Host: Jordan Grotzinger:

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.

Host: Jordan Grotzinger:

Todd Pickles, how are you?

Todd Pickles:

I'm doing great, Jordan, how are you doing?

Host: Jordan Grotzinger:

I'm good. We're laughing because I'm recording in the office for the second time since the pandemic and the first time with the guest. So we were working through and laughing about some technical difficulties. In any event, you might remember my colleague, Todd Pickles, from an episode we did late last year on the China Initiative based on his expertise. And I recall it because it was one of my favorite episodes. And also my Lakers had just won the championship, which means we must have done that episode in late October or early November. And how things have changed. And Todd, you being from Sacramento, you must be at least a little happy given the history, but...

Todd Pickles:

As a Kings fan, sometimes we don't get our own wins. We take joy in the Lakers losses.

Host: Jordan Grotzinger:

There you go. Well, you got one this year. So this episode, we're going to talk about two important subjects. One is a recent decision from the United States Supreme Court about the Computer Fraud and Abuse Act, which is an act under which plaintiffs often assert claims that accompany trade secret claims. And we're also going to revisit the China Initiative and where the government is on that, given the change of administrations since we last spoke. So Todd, want to jump into the Supreme court decision?

Todd Pickles:

Yeah, there's a really recent decision just came out last Thursday. The case was United States versus Van Buren and was really the first time the Supreme Court [inaudible 00:02:08]. One of the main statutes, at least federally, that governed protection of digital information. And just by way of background CFAA was passed in the 1980s in reaction to perceive increase in hacking, primarily for government or financial institutions. Although you may remember the 1980s classic, War Games, it actually made its way into the Congressional Record. Congress talked about that as a realistic portrayal of hacking and kind of one of the reasons for CFAA. It's been expanded a lot over the years. For example, it no longer just applies to government or financial institution's computers, and now applies to computers that are engaged in interstate or foreign commerce, which as the Ninth Circuit has noted as basically any computer you're going to attach to the internet. And also now includes, in addition to the original criminal penalties, a civil right of action that you were mentioning for damages if there's been a violation of CFAA.

Host: Jordan Grotzinger:

And we're certainly dating ourselves by referring to War Games, and I'm sure our younger listeners have no idea what that is, but I do remember that movie. It was with the kid with the DOS looking computer. It was even pre MS DOS, I believe, but yeah, I guess we're old.

Host: Jordan Grotzinger:

So CFAA as people abbreviate it, prohibited unauthorized access of a computer, that is traditional outside hacking, as well as situations where an individual "exceeds authorized access" of a computer to obtain information. And the phrase "exceed authorized access" is further defined in the statute as "to access a computer with authorization and to use such access, to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter".

Host: Jordan Grotzinger:

The Federal Circuit Courts of Appeal have been split on exactly what that definition meant. Some, like the Ninth Circuit, held that it only applied when a person didn't have authorization to access the particular information, but other Circuits have held that CFAA covered situations where individuals misused the access they had for an unauthorized purpose. So the Supreme Court took up the case to resolve the dispute and clarify the reach of this act.

Todd Pickles:

Exactly. And it ended up that the case they used was the Van Buren case and the facts are somewhat interesting that led to the prosecution of Mr. Van Buren. He was a police Sergeant in Georgia and he was interacting with this guy named Andrew Albi. The way that the Supreme Court decision describes Mr. Albi is he was volatile and the folks in the precinct had been warned not to deal with him. Nonetheless Mr. Van Buren befriended Mr. Albi and, at least according to Mr. Albo's account, tried to shake him down. In fact, I saw one reference to the underlying case that Mr. Albi confessed to his priest about the situation and the priest said "Hey, you need to, you need to do something about it".

Todd Pickles:

Regardless of how it kind of really worked out, FBI begins an investigation of Van Buren to see if he's involved in political corruption and they set up a sting where Albi acting as an informant, goes to Van Buren and says "Hey, I met this woman at exotic club. I think she might be law enforcement, but I want to make sure she's not, I've got her license plate. Can you go ahead and run the plate? I can figure out if she's law enforcement and I'll pay you five grand."

Todd Pickles:

Van Buren agrees and the way it works out thereafter, Albo pays Van Buren a thousand bucks. Van Buren goes onto his police computer, searches up the dummy information that FBI had put in there. And with that Van Buren is arrested and he's charged with, among other things, a violation of CFAA on the theory that he exceeded authorization when he went and looked up this information on the police computer, to which he wasn't entitled; at least for that purpose.

