Trade Secrets – Annual Year in Review (2020)

Russell Beck
Beck Reed Riden LLP
155 Federal Street, Suite 1302
Boston, MA 02110
(617) 500-8660
rbeck@beckreed.com

Hannah T. Joseph
Beck Reed Riden LLP
155 Federal Street, Suite 1302
Boston, MA 02110
(617) 500-8660
hjoseph@beckreed.com

Erika Hahn
Beck Reed Riden LLP
155 Federal Street, Suite 1302
Boston, MA 02110
(617) 500-8660
ehahn@beckreed.com

TABLE OF CONTENTS

I. INTRODUCTION

There have been several significant trade secret cases this year, involving issues of standing, spoliation, the level of specificity required in identifying alleged trade secrets, the extraterritorial reach of the Defend Trade Secrets Act ("DTSA"), calculation of damages, jury instructions, and others.

In addition, there have been several potentially far-reaching trade secret-related developments. In particular, a decade-plus divide over application of the Computer Fraud and Abuse Act ("CFAA"), once a tool used in trade secret cases to create federal court jurisdiction and avoid questions about whether information taken by a former employee is a trade secret, is heading to the Supreme Court. And, the federal government has been considering federal regulation of noncompetes, one of the key tools used by companies to protect their trade secrets.

Each of these cases and developments is discussed below.

II. REVIEW OF RECENT TRADE SECRET DECISIONS

A. Ownership and Use of Trade Secrets

1. *Ledbetter Trucking & Excavating, Inc. v. Miller's Classic Carpet, Inc.*, 2019 IL App (3d) 190147-U (Nov. 8, 2019) (unpublished)

Background: Ledbetter Trucking and Excavating, Inc. ("Ledbetter") entered into an asset purchase agreement with Miller's Classic Carpet, Inc. ("Miller") in 2017 by which Ledbetter purchased all of Miller's assets, including its client list and client goodwill. Claiming that certain of the defendants (including Miller's former employee, Brian Furr) had misappropriated the client list, Ledbetter sought a motion for preliminary injunction for threatened violation of the Illinois Trade Secrets Act.

The Circuit Court for the 14th Judicial Circuit, Rock Island County, Illinois, denied Ledbetter's motion. Ledbetter appealed.

Holding and analysis: The Appellate Court of Illinois, Third District, affirmed the lower-court's denial of the preliminary injunction, holding (among other things) that the client list did not qualify as a trade secret within the meaning of the Illinois Trade Secrets Act.

Applying the six-factor test derived from section 757 of the Restatement (First) of Torts, the court reasoned that any of the names and phone numbers on the client list could have been obtained through the phone book and that the list could have been easily duplicated by any of Miller's former employees. Moreover, Furr knew the contacts and had maintained the customer relationships. Significantly, Furr's personal cell phone number was used in Miller's and, later, Ledbetter's advertisements, and Ledbetter did not ask Furr to delete any of the client contacts from his phone. The court thus also found that Ledbetter did not make any reasonable efforts to protect the list at any point. The fact that Ledbetter paid seven percent of the purchase price for

Miller's goodwill and the client list was of no moment because the list had little worth without the goodwill Furr had developed.

Takeaways: For employers wishing to protect their client lists, *Ledbetter* contains some language that may be concerning. Among other things, in determining that the client list did not rise to the level of a trade secret, the court twice observed that the client list could have been recreated using a phone book. Particularly troubling, the court explicitly acknowledged that "[the list's] contents *require knowledge as to who frequently solicited Miller's services* and how to use a phone book." *Ledbetter Trucking & Excavating, Inc.*, 2019 IL App (3d) 190147-U, ¶ 29 (emphasis added). The fact that the court did not consider (at least expressly) that the "knowledge as to who frequently solicited Miller's services" could make the client list a trade secret is a departure from many other trade secret cases addressing the issue of customer lists. Nevertheless, *Ledbetter* addressed a unique fact pattern that may not apply in other cases. For instance, Furr did not sign the asset purchase agreement or any other restrictive covenants agreement with Ledbetter. Moreover, the client list in this case was relatively short, consisting only "of a typed page of Miller's 10 largest accounts that frequently solicited its hauling and excavating services and another page of snowplowing clients." *Id.* at ¶ 6. Employers facing a *Ledbetter* challenge to their trade secret claims will want to be sure to distinguish their matters from the *Ledbetter* facts.

2. *Nat'l Tractor Parts Inc. v. Caterpillar Logistics Inc.*, 2020 IL App (2d) 181056 (Feb. 28, 2020) (not released for publication)

Background: In 2004, National Tractor Parts Inc. ("NTP"), a tractor parts company, entered into a services agreement with Caterpillar Logistics Inc. ("CLI"), to perform assembly and sub-assembly services for CLI's parent company, Caterpillar. That work was performed by NTP at a designated area in a Caterpillar facility.

