concern there is, is, is this kind of data, these logs, these connection points, are they a femoral or [00:16:30] was your, was your statement more based on a concern that the bad actor could, uh, essentially erase their tracks

Speaker 3: In terms of auditing logs? Those are generally outside the reach of the quote, bad actor, right? Unless the bad actor is the it person. We can talk. That's, that's probably a drinking story there. Cause I can tell you a lot of stories about a bad, uh, it people and what they do because they have, but let's say your average [00:17:00] employee and, and by the way, all the trade secrets for today, we're talking about generally have to do with insider threats versus hackers. I think the audience may catch onto that, but I'll just say that out loud. And so in this, in this regard, what I really mean is that is logged to become perishable. A lot of companies will, by default, you know, by nature is they won't keep logs forever. You know, and some of your third-party providers [00:17:30] won't keep logs forever. You know, there's, some can be kept for 30 days. Some might be kept for two weeks. Others could be kept for 90 days. But in my experience now, generally speaking that any type of auditing of this nature, if it's not federally regulated for retention purposes, that it can disappear fast. That's why I say go get those logs as soon as possible. Right.

Speaker 2: That makes sense. Let's talk about enterprise collaboration [00:18:00] systems like slack and teams. Uh, I assume those systems, I think you, we may have mentioned it, uh, should be considered for this type of investigation. If, if I'm right. Can you talk about why?

Speaker 3: So ironically, uh, these, these systems will allow, you know, the name is, uh, in and of collaboration allows you to collaborate. You can attach files, you can send them to

people in teams, [00:18:30] or you can send them to people in other, uh, collaboration systems. That's what they're designed for. They're designed to make your life easier. So the sharing of that information in of itself is, is, you know, normal course type stuff. But if you start seeing, uh, you know, as an example, I've had cases where there's been mass departures of employees, you know, upwards of dozens of people leaving. And there's been incidents where [00:19:00] they have, uh, done this in concert, they've discussed their resignation letters, have all been the same template. They all end up going to the same company around the same timeframe, et cetera. And the chatter that is found in these types of collaboration tools can be quite significant and important as well as the trading of files. You still have the, the problem I'll call it of if somebody [00:19:30] opens a document and they pull out their camera and they take a picture of it, whatever you have, if you don't have the camera other than the file being open. So these collaboration tools should still be considered as part of your holistic investigation in determining the level of activity, the type of activity who the people are being communicated with, whether or not files were being attached, be set back and forth. Things of that nature.

Speaker 2: If colleagues are or bad actors or whoever we're [00:20:00] talking about that that's at issue in the investigation are say chatting on, on an application like a slack or a teams or, or similar applications like zoom. You know, there's a chat on zoom and other video chat apps as well are those. So they have that conversation on these apps, they're done with the conversations, they shut the apps off, they shut down their computer and they go on with their evening [00:20:30] or whatever they're doing. Are the chat logs a femoral, or are they a preserved for some time? And does it matter or does it depend on the app?

Speaker 3: It depends always. It's a depends. So you may have organizations that have default setting to where they keep everything in finale. You may have organizations that decide, Hey, we're going to get rid of that. After a certain amount of time, [00:21:00] it's also dependent on whether or not it's a enterprise type environment, versus as you just indicated, a personally purchased licensed that's being used. So all of that comes into play. And part of that is that is part of your holistic investigation is understanding that what technology is in place, what is the settings for the technology? What logging might be in place, [00:21:30] what's the retention look like for that type of logging? All of these things are part of your investigation,

Speaker 2: Right? You know, uh, and I might date myself here, but there was a time I'd like to think not too long ago, when, when you talked about electronic communications, you're talking about emails. And of course there is a perception that you can never really delete emails. And I, you know, I even recall cases from, well, I don't [00:22:00] want to date myself too much, but years old emails that were deleted or purged or whatever. Uh, but you could retrieve them from backup tapes. Remember that? Yeah. So there's this perception that you can always find emails, even if there were deleted, but now there's this newer technology, uh, with these chat capabilities. And it's interesting that you say, uh, that the degree to which those chats are preserved or ephemeral [00:22:30] depends, uh, including on the, the company's settings. And maybe my next question also will elicit the answer. It depends, but I'm curious, are these apps I'm curious about

the default, uh, setting, uh, on these apps? Is, is it generally that let's take slack for instance, no particular reason. Is it, is it generally the case that the default setting in, uh, in, uh, an app [00:23:00] like that is you have your chat, you get out of the app and shut your computer down and it's gone, or is the default setting that it's preserved for amount of time or just again, does it just depend on each app and

