Podcast Transcript

Alternatives to Noncompetes: Intellectual Property Alternatives to Noncompetes

Date: December 5, 2023

Guest: John Siegal, Joyce Ackerbaum Cox, Lisa Collins, Christina Moser, **Host:** Leeann Lee

Run Time: 36:35

For questions and comments contact:

John Siegal

Partner
New York
T: +1.212.589.4245 | jsiegal@bakerlaw.com

Joyce Ackerbaum Cox

Partner
Orlando
T: +1.407.649.4077 | jacox@bakerlaw.com

Lisa Collins

Partner
Atlanta
T: +1.404.256.8231 | LNCollins@bakerlaw.com

Christina Moser

Partner
Cleveland
T: +1.216.861.7818 | cmoser@bakerlaw.com

Lee: The use of noncompetes is now shifting across the country. Many states are limiting the use of noncompetes. Several states have enacted or are considering prohibitions on noncompetes. Nationally, the Federal Trade Commission is engaging in a rulemaking that could ban noncompete agreements between employers and employees. What does all of this mean for your business? Are there alternatives to noncompetes that can protect your business? To help bring all of this into focus, we've created a three-part series called Alternatives to Noncompetes. I'm Leeann Lee, and you're listening to BakerHosts.

Our third and final episode, Intellectual Property Alternatives to Noncompetes, dives into specific intellectual property tools and approaches that can serve as alternatives to noncompetes. Our guests today are Joyce Ackerbaum Cox and John Siegal, co-leaders of BakerHostetler's Noncompete and Trade Secrets team, and intellectual property partners Lisa Collins and Christina Moser. Let's listen in.

Siegal: Thank you for joining us today for the third and final installment of our three-part series, Alternatives to Noncompetes. My name is John Siegal, and I'm hosting this together with Joyce Ackerbaum Cox. We're the co-heads of BakerHostetler's national Noncompete and Trade Secrets Practice Group, with lawyers who do this work located in 16 offices from New York to L.A., Orlando and Atlanta, to Seattle and San Francisco.

Today, we're going to discuss intellectual property alternatives to noncompetes. Our panelists are Lisa Collins, the leader of BakerHostetler's Atlanta Intellectual Property practice, and Christina Moser, a Cleveland-based Intellectual Property partner. Joyce, why don't you kick things off?

Cox: Thank you, John, and we are very happy to have Lisa Collins and Christina Moser here with us to answer some questions. I'll start with you, Lisa. As an IP practitioner, what framework do you employ when drafting NDAs or confidentiality agreements from a transactional perspective?

Collins: Thank you, Joyce. So, I'll answer this from a transactional perspective, and then I'll flip it to Christina to answer from a litigation perspective.

So, from an IP perspective, you want to make sure you understand the scope and purpose of the agreements. So with that, you want to make sure you understand what is confidential, what is trade secret, and what is proprietary information, and you want to define these terms. So within your NDAs or confidentiality agreements, you want to make sure that all three of those terms are defined. You also want to make sure you define who has access to the information and for what permitted purpose, and so you put that clearly within your agreements so everybody knows kind of what the definitions are of the terms and how you can access them and how you're permitted to use them.

You also want to define limited disclosure, when it is permissible in some instances, and how it is permissible. So for an example, let's say you are creating a product and you have to work with a manufacturing company to create that product. So in the NDA with them, you want to make sure you're very clear on the permitted use that they can have to your trade secrets or confidential information to create that product for you.

From an IP perspective, sometimes you'll have a joint venture or you'll have a collaboration with others, and you want to make sure that ownership is clearly defined because that is something that is very important from the IP perspective. So, you want to make sure who owns the trade secret and which trade secret is owned by which part of the collaboration, who has access to the trade secrets or confidential information. And additionally, if something is created from it like a derivative work, you want to make sure that you also understand who has ownership and access and use of that derivative work, and how that derivative work can be used.

You want to make sure you understand the end goal of the collaboration and the joint venture, how confidential information is handled. Is it going to be in perpetuity, like forever? Or essentially, would it be when the joint venture is over? And sometimes, you have to have it in one versus the other, and you want to make sure that you've thought of those scenarios, because sometimes there could be changing circumstances which you would need to disclose a trade secret which is no longer a trade secret. In essence, if it's become an industry norm. But you want to make sure that you have that documented properly.