The 2004 services agreement provided that "NTP may receive Confidential Information from Cat Logistics or create Confidential Information as a result of Services, and any such Confidential Information is and shall be owned by Cat Logistics." *Nat'l Tractor Parts Inc.*, 2020 IL App (2d) 181056, ¶ 6. The parties entered into subsequent services agreements in 2005, 2007, and 2011, with each agreement containing confidentiality provisions identical to those in the 2004 agreement.

By 2012, Caterpillar decided to in-source its sub-assembly work and CLI began preparing to transition the work from NTP to Caterpillar. NTP allowed CLI unrestricted observation of its work, disclosed its build books for the wheel loader sub-assemblies, and permitted CLI to observe the sub-assembly process.

In March 2013, with more than a week left of work scheduled for NTP and its workers, a Caterpillar security team appeared at NTP's designated area, stopped NTP's work, and escorted NTP out of the building. According to NTP, CLI locked NTP out and took possession of the designated space and the trade secrets located therein.

NTP sued CLI, Caterpillar, and ten of its employees in June 2014, alleging, *inter alia*, misappropriation of its trade secrets. The trial court granted CLI's motion to dismiss, finding, in relevant part, that the 2011 services agreement (specifically, the confidentiality provision, which conveyed ownership of anything that NTP created as a result of performing services to CLI) barred NTP's misappropriation claim. NTP amended its complaint, naming only CLI as a defendant, to allege that it had a trade secret "for assembling component parts and sub-assemblies" that was developed before NTP began performing services for CLI. NTP's misappropriation claim survived dismissal and the parties proceeded to discovery.

During discovery, CLI pressed NTP through various motions to describe its claimed trade secrets. In July 2018, CLI filed a motion for summary judgment, arguing in relevant part that NTP had not identified anything that could be deemed a trade secret and that CLI owned the materials it was accused of misappropriating. At hearing, NTP agreed with the court's characterization of NTP's alleged trade secret as "the organization of the assembly process" for doing the sub-assembly work. *Id.* at ¶ 28.

The trial court granted CLI's motion for summary judgment. The court found that NTP's information was too general to be deemed a trade secret and, moreover, the evidence showed that CLI owned the materials it was accused of misappropriating. The court also found that the evidence undermined NTP's argument that it had developed its trade secret process prior to the contract, as the machines for which NTP claimed the trade secret did not exist then. The court also found that NTP did not take reasonable steps to protect the information.

NTP appealed.

Holding and analysis: The Appellate Court of Illinois, Second District, affirmed the lower court's grant of summary judgment.

Applying the six-factor Restatement test, the appellate court agreed with the lower court that the information was not a trade secret. With respect to factors one (the extent to which the information is known outside the business) and six (the ease of replication), the court pointed to language in the services agreement, which entitled CLI to participate in the design of, and access to, the sub-assembly process. This, coupled with the fact that CLI observed NTP's workers before terminating the contract, weighed against NTP on these factors. On factors four (the value of the information) and five (the investment in developing the information), the court found that NTP's failure to explain its trade secret "other than in the most very general terms" cut against a trade secret finding. *Id.* at ¶ 50.

The court also agreed with the trial court that the record did not support NTP's claim that it, as opposed to CLI, owned its process.

Takeaways: Contracting parties should be wary of broad contractual language that may have the effect of assigning away valuable IP. Moreover, before asserting a claim for trade secret misappropriation, parties should make sure that they are able to identify (with reasonable particularity) the trade secret(s) and offer evidence that the information in fact qualifies as a trade secret, *i.e.*, it is valuable, unique, and was subject to reasonable measures of protection.

3. *Advanced Fluid Sys., Inc. v. Huber*, 958 F.3d 168 (3d Cir. 2020)

Background: Advanced Fluid Systems, Inc. ("AFS"), a designer and manufacturer of hydraulic systems, sued its former sales engineer, Kevin Huber, and others for trade secret misappropriation under the Pennsylvania Uniform Trade Secrets Act ("PUTSA"). The United States District Court for the Middle District of Pennsylvania granted summary judgment in favor of AFS and, following a bench trial, awarded AFS compensatory damages, exemplary damages, and punitive damages. Defendants appealed.

Holding and analysis: On appeal, appellants argued that AFS could not maintain its PUTSA claim. Appellants advanced three arguments in support of this theory: (1) pursuant to a "work for hire" agreement that AFS had signed with the Virginia Commonwealth Space Flight Authority (the "Authority"), AFS did not own the confidential information; (2) even if PUTSA does not require ownership as a prerequisite for standing to sue, AFS still lacked standing because it did not "lawfully possess" the trade secrets; and (3) the confidential information did not constitute a trade secret because it was not subject to reasonable measures of protection.