Speaker 3: Yeah, I think it, it depends. I don't, if, if I don't know that there is a one size fits all quote default, per se. I know in my experience, I've seen things last [00:23:30] for a little while, but you know, it can build up, it can add up. So, uh, I honestly couldn't say that there is a single quote default, uh, safe period. I think it's, it's all based, uh, unique to that, that organization or, or individual I'm sure out of the box. There's probably, I'm sure if I were to go to their website and I see, okay, what does it look like straight out of the box if I don't make any change and I buy this [00:24:00] license here, what would my, my default setting be? And it would probably say something to that effect. And so there's because there are so many variants to that that I don't know what would be a default.

Speaker 2: Yeah, it's interesting because I would assume, uh, although I, I guess, um, bad actors are more savvy than others that, that someone with bad intent, uh, that wanted to communicate about their scheme electronically, [00:24:30] wouldn't be stupid enough to do it by email anymore. Although, as you know, there's still plenty of people who do that, but I guess the bottom line as to these chat apps is that, um, unless, you know, you, you should be careful about what you say on those apps. Uh, even though it's not email and on the other side of the coin, um, if you want to find out what, if any of those communications were in your investigation, [00:25:00] you better do it as soon as possible.

Speaker 3: Yeah. I think it's always a situation of try to do something as soon as reasonably possible again, regardless of which side you're on, if you're, if you're on, uh, you know, if you're on the defense side and you're trying to show it, nothing was done wrong. We hired 10 people and they brought nothing with them. Just go get the stuff as soon as reasonably possible. If you're the plaintiff, you want to show something was taken, it's something as reasonable as possible. [00:25:30] I always take that approach because it's so, uh, discrepant in terms of, uh, sort of different in terms of how things are available on one day and not available on a different day, even from one organization to another,

Speaker 2: What about companies, uh, that want to go beyond their networks or, or systems and, and find out what's going [00:26:00] on on social media or websites they don't control. Do you have any tips for consideration on that subject?

Speaker 3: Sure. I get asked all the time about, you know, when we're doing, uh, employee risk assessments and let's say on the, you know, on the, on the, on the plaintiff's side, if you know, some people have left and they want to do discovery, I get asked all the time, how do you do that while still protecting a person's privacy interest? And the answer is it's, it's easy. Entry is it's [00:26:30] easy. You, you, first off you're, you're aware and you're cognizant and you understand and value a person's privacy as if it were your own. And so we have experience in considering all of those things and you come up with protocols and you, you know, you work to protect the privacy, but in terms of, of getting

the data again, you know, there's different ways to get it. Uh, some, some require credential based, [00:27:00] uh, collections.

Speaker 3: Others can be publicly available yet. Others might require some sort of, uh, you know, subpoena things of that nature. But I think that in terms of getting that again, I would say that stuff is extremely, uh, volatile or perishable, you know, as you probably know, you can put a post up and you can take down, oh, Ooh, that, that, uh, that that's a celebrity tweeted that then 10 minutes later, they took it down because of all the reaction. [00:27:30] So, you know, I think that there's a, there's a healthy balance in terms of wanting to go after that stuff, at least trying to get it preserved initially right away. And then, and then getting that later, but there's always ways to consider privacy. And that's the biggest pushback that I hear whenever that topic is broached is it's privates. It's, it's sensitive. Of course it is, but that doesn't mean somebody is going to go trample all over it and look at it. It's, that's people aren't [00:28:00] really interested in that stuff.