Thirdly, you want to examine the appropriate standard of care with trade secrets or highly confidential information. They should always be at a heightened standard and one no less than that you would hold the documentation and the information within your company, but you still want to make sure it is at least at a heightened standard that you have. You want to be clear to review the representations and warranties and ensure that they're right sized. So not all deals are the same, and so you want to make sure that they're right size and fit for this appropriate instance. You want to look at the notice language within the contract and you want to pay attention to the DTSA, and so make sure that you know whether or not you need to include the whistleblower retaliation claimant protections within your non-disclosure or confidentiality agreements. You want to create protocols to comply with non-disclosure and confidentiality agreements if you don't have them. And if you do have them, you want to make sure that you're enforcing them and that there are appropriate measures being in place.

You should consider establishing an identification process so that you can flag in advance any particular trade secrets that are very highly confidential. And these are the ones that if they're accessed, they have unauthorized access to them, they might require a seizure order. And so those you want to make sure you flag so that it is easier from a litigation standpoint, as Christina will talk about in a minute, that you're aware of those in advance. You want to make sure you have procedures in place and within your agreements to handle breaches. If there is any breaches of the confidential information, if it is disclosed, if there is an unauthorized disclosure, you want to understand how to handle that. And not all disclosures are the same, so if it is an internal disclosure where somebody that had access to it is an employee of the company but it stayed within it, it was just a breach because they shouldn't have accessed it, it is different than if it is disseminated to the public. And so you want to make sure that you have different scenarios.

And then lastly, if you're in a company where international theft is a concern, you want to be sure that you monitor the biannual reports from the attorney general of Congress and the recommendations and educational materials that are generated from that process. And the reason you want to do that is because you want to make sure that you evaluate the reporting options that your company can pursue based on the industry that they're in. And also, that your company is appropriately represented in any future congressional evaluations and developments on the issue. So now, I'll turn it over to Christina to talk about from a litigation standpoint.

Moser: Thank you, Lisa. And from a litigation standpoint, while a run of the mill kind of one size fits all non-disclosure agreement is better than nothing, it is not optimal when it comes to litigation for several reasons that companies sometimes find out when they're well into litigation. One of the first things that companies need to consider is their jurisdiction. So, while the federal Defend Trade Secrets Act is federal in scope, each state has their own interpretation of it based on the cumulative effect of their trade secret law to that point, and so that provides a framework through which they're interpreting the federal act. And some of the states have a lot more leeway in terms of how they allow things like misappropriation of trade secrets to be alleged.

So, for example, some states have stronger inevitable disclosure doctrines, and some states don't recognize it at all. So, it is important to know which state your agreement is likely to be litigated in and identify those likely, the place of incorporation for the parties, the principal place of business for the parties, where, if it is a joint development, any work is going to be carried out. Those are the most likely for consideration of these types of disputes, and in choosing one of those based on how favorable it is to protecting your trade secrets is a good idea ahead of time. And that way you can also minimize any future debates over jurisdiction or venue by having an exclusive jurisdiction or venue clause choosing that jurisdiction. And there are other procedural advantages and substantive advantages depending on where you are. So, keeping the location and the choice of law and venue in mind is important.

Also, some states I mentioned the differences between the states. Some states treat nondisclosure agreements as restrictive covenants, so noncompetes aren't the only restrictive covenant out there. A lot of courts will look at nondisclosure agreements through the same lens. And so, if your language is really broad and the court finds that it is too broad, then you run the risk of some courts holding it to be unenforceable. So, one of the things that you should consider in drafting a nondisclosure agreement is including a detailed severability clause so that if one portion of the agreement is held to be unenforceable, the court has the power granted by the parties to rewrite the agreement. Many states will do that anyway. They will rewrite an agreement to make it enforceable, to lessen the scope of it, to make it more specific. But some courts do not, and so if you're in one of those jurisdictions or you might be in one of those jurisdictions, it is important to pay attention to protecting yourself ahead of time by getting that detailed separability clause in place.