As to the first argument, the court looked to the district court's "reasoned opinion," which surveyed cases from other jurisdictions and ultimately followed the reasoning set forth in *DTM Research, L.L.C. v. AT & T Corp.*, 245 F.3d 327 (4th Cir. 2001). In *DTM*, the Fourth Circuit held that a party asserting a misappropriation claim under Maryland's Uniform Trade Secrets Act ("MUTSA") need only demonstrate lawful possession of a trade secret, not "ownership in its traditional sense." 245 F.3d at 333.

With respect to the *DTM* holding, the court in *Huber* observed:

> That holding was based on the premise that "[t]he proprietary aspect of a trade secret flows, not from the knowledge itself, but from its secrecy[,]" because "[i]t is the secret aspect of the knowledge that provides value to the person having the knowledge. ... While the information forming the basis of a trade secret can be transferred, as with personal property, its continuing secrecy provides the value, and any general disclosure destroys the value." [*DTM*, 245 F.3d] at 332 (internal quotation marks omitted).

958 F.3d at 177.

Although *DTM* involved MUTSA, the relevant language of that act was functionally identical to the language in PUTSA.

The court next rejected the appellants' argument that AFS did not lawfully possess the information, which was premised on the faulty logic that the work for hire agreement transferred to the Authority not only AFS's rights in the trade secrets but also its right to lawfully possess them. The court found that appellants' assertion in this regard was unsupported by the record, which established that AFS not only physically retained possession of the information but was required to use (and did use) those trade secrets in order to perform its obligations under the agreement. The Authority never objected to AFS's possession of the trade secrets.

Finally, the court rejected appellants' reasonable measures argument, finding it unsupported by the summary judgment record.

Given the above, the court affirmed the district court's rulings and judgment in their entirety.

Takeaways: With its *Huber* decision, the Third Circuit adopted the Fourth Circuit's reasoning in finding that lawful possession of a trade secret, without ownership, can be sufficient to maintain a claim under the Pennsylvania Uniform Trade Secrets Act.

4. *Hoover Panel Sys., Inc. v. HAT Contract, Inc.*, No. 19-10650, 2020 WL 3273003 (5th Cir. June 17, 2020) (unpublished)

Background: HAT Contract, Inc. ("HAT") hired Hoover Panel Systems, Inc. ("Hoover"), a product developer, to manufacture and develop a power beam for desks in an open office environment. The parties' contract contained a confidentiality provision. After Hoover completed the development of a prototype, HAT sent the prototype to an overseas manufacturer and started using it to manufacture similar products. Hoover sued HAT, bringing claims for breach of contract, trade secret misappropriation, promissory estoppel, quantum meruit, and unjust enrichment.

HAT moved for summary judgment on all of Hoover's claims, which the United States District Court for the Northern District of Texas granted in full. Hoover appealed.

Holding and analysis: On the issue of Hoover's trade secrets claim under Texas law, the district court found that – because Hoover voluntarily sent HAT the alleged trade secret without HAT engaging in improper or unlawful activity – Hoover could not satisfy the second prong of the claim (requiring that the trade secret was "acquired through a breach of a confidential relationship or discovered by improper means"). *Hoover Panel Sys., Inc.*, 2020 WL 3273003, at *6. On appeal, Hoover argued that its misappropriation claim was not negated by the fact that it sent the prototype to HAT because the parties' agreement required HAT to maintain its confidentiality.

The Fifth Circuit reversed the district court's grant of summary judgment on Hoover's misappropriation claim, finding that a "breach of duty to maintain secrecy is a way of establishing improper means," and that "Hoover's allegation that HAT breached [their] confidentiality agreement create[d] a factual issue as to whether HAT misappropriated Hoover's alleged trade secret." *Id.* The court thus remanded the case for further findings on this issue.

Takeaways: The Fifth Circuit's holding appears to be inconsistent with the Texas Court of Appeals' decision in *Title Source, Inc. v. HouseCanary, Inc.*, which found that "[a] post-acquisition breach of a confidentiality or non-disclosure agreement . . . is irrelevant to the method by which [a defendant] obtained access to the trade secrets in the first instance and thus cannot support an improper means finding as a matter of law." No. 04-19-00044-CV, 2020 WL 2858866 (Tex. App. June 3, 2020) (internal quotations omitted). As others have observed, this raises a potential *Erie* concern. In addition, it bears note (although it is unclear what, if any,

impact it had on the court's analysis) that – in articulating the elements for misappropriation under Texas law – the court cited to pre-TUTSA case law and applied a conjunctive (requiring both acquisition by improper means *and* unauthorized use) rather than disjunctive (requiring only acquisition by improper means *or* unauthorized use or disclosure) test. *Compare Hoover Panel Sys., Inc.*, 2020 WL 3273003, at *6; *with* TEX. CIV. PRAC. & REM. CODE § 134A.002(3).