Host: Jordan Grotzinger:

So he basically set out to do something which clearly isn't kosher as a police officer. He's prosecuted and he's convicted and sentenced to 18 months in federal prison. He appealed to the 11th Circuit Court of Appeal, which upheld his conviction under CFAA, finding that his conduct of accessing the computer for

financial gain exceeded authorization for public officials. So the Supreme Court takes up the case and in a 6-3 decision held that the phrase "exceeds unauthorized access" only "covers those who obtain information from particular areas in the computer, such as files, folders, or databases to which their computer access does not extend". However, "CFAA does not cover those who ... have improper motives for obtaining information that's otherwise available to them." And Justice Barrett wrote the majority opinion and noted that there was an agreement between the parties that "Van Buren access to computer with authorization when he used his patrol car computer and valid credentials to log into the law enforcement database", and "that Van Buren obtained information in the computer when he acquired the license plate record" for the benefit of the informant.

Host: Jordan Grotzinger:

Thus, the dispute for the court to resolve was "whether Van Buren was entitled so to obtain the record".

Todd Pickles:

Exactly, and so that's where the court's focus is and the opinion. I think we can skip over the details of the court debating what the word "so" meant in that phrase "entitled so to obtain". A lot of the opinion goes into statutory interpretation and, for example, does that word get rendered superfluous by the court's analysis? The bottom line is the court rejected the government's proposed interpretation of CFAA. At least this exceeds authorized access prom. And specifically the government had been advocating that capital would be implicated when someone accesses information one was not allowed to obtain in the particular manner or circumstances in which he obtained it. The court went through the real world problem with the government's proposed interpretation, as Justice Barrett noted, that everyone uses work computers. Work computers have restrictions on what you're supposed to do with your computer.

Todd Pickles:

Typically you're only supposed to use them for business purposes. In reality, people send emails, they check news articles while they're at work. And, at least according to Justice Barrett, under the government's interpretation, that would be a violation of CFAA because under those circumstances, the employee would not be using their work computer in a manner entitled. The majority also noted in addition to the work setting that people often will visit websites, where there may be a term of use restriction that you have to agree to, to click the box, when you access a website or an app on your phone. The court stated, and this is directly from the opinion "if the exceeds authorized access clause encompasses violation of circumstance based access restrictions on employers computers, it is difficult to see why it would not also encompass violations of such restrictions on website provider's computers". And so Justice Barrett summed up kind of the problem with the government's broad interpretation is that under its interpretation, CFAA would criminalize "everything from embellishing an online dating profile to using a pseudonym on Facebook and when to reach 'checking sports scores or paying bills at work'".

Host: Jordan Grotzinger:

So just for the record, you don't, you don't check news articles or send personal emails from our GT system. Do you?

Todd Pickles:

Of course not. I would never violate the office restrictions in that way.

Host: Jordan Grotzinger:

Right. Good to hear. So instead of the government's interpretation, the majority found that the 'exceeds authorized access' prong of CFAA refers to "information that a person is not entitled to obtain by using a computer that he is authorized to access". And the court described these people as "inside hackers who access a computer with permission, but then exceed the parameters of authorized access by entering an area of the computer to which that authorization does not extend." So that was the court's conclusion. And we're going to do two sets of takeaways in this episode; The first on this Van Buren case. Takeaway number one is, as I mentioned in the past, CFAA claims could be considered alongside trade secret claims and had the benefit of not requiring the data accessed to rise to the level of trade secret status, although with more limited damages under CFAA, in situations where someone was authorized to access a company's data, but used it for an improper purpose. Thus, you could bolster a trade secret claim with one under CFAA that didn't require all the data to be a trade secret as you must in asserting a trade secret claim.

Todd Pickles:

Exactly. And then, so then the second takeaway is that after Van Buren, the range of CFAA is going to be much more limited and really you're just going to be situations of either outside hacking or the inside hacking type situation that the court explained, where you have authorization to a computer, but not to the file and then that's the file that you're accessing.

Host: Jordan Grotzinger:

Takeaway three is on the flip side, the Supreme Court has made clear that using a credential to get access to data that an employee is otherwise not authorized to access squarely falls under CFAA. So those "inside hacker cases" remain fair game and can be considered alongside potential trade secret claims.

Todd Pickles:

Right. And so what that means is after Van Buren, the fourth takeaway I would suggest is that when you have ... in the past, you may have considered CFAA, as you mentioned. Now, it might be that a trade secret analysis is really the main way you're going to police situations. It's on accessing files that they're entitled to access. And so really the investigation is going to be about whether or not it's a trade secret, in addition to considering common law claims of a breach of fiduciary duty, or maybe breach of contract with a confidentiality agreement, all those are going to be much more limited by the facts and circumstances.

Host: Jordan Grotzinger:

And the fifth and last takeaway is that evidence of the hacking itself, for example, entering a restricted database, overcoming encryption or firewalls, et cetera, might aid in establishing evidence of the reasonable steps taken to protect data and thus support a trade secret claim, which as our listeners know, requires, among other things, that the claimant took reasonable measures to protect the secrecy of its information.