And based on the nature of the agreement, you might want to consider going into more detail than you ordinarily might in terms of defining the trade secret and the types of information. So for example, if you're in a jurisdiction that doesn't enforce noncompetes, one potential way of addressing that is to identify customer information as something that is protectable, and not just customer information but specific types of customer information. So, a customer or subscriber or client ordering history and preferences, the vendor or supplier or reseller pricing or customization capability, all of those are more specific and are more likely to be held to not be overbroad if they come before a court.

And another important consideration is how the information is likely to be shared between two parties. Is it going to be via email? Is it going to be in person? Are there going to be hard copies or is everything going to be electronic? And then develop methods in the agreement for addressing those specific modes of communication so that there is less confusion later on, on whether or not a disclosure was permitted and making sure that at the conclusion of their relationship, the information can be disposed of.

And finally, one of the additional clauses that you could consider is, in addition to having your specific trade secrets that you anticipate exchanging identified in the agreement, include also a savings clause for disclosures that might not be marked but are of a specific type that parties ordinarily would recognize to be confidential information. And also keep in mind that when you're drafting a nondisclosure agreement, there is a potential in third-party litigation that information regarding that other party needs to be released. So the more specific you are about what type of information is actually covered by a nondisclosure agreement, the better off you'll be down the line if you're called to produce information about that customer or that business relationship in litigation involving a third party. And specifically, what notice requirements there are.

Cox: Great, thank you. Lisa, I'm going to ask you another question because we're trying to give folks some tools in terms of protecting their trade secrets from the outset. What can you tell us about trade secrets protection plans or protection programs that companies can put in place? And maybe you can highlight some of the key things you see that companies typically forget?

Collins: Okay, so I think there is generally five general guidelines for a good trade secrets protection program, so I'll go over each one of those. So the first one, audit, audit, audit. So, you want to make sure that you have an initial audit of your trade secrets and that you routinely conduct an audit and that you consistently enforce any policies you have. It is very important that you know what you have as a trade secret. So that is the importance of the initial audit essentially, so that you can understand exactly what you have as trade secret, confidential, and proprietary information. And the reason you want to make sure you routinely conduct it is to make sure that it is still maintained and also that the same things that you had previously are still a trade secret.

And when you're doing this audit, some of the things that you want to consider are what measures do you have in place to secure the trade secrets. You always want to make sure that the measures you have in place are in industry standards and best in practice. You want to also make sure that you're utilizing these measures. So, sometimes people have things that they can do to protect their trade secrets, but then they don't do it, so you want to make sure that you actually are utilizing these measures and keep abreast of standards.

If you have a compliance program, you want to make sure that you consistently review it and enforce it in relationship to your trade secrets. If you do not have a compliance program, you could consider developing one, because you want to make sure that you have the policy in place that individuals know how to maintain your trade secrets and that they are enforcing it appropriately.

The second thing you want to make sure you do is that you have the right agreements in place, and so you want to think of having a non-disclosure agreements. All employees should sign an agreement that requires them to keep the company's proprietary information, trade secret information confidential, and this agreement should not be in like a handbook. It should not be buried in a document that people may or may not read. It should be a standalone document that you have, and so you want to make sure that you have that and that you have the employees execute it. Christina talked a little briefly about noncompete and non-solicitation agreements for key employees and jurisdictions in which they're still allowed to have them. You want to make sure that you have those and that you want to make sure that you know the proprietary information that they are allowed to access, and then the permitted use that they have, but that they're aware that they can't compete with this information or solicit with it. And John will speak on this a little bit later as well when he talks more in detail about noncompetes.

And another document that people sometimes don't have but they should, is a trade secrets policy and restricted access policies. So, you want to make sure that you have written policies in place that specifically and in detail, describe what is a trade secret. Not necessarily your trade secrets, because those you want to keep secure, but just what it is, what is proprietary information, how should they be accessible? And so, employees that need to know this from a need-to-know basis and for their permitted usage, they understand what the policy is and what the restrictions and so forth are.