B. Spoliation

1. *WeRide Corp. v. Kun Huang*, No. 5:18-CV-07233-EJD, 2020 WL 1967209 (N.D. Cal. Apr. 24, 2020)

Background: WeRide Corp. and WeRide, Inc. (together, "WeRide") create autonomous driving technologies. In November 2018, WeRide sued two of its former executives (Kun Huang and Jing Wang), their new company (AllRide.AI, Inc. ("AllRide")), and other parties for trade secret misappropriation and a host of other claims arising in part out of their alleged misappropriation of WeRide's source code.

In March 2019, the United States District Court for the Northern District of California entered a preliminary injunction that, among other things, enjoined certain of the defendants from "[d]estroying, concealing, disposing, deleting, removing or altering any and all documentation of any kind, whether paper or electronic, . . . data, drafts or other things or materials" that were related to WeRide's confidential material or information or AllRide's source code. *WeRide Corp.*, 2020 WL 1967209, at *2.

In the summer of 2019, just before the parties were scheduled to appear at a hearing on several discovery disputes, AllRide filed a letter with the court disclosing that, two months prior, it had become aware that it had not turned off an auto-delete setting on the company's email server, resulting in the company-wide destruction of emails predating the middle of March 2019. The letter separately disclosed that several individual email accounts associated with Wang and his wife had been destroyed.

The court appointed a neutral forensic inspector to investigate the destruction and a special master to resolve any disputes relating thereto. Following the investigation, WeRide moved for sanctions based on: (1) the widespread destruction of emails, (2) spoliation of five different categories of source code, and (3) spoliation by other means.

Holding and analysis: After engaging in a detailed discussion concerning the nature and scope of the defendants' destruction, the court observed that "[t]he amount of spoliation that AllRide concedes is staggering." *Id.*, at *9. Indeed, AllRide had admitted that it (a) maintained its company-wide policy of deleting from its server all emails older than 90 days until months after the preliminary injunction issued, (b) that it deleted several key email accounts, including after the complaint was filed and, at least with respect to one account, after the preliminary injunction issued, (c) that it did not end its policies of deleting email accounts and wiping computers of former employees until months after the preliminary injunction issued, and (d) that AllRide's employees began using an ephemeral messaging application after the preliminary injunction issued.

Applying the Ninth Circuit's framework analysis for considering sanctions under Fed. R. Civ. P. Rule 37(b) (failure to comply with a court order), set forth in *Leon v. IDX Sys. Corp.*, 464 F.3d 951, 958 (9th Cir. 2006), the court first held that terminating sanctions against AllRide were appropriate. Notably, the court found that "AllRide's destruction of evidence was so sweeping that this case [could not] be resolved on its merits" and that "any jury instruction or exclusion of evidence would be inappropriate here because the spoliation occurred on such a massive scale." *WeRide Corp.*, 2020 WL 1967209, at *11. The court found the case against AllRide "even more damning under Rule 37(e)" (failure to preserve electronically stored information ("ESI")), as "AllRide's conduct show[ed] a disturbing pattern of destroying discoverable material that began with the company's founding and continued not only through the commencement of th[e] litigation but past the preliminary injunction as well." *Id.*, at *12.

The court held that Wang and Huang were also both subject to terminating sanctions because Wang controlled AllRide and must have had knowledge of its spoliation and Huang willfully violated the preliminary injunction when he modified over 1,000 source code files in late March 2019, thereby severely prejudicing WeRide's case against Huang. Huang also destroyed ESI on two WeRide laptops and wiped and returned a personal laptop on the same day he received a cease-and-desist letter.

Based on these findings, the court ordered Wang, Huang, and AllRide to pay WeRide's reasonable attorneys' fees and costs incurred in connection with the spoliation motion, all discovery related to defendants' spoliation of evidence, and certain discovery motion practice. The court also struck the answers of Wang, Huang, and AllRide and directed the clerk to enter the default of those defendants. *Id.*, at *16.

Takeaways: Through the myriad missteps of the defendants, *WeRide* provides a clear roadmap of what to do (and, more importantly, what not to do) once a party's preservation obligations are triggered. Once an employer has a duty to preserve evidence, it should immediately implement a litigation hold, discontinue policies and disable settings that result in the deletion or destruction of potentially relevant information, and take affirmative steps to identify and preserve all repositories of potentially relevant information. The employer should involve its IT department and outside counsel in these steps to ensure best practices. In addition, the employer should work to ensure that its employees also preserve potentially relevant information. Among other things, employees should not use personal devices or ephemeral messaging applications to discuss potentially relevant matters. Finally, the employer must not only comply with all court orders – including any orders dealing with the preservation or production of information – but it must ensure that its employees do the same.

