Trade Secret Law Evolution Podcast
Greenberg Traurig, LLP
Episode 72

Speaker 1: This podcast episode reflects the opinions of the hosts and guests and not of Greenberg Traurig, LLP. This episode is presented for informational purposes only, and it is not intended to be construed or used as general legal advice nor a solicitation of any type.

Jordan Grotzinger: Emily, how are you?

Emily Livermore: I'm doing well, Jordan. Excited to be here.

Jordan Grotzinger: Good. Me too. Let's start this conversation. This is going to be a big one, AI.

Welcome to the podcast. I know we've talked about this for [00:00:30] a while. And I'm really glad you're on. Why don't you say a few words about yourself and your practice. I know this is not the interesting fact section yet.

Emily Livermore: Absolutely. I'm a litigation associate in our Los Angeles office. I'm in my second year of practice. And my practice is quite generalized. I've worked on a variety of contractual disputes, couple of trusts in estates matters, and recently I've even dipped my toe into the trade secret world on the case that we're working on together.

Jordan Grotzinger: There you go. I love [00:01:00] it. Really happy you're here. And you are, as I've said many times, one of our rising stars. Obviously, there are major intersections with trade secret law, so we want to talk about how this revolutionary technology is going to affect this space and talk about an evolution. I love that word. It's part of the title of our podcast. It's kind of a synonym for growth. And so what a perfect subject for this show.

So how is this technology going to affect trade secrets [00:01:30] and trade secret law? The answer is in a big way. And one challenge that we've got right now is going to be not speaking in platitudes. We discussed offline so many of the things that I've read or heard about AI seem to be platitudes, and I get that because everyone is literally learning as we go. So we'll try our best to be concrete, but I promise, listeners, there will be some platitudes and definitely some [00:02:00] speculation for the simple reason that this thing is evolving at lightning speed and in a way that's going to change the world. So we're all learning as we go. So let's dive in.

On December 13th, just a few days ago, I asked the following question, "How will AI affect trade secrets and trade secret law?" And here's how AI itself, through the chatbot ChatGPT, answered that question, "AI's impact on trade secrets and trade secret law is multifaceted. [00:02:30] It will create new forms of intellectual property to protect while simultaneously making it harder to safeguard against misappropriation due to increased risks of reverse engineering, automation, and global data sharing. The evolving nature of AI will likely require modifications to current trade secret laws and a rethinking of legal strategies for safeguarding proprietary information in the digital age." There's that word again, [00:03:00] evolving.

Emily Livermore: The AI answer is correct, although I think it only scratches the surface of the intersection between AI and trade secrets. Like you said, today we're going to see a human dialogue can take that a little bit further. Listeners, rest assured the rest of this discussion is not generated by AI.

But before we get too much further, let's level set by defining a trade secret. A trade secret is simply any method, process, formula or other information [00:03:30] that, one, is actually secret, two, is valuable to its owner and the owner's competitors because of its secrecy known as independent economic value, and three, subject to the owner's reasonable measures to maintain the secrecy. So that's actually secret valuable because of its secrecy and reasonable measures to maintain that secrecy.

Jordan Grotzinger: Okay. So with that definition, we can expect AI to create innumerable systems, algorithms, [00:04:00] and other material that constitute trade secrets, which raises a host of issues like who owns them and how to protect them.

What about reverse engineering? Remember, if you reverse engineer a trade secret, that is not trade secret misappropriation. And reverse engineering, of course, raises the issue of how best to protect against it, which is part of the definition of a trade secret in the first place. That is, as you mentioned, Emily, the requirement that the owner take reasonable measures [00:04:30] to maintain secrecy. There will be no shortage of trade secret issues raised by AI, so let's start with these. And yes, we plan to increasingly revisit this subject in this podcast.

Emily Livermore: I think trade secret ownership is a great place to start. Obviously this is important. The owner of the trade secret is the one withstanding to protect it. And for listeners that aren't lawyers, that means the owner is the one that can sue for misappropriation. If you're not the owner or the licensee even of the trade secret, [00:05:00] you don't have standing. You can't sue to protect that trade secret from misappropriation. So that immediately prompts some questions in my mind in the context of AI. If an internet user, for example, has a publicly available AI tool, something like ChatGPT, creates something that constitutes a trade secret, is that AI user the owner of the trade secret? Or what if hypothetically a different user inputs the same or similar requests and gets [00:05:30] the same output? Are both AI users owners of the trade secret or is it just the prior user that owns it? What is the law on trade secret ownership?

So under the Defend Trade Secrets Act, an owner of a trade secret is the person or entity with rightful legal or equitable Title II or license in the trade secret. Now, state law doesn't always define it so rigidly. Many states are just looking for some substantial interest in the trade secret, maybe an exclusive license [00:06:00] to the trade secret or even just lawful possession in some states. But regardless of how it's established, what I find really interesting about trade secret ownership is that it's not necessarily absolute or exclusive.