The third thing that you want to do is have employee training, so you want to make sure that your employees know how to handle your proprietary information. And a trade secret policy is really only as effective as the employees that know about the policy and the supervisors or managers who know how to administer the policy appropriately. So, you want to teach the supervisors and managers about their roles and responsibilities relating to trade secrets and company confidential information, and you want to educate the employees about that as well. And then you want to remind them, I would recommend annually, at least reminding them.

The more specific and consistently apply the policy, the easier it is for employees and everybody to apply. Think of it like your cybersecurity policy, like most companies have to do yearly now, and so you can institute this as part of that yearly procedure and then have them do like a quiz after to make sure that people are aware of these policies, and they know how to enforce them and protect them. And for an example of this, the importance of this, an employee could post like a social media post about just a routine thing that the employee has done that day and that could inadvertently disclose sensitive information from the company. So, you want to make sure that this doesn't happen, so the employees know that this is something they shouldn't be doing.

The fourth thing you want to think of is your IT, right? So, you want to make sure that you have the necessary IT infrastructure to protect your proprietary information in place. You want to make sure that you have software installed that monitors sensitive information and that provides alerts to improper disclosure of that information. You want to make sure you have the ability to remote wipe and remote lock any capabilities within the system so that if something happens, if there's a breach, you can address it pretty immediately and effectively.

If you're a company where employees are allowed to bring their own device or have their personal devices that they can use for company related business, you want to make sure that if it is not synced to the company's network, that it has to be accessible to the company. And you will need a document for that, essentially where the individual employee is signing off, allowing you to be able to access their device if they want to use it for company business. Or you could install software on the employee's personal device to allow them to use it for company business, or otherwise they shouldn't be allowed to use it. You want to monitor and manage any downloads and uploads of information, especially your trade secrets and proprietary confidential information. You want to limit use of portable storage devices, and then you want to track utilization of employees for utilizing this information to make sure it is authorized access and it is just for the permitted purpose. And you especially want to do this with any outgoing employees.

And so the fifth step is you want to have a detailed employee exit plan strategy. So, companies should be conducting exit interviews of all their employees and you should use part of the exit interviews to talk about the trade secrets and the confidential information and making sure that the departing employee is aware of their obligations with respect to those. You could also use this as an opportunity to understand where the employee is going next and if they're going to a competitor. And say they're in the sales department within your business and they're going that to a competitor, you want to make sure with heightened awareness what they are and are not taking with them, and to pay attention to that. And so these are just some of the steps that you can take to establish a successful trade secret program.

Siegal: So, we're moving towards a discussion at the end here about trade secrets in litigation as an alternative, sort of ultimate fall back alternative to noncompete. And Christina, if the measures that Lisa has outlined aren't in place or there is some other problem and you're in a situation where a client is headed towards litigation or thinks there may be litigation, what are the measures you recommend to protect the company's trade secrets in that process?

Moser: So, the first step is to preserve. If you have an employee going to a competitor, preserve their electronic device and the metadata associated with it that will show what they accessed, when, and what they did with it, if it was exported or printed or anything like that. Also, when litigation is on the horizon, some of the issues we discussed earlier come into play. For example, having an exclusive jurisdiction or venue clause. But in the absence of that clause, choosing the most favorable jurisdiction in venue and being able to defend that choice is critical.

As mentioned, states have different approaches to inevitable disclosure, also to what reasonable measures are in order to protect your trade secrets and maintain protection of the trade secret. It is also important, and if you've already done the audit that Lisa talked about, you would have this, but it is important to be able to articulate what your trade secrets are, because if you get involved in litigation, you're going to have to disclose them. First of all, have a public viewable version of your trade secret, a way in which to describe it that is suitable for public consumption.

And then, you'll also need to have a confidential version of what that trade secret is in order to be able to conduct discovery. Some states have early disclosure requirements where prior to discovery, a party has to identify with specificity what their trade secret is. So, having that description before you file is important. Also, do your diligence. Make sure that the information has a history of being protected and is not readily publicly ascertainable. If so, then a lot of trade secret statutes have an attorneys fees provision. So if you bring a misappropriation claim and the court finds that it wasn't well founded from the beginning, then that could open you up to attorneys fees and costs.