2. *Packaging Corp. of Am., Inc. v. Croner*, 419 F. Supp. 3d 1059 (N.D. Ill. 2020)

Background: In May 2019, Packaging Corporation of America, Inc. ("PCA"), a producer of containerboard and uncoated freesheet, sued its former employee, Patrick Croner, for breach of employment agreement and trade secret misappropriation under the DTSA and Illinois Trade

Secrets Act. PCA moved for a preliminary injunction and Croner moved to dismiss the trade secret counts.

Holding and analysis: In opposing Croner's motion to dismiss, and in support of its motion for preliminary injunction, PCA argued, *inter alia*, that Croner – who was permitted to use his personal computer during his employment with PCA – had wrongfully deleted material from his laptop after his resignation. PCA contended that this amounted to spoliation and, accordingly, that the court should infer that Croner was being deceptive and had misappropriated PCA's trade secrets.

The court rejected PCA's argument, holding that the fact that Croner deleted information did not plausibly suggest that he intended to deny PCA access to material evidence of misappropriation. Noting that PCA's corporate representative had admitted during the preliminary injunction hearing that the company did not want its employees to keep confidential information on their personal computers, the court found that Croner's deletions supported his claim that he did not use or disclose any trade secrets but, rather, took active steps to divest himself of PCA's confidential information.

The court also rejected PCA's argument that the court should infer that Croner was still in possession of confidential material. The court instead found that Croner's actions (leaving files and his work computer on his work desk and deleting files from his personal laptop) were a reasonable method for complying with PCA's demand to return materials to the company.

Takeaways: *Packaging Corp.* provides an example of when it may be acceptable and even advisable for a former employee to delete an employer's information in his or her possession (*e.g.*, at the time of resignation, before preservation obligations have been triggered).

C. Identification of Trade Secrets

1. *Coda Dev. S.R.O v. Goodyear Tire & Rubber Co.*, No. 5:15-CV-1572, 2019 WL 6219745 (N.D. Ohio Nov. 21, 2019)

Background: Coda Development S.R.O. ("Coda") brought suit against Goodyear Tire & Rubber Company ("Goodyear") for the alleged theft of Coda's self-inflating tire ("SIT") technology, which Coda alleged it disclosed *orally* to Goodyear during two meetings.

Following a status conference, the United States District Court for the Northern District of Ohio issued an order requiring Coda, in response to certain interrogatories, to provide a description of what was said during the meetings and a complete list of the trade secrets that Coda claimed were orally disclosed. The court also directed counsel to brief "the issue of whether any description of what was said at the meetings may be supplemented at a later date or whether plaintiffs are bound by their written response." *Coda Dev. S.R.O*, 2019 WL 6219745, at *1.

On this issue, Goodyear argued that, "[s]ince Coda contends that its spoken words at these two meetings are worth hundreds of millions of dollars, it is only fair to require Coda to provide a complete, straightforward, and closed answer[.]" *Id.*, at *2. Goodyear contended that, absent a

"closed" discovery response, the central facts of the case could become "moving targets" and, further, that Coda might mold its claims based on discovery received from Goodyear. *Id.*, at *3.

Coda asserted that it should not be bound to a "closed" interrogatory answer or precluded from supplementing its answer at a later date, as that would be contrary to the Federal Rules of Civil Procedure and amount to "punish[ing] litigants for having imperfect memories[.]" *Id.*

Holding and analysis: In analyzing whether or not Coda should be required to provide a "closed" discovery response, the court considered the competing policies in trade secret disputes relating to "allowing the trade secret plaintiff to take discovery prior to identifying its claimed trade secrets" versus "delaying trade secret discovery until the trade secret plaintiff has sufficiently described the trade secrets at issue." *Id*.

As the court noted, the policy arguments that have been advanced in support of permitting pre-identification discovery include: (1) the broad right to discovery afforded under the Federal Rules of Civil Procedure; (2) that a plaintiff may not know which trade secrets have been misappropriated prior to discovery; and (3) that requiring a plaintiff to identify its trade secrets without knowledge of the defendant's conduct places the plaintiff in a "Catch-22."

The policy arguments that support requiring pre-discovery identification include the desires to: (1) avoid fishing expeditions by plaintiffs seeking to discover their competitors' trade secrets; (2) enable parties and the courts to determine the relevance of certain requested discovery; (3) enable the defendant to mount its defense; and (4) preclude the plaintiff from molding its cause of action around the discovery it receives.