Host: Jordan Grotzinger:

Okay. Let's pivot to the China Initiative and Todd, why don't you kick that off since you're you're the China Initiative expert?

Todd Pickles:

Well, I don't know about that, but I'll be happy to kind of remind folks of what we had talked about when we were last here, back when your Lakers were still gloriously triumphant. We had talked about how back in 2018, the Trump administration announced that as part of official DOJ policy they're instituting something called the China Initiative. And that was meant to "identify priority Chinese trade theft cases, ensure that we have enough resources dedicated to them, and make sure that we bring them to an appropriate conclusion quickly and effectively". Since that, we had noted in our past podcast, there've been a number of defendants charged federally with alleged trade secret theft for the benefit of Chinese or Taiwanese companies, including oftentimes state-owned companies. And these prosecutions were happening all over the United States' weren't just limited to the coasts. And it turns out the China Initiative is still a thing.

Host: Jordan Grotzinger:

Yes, it is alive and well in the Biden administration. And the Department of Justice has maintained information about the Initiative on its website and continues to be run under the National Security Division under the helm of Assistant Attorney General, John Demers, who is a holdover from the Trump administration. Also there have continued to be prosecutions of alleged trade secret theft from US companies by individuals or entities believe to receive support from the Chinese government. And these include an indictment in February of this year of a Chinese national allegedly conspiring to steal trade secrets from a prominent American manufacturer regarding the company's Silicon Carbonate technology, which was filed in New York. And in April of this year, the department also obtained a conviction of a Tennessee man for conspiracy to steal trade secrets, economic espionage, and wire fraud after a 12 day jury trial. Also that month in April an Ohio man was sentenced to 33 months in prison for conspiring to steal exosome - am I pronouncing that correctly?

Todd Pickles:

As far as I know you are.

Host: Jordan Grotzinger:

Okay, good.

Host: Jordan Grotzinger:

- exosome related trade secrets concerning the research, identification, and treatment of a range of pediatric medical condition. And his wife was sentenced to 30 months in February as part of the same scheme. So the DOJ continues to be very active in criminal prosecutions of trade secret theft relating to China.

Todd Pickles:

Exactly. And I note that in many of these situations, you actually had press releases issued by the Assistant Attorney General, indicating this as a matter of policy, these aren't local prosecutions only. And then you're seeing these continuing prosecutions by DOJ at the same time that Congress remains very active in the same area of trying to protect trade secrets.

Todd Pickles:

With respect to China, the Senate, I believe today potentially is poised to pass bipartisan legislation that would, among other things, require the state department with the assistance of other departments, such as DOJ to develop a list of Chinese owned enterprises that have benefited from intellectual property theft or coerce transfer of intellectual property by the Chinese government. I know you just had a podcast, I think last week, -

Host: Jordan Grotzinger:

Last month.

Todd Pickles:

- about our last episode about the Protecting Intellectual Property Act of 2021 that has similar focus of protecting intellectual property and in connection with China. So you put these things together, you have the political winds that are aligned with DOJ, continuing to focus on China. I think that means you're going to continue to see these type of criminal prosecutions where there's purported trade secret theft that relates to a Chinese owned company or to the Chinese government itself.

Host: Jordan Grotzinger:

Two takeaways from the latest on the China Initiative. One is that perceived victims of trade secrets theft involving China might consider contacting law enforcement, which might be now a receptive audience for investigating and prosecuting what traditionally has been left to civil litigation.

Todd Pickles:

Exactly. And then the second piece is obviously the flip side of that. If you're the recipient of an accusation of trade secret theft via the letter, or it's already reached the stage of a formal complaint filed in civil court, that doesn't mean you're out of the water when it comes to potential criminal exposure. You still want to consider the fact that there could be a criminal investigation and then even later prosecution of what otherwise seems to be a civil litigation accusation of trade secret theft.

Host: Jordan Grotzinger:

Okay. Well that concludes our discussion and this episode. Todd it's always a pleasure to do these with you. I hope to do it again soon. And remind me, when was the last time the Sacramento Kings were in the playoffs? Sorry, you took that dig in the middle of the episode and I couldn't resist. Terrible, terrible, terrible. All right, my friend.

Todd Pickles:

It hasn't been as long as we're working, so let's put it --

Host: Jordan Grotzinger:

Yeah. Okay. Fair enough. All right. Well have, have a good one and forward to seeing you soon.

Todd Pickles:

Same here. Thanks. All right.

Host: Jordan Grotzinger:

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 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 US on the Law360 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 E I T period, L Y slash GT law disclosures. This podcast is eligible for California self study CLE credit. Certificate of attendance will not be issued. California attorneys are responsible for self reporting the amount of time they listened. For all other jurisdictions, please contact your state's MCLE board or committee for guidance on their rules and regulations as it relates to the self study credit.