One other thing is that you want to take any opportunity that you can to notify relevant third parties that might have metadata that is relevant to prove access or transmission of trade secrets like communication platforms of the pending litigation for preservation purposes, and then subpoena those records and get them as soon as possible. You'll also want to, and this is probably further up on the list after you make sure everything's preserved, to provide notice to any new employer of the unauthorized disclosure, or if it's a former business relationship, notify your former business partner of what you believe to be the unauthorized disclosure. And what this does is kind of puts a place holder in time beyond which the other party can't say, well, we weren't aware that the disclosure was unauthorized. You're putting them on notice that it is unauthorized.

And finally, before you get into litigation, it is important that you understand the potentially broad scope of discovery that you as a trade secret holder will have to engage in, because you're having to prove, first of all, what your trade secret is. And then second, that it hasn't been publicly disclosed and that it's been appropriately protected, and so that can lead to fairly wide-ranging discovery requests and response obligations.

Siegal: So thank you for that. Now we're going to talk a little bit about trade secrets litigation and whether and to what extent it really is an alternative to noncompete, because the movement toward reducing or eliminating the role of noncompetes and regulating the market for employment has been premised on the idea that trade secrets litigation is a viable and efficacious alternative. This whole thing started basically in 2016 with the adoption of the Defend Trade Secrets Act overwhelmingly passed by Congress in the fall of 2016, perhaps the last genuinely nonpartisan consensus legislation, maybe in American history, the way it seems.

But parallel with that congressional action, was a White House and treasury effort through policy papers, white papers, advocating for states to cut back or eliminate the use of noncompetes. And the idea was, we have federal protection for trade secrets, so why do we need noncompetes now? And the entire body of academic research comparing the California example where noncompetes are banned with other states is likewise premised on the idea that trade secrets litigation is a viable alternative to noncompetes. The FTC's proposed rule says so expressly. So, to see the impact of the scaling back or prohibition of noncompetes on trade secret litigation, I think it, we have to take a step back and just revisit the basics of noncompetes, right? Their restraints on trade, restraints on the employment market measured under a rule of reason.

And in every state, in every jurisdiction, to enforce a noncompete the party seeking to enforce has to establish that it has a legitimate protectable interest that deserves protection through the restrictive covenant. There are five or six such, and I think we need to talk about each in terms of what will happen with trade secrets litigation if and when noncompetes and other restrictive covenants disappear or are limited in your jurisdiction. So, the protectable interests are trade secrets, confidential, proprietary information that does not rise to the level of a trade secret, customer relationships, employee relationships often described in some jurisdictions as goodwill, and then the amorphous concept in some jurisdictions of unique employees. So, is trade secrets litigation an alternative to protecting these interests?

Let's start with protecting trade secrets. It is not as obvious as it sounds. If you look at California, there is certainly more trade secrets litigation. But is that because of the prevalence of the technology industry there? Is that because of the legal prohibition against noncompete and non-solicitation provisions, or both? Hard to say. Certainly one thing we could say definitely looking at California and looking at other states where noncompetes get limited or nationally if it happens, is far more of this litigation goes to federal court now because of the DTSA. But there are other unintended consequences. For instance, California is where the Justice Department crackdown on no hire agreements between competitors began as well, so that too may be an ancillary consequence of the elimination of noncompetes.

Is it harder to protect trade secrets when there is no noncompete? Theoretically it ought to be the same, right? It is the same injunction standards. Is there a likelihood of success of establishing that there is a trade secret? Is there irreparable injury absent an injunction? What is the balance of equities or public interest? But the reality, I think, is that noncompetes are an interim quicker solution that gives a court another likelihood of success, not just is there a trade secret, but is there a breach of the noncompete contract?

So, is there a higher bar for a trade secrets injunction than a noncompete injunction that is based on protecting trade secrets? I would say yes, at least when the trade secrets involved are not technology based. Now, Lisa alluded to this in her drafting guidelines. What are non-technology, non-trade secrets that are protected by noncompetes and other restrictive covenants? I think if we were all in a room and everybody who practices in this area, we could have a great theological discussion about whether there actually is confidential, proprietary, non-trade secret information.