Further observing that courts are trending toward requiring plaintiffs to identify their trade secrets with reasonable particularity, the court found that "[u]nder the peculiar circumstances of this case, where the alleged disclosure of trade secrets was *entirely oral*, the danger of plaintiffs 'molding' their claims by way of subsequent supplementation of their original recollection of those two 2009 conversations [wa]s of particular concern." *Id.*, at *4 (emphasis in original).

The court accordingly required Coda to supply a "closed" response with "sufficient specificity and description to permit defendants to know what discovery will be relevant and what specific claims of trade secret misappropriation they must defend against." *Id.* The court warned Coda against providing a vague or evasive response, under threat of sanctions, and held that supplementation would only be permitted in limited circumstances and only upon a showing of exceptional reason for doing so.

Takeaways: In those instances where a party seeks to maintain a trade secrets claim based entirely on an oral disclosure, it should expect limited judicial tolerance for modifications to early specifications of what trade secrets were discussed and that it may be prohibited from relying on information received through discovery in defining its trade secrets.

2. *TLS Mgmt. & Mktg. Servs., LLC v. Rodriguez-Toledo*, 966 F.3d 46 (1st Cir. 2020)

Background: TLS Management and Marketing Services, LLC ("TLS") is a tax planning and consulting firm in Puerto Rico. Defendant Ricky Rodríguez-Toledo ("Rodríguez"), who was the founder of defendant ASG Accounting Solutions Group, Inc. ("ASG"), also offered tax planning and accounting services.

In March 2012, ASG signed a subcontractor agreement with TLS containing a nondisclosure agreement. In September 2012, Rodríguez begin working for TLS and signed an agreement also containing nondisclosure obligations.

In early 2015, Rodríguez's and ASG's relationship with TLS came to an end. Thereafter, Rodríguez acquired a majority interest in defendant Global Outsourcing Services, LLC ("GOS"), and all three defendants competed with TLS.

TLS sued the defendants alleging trade secret misappropriation (*i.e.*, downloading and taking certain documents through Dropbox) by Rodríguez and ASG and breach of nondisclosure agreements by all three defendants (by providing services to certain former clients of TLS using TLS's information).

Judgment entered in favor of TLS, and defendants appealed to the First Circuit.

Holding and analysis: Distinguishing trade secrets from other types of intellectual property, which involve knowable metes and bounds, the First Circuit noted that Puerto Rico's Industrial and Trade Secret Protection Act requires early identification by the plaintiff of the information claimed to be the misappropriated trade secrets. As the court explained, this is in part to avoid the possibility that (as happened in that case) "the trade secret owner will tailor the scope of the trade secret in litigation to conform to the litigation strategy." *TLS Mgmt. & Mktg. Servs., LLC*, 966 F.3d at 52.

TLS offered the following descriptions as to the first of its two claimed trade secrets: "53 different methods or techniques" based on a compilation of public or client information by which:

> TLS would conduct a "salary analysis," consider "fringe benefits," look at the client's "retirement plan," and use "captive insurance company" techniques, or decide "whether or not [the client] can get a race car and modify how they use it to write it off as advertising," and that its recommendations would result in tax savings.

Id. at 53-54. The court concluded that "[s]uch general description was insufficient to establish a trade secret." *Id.* at 54. Specifically, the court held that TLS failed to "separate the [purported] trade secrets from the other information ... [that was] known to the trade." *Id.* (citation omitted).

Rejecting the other claimed trade secret (TLS's loan strategy), the court held:

> TLS could not claim a trade secret protection simply because its loan strategy was not publicly known. TLS also had to establish that this aspect of the Strategy was not readily ascertainable from public sources. On this issue, TLS presented no evidence. We thus conclude that TLS failed to show that the Strategy was not readily ascertainable.

Id. at 54-55.

Having dispensed with the two alleged trade secrets, the court turned to the claimed breaches of the nondisclosure agreements. The court explained that "[a] nondisclosure agreement is overly broad if the restriction is unnecessary for the protection of the employer's business, unreasonably restrictive of the employee's rights, and prejudicial to the public interest." *Id.* at 58 (internal quotations omitted). The court then concluded TLS's nondisclosure agreements as overly broad because they prohibited use and disclosure of information that (1) is general knowledge, (2) is otherwise publicly available, and (3) was received from third parties (such as TLS's former clients). Refusing to narrow the "astounding [over]breadth," the court explained that, "while not specifically prohibiting an employee from entering into competition with the former employer, [overly broad nondisclosure agreements] raise the same policy concerns about restraining competition as noncompete clauses where, as here, they have the effect of preventing the defendant from competing with the plaintiff." *Id.* at 57, 59.