Another party could independently discover a trade secret and use that independent discovery to defend against a misappropriation claim brought by the prior owner. So bringing it back to AI, if a publicly available [00:06:30] AI tool is used to create a trade secret, I think there could be an increased risk of independent discovery because again, someone else could put in the same things, potentially get out the same results. And even in cases where AI isn't the creator of the trade secret, the rapid evolution of AI technology will inevitably present new avenues for independent discovery. It could make it easier to discover trade secrets, even those that aren't created by AI. And this could minimize their lifespan or even their value.

[00:07:00] Trade secrets can also be jointly owned as courts have recognized in the case of parent companies and their subsidiaries in the context of joint ventures. With that in mind, is there a world where an AI tool used to develop a trade secret or maybe the inventor or the owner of that AI tool is a joint owner with the AI user that used the AI to create a trade secret? This got me thinking about the employment context and how an employee might have a work product that they create in the course of their employment. [00:07:30] That work product belongs to the employer typically. I mean, absent an agreement to the contrary, right? Maybe we need to be thinking about incorporating similar terms to govern the work product of AI when licensing AI technology for corporate use.

Jordan Grotzinger: Those are some serious issues on a fundamental issue which is ownership, and it'll be really interesting to see where the law goes on that. And thanks for laying that out.

I do want to talk about reverse engineering for a minute. But independent discovery, so that is different [00:08:00] from reverse engineering, right?

Emily Livermore: That's right.

Jordan Grotzinger: And as I understand it, when you're talking about independent discovery, you're talking about a situation where there's two people, say, on the opposite sides of the world, one person invents something that can constitute a trade secret. The other person on the other side of the world with zero knowledge of the first person or the first person's trade secret happens to invent the same thing. That is independent discovery, right?

Emily Livermore: That's right.

Jordan Grotzinger: [00:08:30] And that's distinguished from reverse engineering, which is, "I am drinking this cola. It's so good and it makes so much money that I want to replicate the formula. I'm a chemist, or I hire a chemist and I figure out how to do it." And I do it without stealing the soda company's formula. That's reverse engineering as opposed to independent discovery, right?

Emily Livermore: Right. You're still using some part of the original owner's trade secret [00:09:00] to reach it.

Jordan Grotzinger: Got it. So reverse engineering or independently figuring out how to replicate someone else's trade secret without misappropriating it is a related issue here and one that I see is potentially existential for many trade secrets. AI is way smarter than us. And for a process method formula or system that is susceptible to AI, an AI might reverse engineer it exponentially faster than a human ever could.

So armed [00:09:30] with the genius of AI, is it just open season on trade secrets that AI can reverse engineer? My educated guess, and that's all it is at this point, obviously is probably not. There are good arguments based on current case law that using AI like a cheat code to reverse engineer might not be permissible. For example, in 2020, we discussed a case out of the 11th Circuit where the defendant took the plaintiff's insurance premium information [00:10:00] to generate quotes on the plaintiff's own website by a process called scraping. And scraping is a technique for extracting data from a website. After a bench trial, that means a trial before a judge, not a jury, in which the court found for the defendants, the Court of Appeals remanded for the trial court to consider, among other things, whether the plaintiff obtained the data by improper means, which is the definition of misappropriation, and whether the data were [00:10:30] available because they were not readily ascertainable i.e., because it was secret. Upon remand, the trial court decided that there was misappropriation.

Earlier this year in August, the 11th Circuit affirmed part of that order and the court explained quote, "Actions may be improper for trade secret purposes, even if not independently unlawful. And under the broad definition adopted in [our precedent]," and the words our precedent were in brackets there. That's not actually in the opinion, " [00:11:00] misappropriation occurs wherever a defendant acquires the secret from its owner without his permission at a time when he's taking reasonable precautions to maintain its secrecy."

The court noted, "It is important to note that scraping and related technologies may be perfectly legitimate. Much of the modern internet is built on those technologies," but the court said, "the defendants in this case did not take innocent [00:11:30] screenshots of a publicly available site. Instead, they copied the order of [the plaintiff's] copyrighted code and use that code to commit a scraping attack that acquired millions of variable dependent insurance quotes. If they had not formatted and ordered their code exactly as the plaintiff did, they would not have been able to get the millions of quotes that they got. As we explained in the previous appeal, this deceptive behavior [00:12:00] resembles the acquisition of a trade secret through surreptitious aerial photography, which we addressed in a 'prior case' in the 11th Circuit."

So you can see how this reasoning would apply to an attempted reverse engineering with AI. Despite imposing reasonable measures to maintain secrecy, someone could employ a super intelligent AI to essentially reinvent or reverse engineer something it might've taken humans years to develop. And as the 11th Circuit noted in [00:12:30] its 2020 opinion, "While some of that insurance premium data may have been accessible to humans on a website, using a bot to scrape a huge volume of data, which is not 'humanly possible'," the court said, "was akin to hacking or secret aerial photography."