One thing is for sure, is that you need to think very specifically about that with respect to your business, and we'd be glad to discuss that with you, because if you can't protect it as a trade secret, you have to have a very clear and specific showing that it is a confidential, proprietary information and that deserves another form of protection. But absent restrictive covenants, you're going to have to get to the trade secret level.

Now, customer relationships, customer lists, sure. There are times when those rise to the level of a trade secret. You can bring a trade secrets litigation claim to protect a stolen customer list in the old days. Perhaps sometimes we've all tried it, bringing claims based on contract terms or customer preferences or other insider knowledge of the customer relationship, but those have always been hard. There's always been the defense that customers are perfectly able to disclose the competitors their preferences or their contract terms. So, is that really a trade secret?

But what about the relationships themselves? So much of restrictive covenant practice and the use of restrictive covenants is for the protection of relationships. Look, go industry by industry. Private banking and securities brokering, investment banking, professional services and consulting, insurance brokerage, real estate brokerage, physicians, the doctor-patient relations, these are the industries other than technology that have the most noncompete and restrictive covenant litigation. And absent noncompetes and restrictive covenants, it's going to be the rare exception that those types of relationships are protectable as trade secrets.

Employee relationships, even harder. So, how do you guard against lift outs without restrictive covenants? That is going to be a super huge change in HR and in the way that companies approach these issues. I think it is fair to say that in the absence of restrictive covenants or the, as they become harder to enforce, people-based protections in relationship businesses are far more at risk. And that's why we've done this series, and that is where this discussion comes into play. That is where the tools we discussed in this series need to take a far higher priority in your employment, intellectual property, litigation prevention practices, garden leave, other provisions to protect the business during transitions to make sure you transition the role and you have time to do it.

Employee benefit and compensation tools that we discussed last week, non-solicitation agreements where permitted, but they are decreasing in efficacy everywhere, and obviously, as Lisa and Christine have outlined today, a real deep focus on trade secrets protection programs. In the end, I think you're going to have to be prepared for harder litigation decisions if the decision is trade secret litigation versus noncompete or restrictive covenant litigation.

Whether to bring a trade secret claim at all is often a harder decision. As Christina pointed out, there are attorneys fees provisions, et cetera. You have to be prepared to pay the expense if you're going to bring a trade secret litigation. They are far costlier in the long run, in general, than restrictive covenant litigation. The commitment to litigation in a trade secret claim has a longer time frame, often than in a restrictive covenant litigation, and I'm certain that as this process plays out, there will be more damages litigation than there was noncompete and restrictive covenant litigation that is so often ended at the TRO and preliminary injunction phase.

So, with that outline of the difficulties that we're all facing as we seek alternatives to noncompetes, Joyce, I turn it back to you to close out the session in the series.

Cox: Thank you John, and thank you, Lisa and Christine. I think that the information you provided here is really helpful. I think that from my personal experience, I've really seen clients struggle with the front end on the preventative items audits and having those preventative measures in place which are going to be critical, and I couldn't agree more that we're going to see the most difficult aspect of this in the employee protection sales and other types of jobs and industries where customers are particularly involved. But stay tuned. We are staying abreast of all these issues and will continue to bring them to you.

We hope you found this series informative. As you've seen, we've got lawyers who specialized in this area. In the IP employee benefits employment, commercial litigation areas in all of our offices, we've brought you a little bit of a representation of each of those or some of those folks. To the extent you have any questions, please feel free to reach out to any of us or of course to John or I, and we can always direct you to the appropriate person within our group or our team or for the state you may have an issue, and we hope that you all enjoyed the series. Bye-bye.

Lee: Thank you, John, Joyce, Lisa, and Christina. If you have any questions for them, their contact information is in the show notes. This is the final episode in this series, and we thank you for joining us. As always, thanks for listening to BakerHosts.

Comments heard on BakerHosts are for informational purposes and should not be construed as legal advice regarding any specific facts or circumstances. Listeners should not act upon the information provided on BakerHosts without first consulting with a lawyer directly. The opinions expressed on BakerHosts are those of participants appearing on the program and do not necessarily reflect those of the firm. For more information about our practices and experience, please visit bakerlaw.com.