Takeaways: First, contrary to conventional wisdom, courts do not always reflexively find misappropriation of trade secrets when employees walk out the door with company materials. Instead, courts around the country have become increasingly strict about requiring plaintiffs to identify trade secrets with specificity before moving forward with discovery, and we can expect to see more courts moving in that direction. And, in that regard, phrases like "53 different methods or techniques" or using "'captive insurance company' techniques," or a "salary analysis," without corresponding details about what these things actually are, will likely not be sufficient to satisfy the specificity requirements.

In addition, when it comes to purported trade secrets based on a compilation of public materials, plaintiffs will need to distinguish the claimed trade secret from public information with which it is mixed. A plaintiff will not be permitted to merely identify a type of technology and then expect the court to hunt through the details to find anything that may be a trade secret.

Finally, the decision likely heralds a skeptical view of broad nondisclosure agreements in the First Circuit.

3. *Zoom Imaging Sols., Inc. v. Roe*, No. 219CV01544WBSKJN, 2019 WL 5862594 (E.D. Cal. Nov. 8, 2019)

Background: Zoom Imaging Solutions, Inc. ("Zoom"), a provider of printing and imaging services to commercial businesses, sued its former employees and a competitor for, *inter alia*,

trade secret misappropriation under the DTSA and California Uniform Trade Secrets Act ("CUTSA").

On their Rule 12(b)(6) motion, with respect to Zoom's trade secrets claims, the defendants argued that Zoom had not sufficiently identified its claimed trade secrets.

Holding and analysis: The United States District Court for the Eastern District of California first evaluated Zoom's claim under CUTSA, which requires that plaintiff "describe the subject matter of the trade secret with sufficient particularity to separate it from matters of general knowledge in the trade or of special persons who are skilled in the trade, and to permit the defendant to ascertain at least the boundaries within which the secret lies." *Zoom Imaging Sols., Inc.*, 2019 WL 5862594, at *4 (citing *Alta Devices, Inc. v. LG Elecs., Inc.*, 343 F. Supp. 3d 868, 881 (N.D. Cal. 2018)).

Applying this standard, the court noted that, although Zoom had defined its "Confidential Information," to include, *inter alia*, its customer contact information, pricing, costs, margins, and purchase histories (to name just a few categories), it did not claim that all of its Confidential Information constituted trade secrets. Further, Zoom had not listed its Confidential Information comprehensively, but rather defined it as "business information, including, *but not limited to*" the items listed. *Id.* (emphasis in original). The court found Zoom's other cited-to language in the complaint – alleging that defendants "used Zoom's trade secrets and other confidential business information...including the use of valuable information regarding customers' contract particulars (including, without limitation pricing and end date)" – equally unhelpful as it "neither identifie[d] the purported trade secrets nor clarifie[d] the general category of the purported trade secrets." *Id.*, at *5.

Ultimately, the court found that:

> Because the list of Confidential Information is not exhaustive, and because the trade secrets are an unknown subset of the indefinite Confidential Information, plaintiff does not sufficiently identify anything. The Complaint gives defendants no clue whatsoever about what information forms the basis of plaintiff's misappropriation claim.

Id.

Finding that Zoom's allegations in this regard were similar to those that other courts had deemed too vague, the court found that the complaint did not sufficiently identify the trade secrets and dismissed the claim. For the same reasons, the complaint failed to state a viable cause of action under the DTSA, and the court dismissed that claim as well.

Takeaways: *Zoom* is one of the more recent opinions to come out of California requiring a plaintiff to identify its trade secrets with sufficient particularity prior to taking discovery. The court's harsh treatment of the non-exhaustive language ("including, but not limited to" and "including, without limitation") is particularly interesting, as that language is common in complaints alleging trade secret misappropriation. Putative plaintiffs, particularly in California,

seeking to avoid the outcome in *Zoom* should (where possible) narrow their descriptions of their confidential information to the trade secrets that are alleged to have been misappropriated and avoid non-exhaustive language. Of course, *Zoom* reflects only one end of the spectrum (from requiring pre-discovery disclosure to allowing pre-identification discovery) and a plaintiff's burden may be dictated by the jurisdiction it is in and which law applies. *See, e.g.*, *M.H. Eby, Inc. v. Timpte Indus., Inc.*, No. CV 19-386, 2019 WL 6910153, at *7 (E.D. Pa. Dec. 19, 2019) (A plaintiff's "description of the trade secrets at issue need only be sufficient to (a) put a defendant on notice of the nature of the plaintiff's claims and (b) enable the defendant to determine the relevancy of any requested discovery concerning its trade secrets. . . . A robust consensus of district courts within the Third Circuit have held that a party alleging misappropriation in violation of [the Pennsylvania Uniform Trade Secrets Act] need not describe trade secrets with particularity to survive Rule 12 scrutiny.") (internal quotations omitted).