Speaker 2: I, I assume when, when you get, uh, uh, a case and an investigation to complete, sometimes you'll get it from folks who are voluntarily turning over their devices or accesses to their systems, maybe in the context of a settlement discussion or maybe one side hires you to investigate what happened on, on their network. But there are other situations where, uh, you are getting possession [00:28:30] of or access to, uh, you know, the adversary's equipment or, or I should say the adversary of the person who hired you. Um, and that I presume would be typically more typical and in the junction type situation where a court orders, uh, the defendant to, uh, preserve, uh, his or her devices and, um, make them available for [00:29:00] forensic, uh, inspection. And of course, often those devices do include cell phones, which have a lot more information than is related to any, uh, trade secret theft or the case. And presumably a lot of private information. And I know there are protective orders in those cases that, uh, are designed to protect privacy in those situations. But what, if anything, in addition to protective orders, what kind of assurances do you [00:29:30] give in those situations to ensure that you are only looking for what, what is really needed for the case? You know, those connection points, the files that were, but not some, you know, texts between the bad actor and, uh, and her boyfriend that have nothing to do with anything in our private.

Speaker 3: Sure. A lot of times it's, it's, it's a conversation, uh, with the party, actually that's giving [00:30:00] the access. And as you, you live into, sometimes this can happen for purposes of settlement negotiations. It can happen for other reasons, you know, court order, things of that nature. Sometimes the credentials are turned over and there's a written protocol and it's, it's carried out. In other cases, uh, I find myself often offsite, I'll say to my attorney clients, if you want me to talk to the other side, let me know. [00:30:30] And I do that frequently. And I, and I described the process to them and I let them know aside from the written protocol, the man, I just grabbed the manner in which we go about our work and then the manner in which we do the examination that doesn't require us to look at the other stuff.

Speaker 3: We don't even have to look at it. We won't even know what's there per se. You know, we, if we're doing a search for a dog and there's a document on there that talks about cats, or I wouldn't even handle that [00:31:00] one, but we won't, we're not gonna look at your cats document. So that, that really comes down to just kind of helping them understand that, you know, where when we get engaged, we're even, even one more retained by one party versus another party. We're not in the middle, but we're retained by 40, we're an independent analysis shop. We, you, I don't have any interest in, uh, advocating or not a hired gun. [00:31:30] It's, I'm a, I'm a forensic, uh, independent examiner and, and, uh, reputation is what you do your work on. So it really comes down to a lot of that. It's just making. So I feel comfortable with the process and understanding it well, this

Speaker 2: Is a great discussion and what you just described as a perfect example of why I want it to have it. Because as I said at the beginning, the purpose of this podcast is to stay current on, on trade secret law, but such an important part of how to practice these [00:32:00] cases, um, is, is how to handle these, these forensic investigations and, uh, the cases and the judges just don't talk about this, these kinds of logistics at this level of detail. Uh, so this was all great to hear, and I, I feel like we could talk another half an hour, but I promise the audience that, uh, our episodes are, are about the length of a commute or a workout. And I don't want to put anybody to sleep or give them a heart attack. And my dog is starting [00:32:30] to scratch at the door. So with that said, Jim, I really appreciate this. This has been great. And, uh, I'm sure we'll be in touch soon and thank you everybody for listening.

Speaker 1: Okay. That's a wrap. Thanks for joining us on this episode of the trade secret law evolution podcast as the law evolves. So will this podcast. So we value your feedback, let us know how we can be more helpful to you. Send us your questions and comments. You can reach me by email at Grotzingerj@gtlaw.com [00:33:00] or on LinkedIn. And if you like, what you hear, please spread the word and feel free to review us. Also, please subscribe. We're on apple podcasts, Stitcher, Spotify, and other platforms. Thanks everybody. Until next time,

Speaker 4: Greenberg Traurig has more than 2000 attorneys and 39 offices in the United States, Latin America, Europe, Asia, and the middle east GT has been recognized for its philanthropic, giving diversity and innovation, and is constantly among the largest firms in the U S [00:33:30] on the law 360 400. And among the top 20 on the AmLaw global 100 content is for informational purposes only, and does not contain legal or other advice and or opinions for more information, please visit V I T period, L Y slash GT law disclosures. This podcast is eligible for California self study. CLE credit certificates of attendance will not be issued. California attorneys are responsible for self-reporting the amount of time they listened for all other jurisdictions. [00:34:00] Please contact your state's MCLE board or committee for guidance on their rules and regulations, as it relates to the self study credit.