So I could see a court drawing the same analogy to the use of AI to reverse engineer. So while we don't know how judges will treat AI based reverse [00:13:00] engineering, I think there are enough grounds in existing law like the improper means requirement for misappropriation and the independent economic value element, which requires the secret not to be "readily ascertainable" for judge to hold the line and not effectively let the reverse engineering exception swallow trade secret protection generally.

And ultimately, I would not be surprised if legislatures address reverse engineering to account for today's AI tools [00:13:30] and how they can threaten trade secrets. Remember, and this is one of the reasons we started this podcast and are interested in this subject, trade secrets can be company's most valuable assets, which means that if AI can open them up to wholesale attack, it's a good bet that lawmakers will come in and impose a protection if the courts don't shut it down.

Emily Livermore: Well, and of course as lawyers, we love thinking about how the law can protect against reverse engineering, but we also have to be thinking about the technological measures too. [00:14:00] Remember that the third element of a trade secret is reasonable measures to maintain secrecy. And as regular listeners will recall, this element typically can be discussed in three different categories. Actually, I just learned there was a fourth added based on a suggestion of another guest, so let's say four categories of these reasonable measures to maintain secrecy. And they are: number one, contracts and corporate policies like confidentiality agreements and asset restrictions. Number two, technology [00:14:30] like password protection, VPNs. Number three, physical protection like locks. And the fourth added category is education and training, emphasizing within the company and the importance of confidentiality of certain assets, having trainings on how to comply with the related corporate policies.

Jordan Grotzinger: With AI, of course, the tech bucket becomes even more important than it was before. But what kind of technological measures are available to protect against reverse engineering [00:15:00] by a super intelligent AI? Of course you're asking the wrong person, but I do have some ideas.

First, companies with trade secrets that are susceptible to AI reverse engineering needs to hire a new generation of talent that is AI literate and can help develop methods, if possible, to AI-proof certain reverse engineering. That sounds hard. And how could we possibly know that could work every time? The fact is we don't, but the good news is, under the law, a trade secrets owner's measures [00:15:30] to maintain secrecy don't need to be perfect. They just need to be reasonable.

But with AI, it's going to require more talent to be reasonable. And even so, we still want to make the trade secret protection as airtight as possible. A protection might be reasonable such that you're allowed to maintain a lawsuit for misappropriation. But if your secret is disclosed to the world, it's no longer a secret and all you've got is your lawsuit, obviously far from ideal.

In any event, the measures that [00:16:00] talent comes up with are above my pay grade, but I have no doubt that people smarter than me can develop solutions. Take for example, CAPTCHA technology. That's an acronym C-A-P-T-C-H-A. You know those weird squiggly lines that look like numbers and letters that you have to retype into a field to sign up for something? That's CAPTCHA, which stands for completely automated public touring tests to tell computers and humans apart. And it's used, for example, to [00:16:30] prevent bots from signing up for email accounts. If we can block bots, maybe there are ways to block AI. If you're a tech person listening to this podcast and have some ideas, please reach out. We'd love to talk to you.

And so that, my friends, is the initial conversation about AI. And as I said, we will continue this conversation as the technology develops along with the law. And we will be looking closely for cases that address how AI affects trade [00:17:00] secrets and the law on trade secrets.

And now it is time for one of my favorite sections of the podcast. I don't think we've done this for a few months for one reason or another, but that is the interesting fact that has nothing to do with the law by the new co-host. So Emily, what do you got?

Emily Livermore: All right. Well, I love to travel. I caught the travel bug very young. So young in fact that by the time I was in high school and [00:17:30] most of my friends were either going to Europe with their families or away to summer camp between the school years, I decided to go to Thailand by myself and become a certified assistant elephant trainer, a mahout.

Jordan Grotzinger: Whoa!

Emily Livermore: I went and I lived on an elephant conservation center for a week and learned elephant commands in Thai and bathed my elephant every day. And so my fun fact is that I am a certified assistant elephant trainer in Thailand.

Jordan Grotzinger: That is a [00:18:00] great one. And you might've just jumped to the top on the interesting facts. I mean, as we discussed yesterday, we've had former state troopers, we've had stock exchange workers, we've had art gallery docents. But elephant trainer in Thailand. And did you say this was right after high school?

Emily Livermore: This was in the middle of high school, I think -

Jordan Grotzinger: In the middle of high school.

Emily Livermore: Yeah, I think after that, my parents knew they were in for a wild ride with me.

Jordan Grotzinger: I know our firm, when we're recruiting [00:18:30] summer associates and young talent, we talk about 4D lawyers. That is some 4D stuff right there. That's pretty awesome. Any recent elephant training or have you not been in that space for-

Emily Livermore: No, definitely not. I enjoy admiring them from afar now.

Jordan Grotzinger: That's so great. All right. Well, what a way to end this thing. Love this episode. Love having you on.

Thank you for listening, everybody. We hope you enjoyed it. Please stay tuned. Happy holidays. Happy New Year. See you everybody [00:19:00] in January.