D. Extraterritorial Reach of the Defend Trade Secrets Act: *Motorola Sols., Inc. v. Hytera Commc'ns Corp.*, 436 F. Supp. 3d 1150 (N.D. Ill. 2020)

Background: The parties are competitor radio manufacturers. Motorola Solutions, Inc. and related entities (collectively, "Motorola") claimed that Hytera Communications Corporation Ltd. and related entities (collectively, "Hytera") hired three engineers from Motorola's Malaysian office, that those engineers stole thousands of Motorola's confidential documents, and that Hytera used those documents (containing trade secrets and lines of source code) to develop a state-of-the-art digital radio (that was indistinguishable from Motorola's radios), which was then sold around the world, including in the United States. Motorola sued Hytera for, among other things, violation of the DTSA.

Hytera argued that the DTSA does not have extraterritorial effect and that all damages should therefore be limited to the statute's domestic application. Motorola argued that the DTSA reaches extraterritorially, either because it applies extraterritorially or because the conduct being regulated was domestic, and therefore all damages, including those arising extraterritorially, could be recovered.

Holding and analysis: The court first articulated the U.S. Supreme Court's two-step framework for analyzing extraterritoriality issues:

> At the first step, a court asks whether the presumption against extraterritoriality "has been rebutted—that is, whether the statute gives a clear, affirmative indication that it applies extraterritorially." *RJR Nabisco, Inc., v. European Cmty.*, —— U.S. ——, 136 S. Ct. 2090, 2101, 195 L. Ed. 2d 476 (2016). If no clear, affirmative indication exists, the statute is not extraterritorial and the court proceeds to a second step, in which it determines whether the case involves "a domestic application of the statute." *Id.* This determination is made by determining the statute's focus. "If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad; but if the conduct relevant to the focus occurred in a foreign country, then the case involves an impermissible

> extraterritorial application regardless of any other conduct that occurred in U.S. territory." *Id.*

Motorola Sols., Inc., 436 F. Supp. 3d at 1155.

Applying this test, the court held that the DTSA overcomes the presumption against extraterritoriality.

The court first found that, although 18 U.S.C. § 1836 (the section of the EEA amended by the DTSA to provide a private right of action for trade secret misappropriation) contains no reference to extraterritorial conduct or application, it must be read together with section 1837, which provides:

> This chapter also applies to conduct occurring outside the United States if-
>
> (1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or
>
> (2) an act in furtherance of the offense was committed in the United States.

Id. at 1159 (quoting 18 U.S.C. § 1837).

The court reasoned that the "biggest indicator" that Congress intended for section 1836 to apply extraterritorially is the fact that section 1837 refers broadly to "this chapter," which necessarily includes section 1836. *Id.* Indeed, as the court observed, that the law includes numerous references to extraterritorial conduct that were absent from previous versions indicates that Congress was concerned with actions taking place outside of the U.S. in relation to the misappropriation of U.S. trade secrets when it passed the DTSA.

The court acknowledged that section 1837 contains language limiting the statute's extraterritorial application based on qualities related to the "offender" or the "offense," which could be interpreted as being limited to criminal law. The court also acknowledged Supreme Court precedent under *RJR Nabisco*, 136 S. Ct. at 2108, which – in addition to drawing a distinction between the extraterritorial reach of the criminal and civil provisions of the RICO statute – voiced several policy concerns related to extending a private right of action extraterritorially. In this regard, the court stated that it "takes very seriously *RJR Nabisco*'s directive that 'the need to enforce the presumption [against extraterritoriality] is at its apex' where a risk of conflict between laws is evident." *Id.* at 1162.

Having considered all of that, the court found that, despite arguably limiting language in section 1837, it was clearly Congress's intent to extend the extraterritorial provisions of section 1837 to section 1836. The court therefore held that section 1836 can be applied extraterritorially in a private cause of action if either requirement of section 1837 is met.

The court next held that the requirements of section 1837 were met as it was undisputed that defendants advertised, promoted, and marketed products embodying the allegedly stolen trade secrets within the U.S. and that such "use" had continued after the DTSA's effective date. (The court joined two other district courts in finding that continuous use can bring misconduct within the purview of the DTSA.) The court therefore held that Motorola could recover extraterritorial damages resulting from misappropriation, but only insofar as they occurred after the DTSA's effective date.

Although it did not need to, the court also noted that the case would still present a proper domestic application of the statute, thereby satisfying the second prong of the two-step test for evaluating extraterritoriality. In this regard, the court noted that the focus of the DTSA is on creating a remedy for a trade secret's owner for misappropriation. Given that Motorola provided evidence that the alleged trade secrets had been used domestically, the second prong was satisfied.

On April 2, 2020, Hytera moved for judgment as a matter of law and a new trial, again arguing, *inter alia*, that 18 U.S.C. § 1837 does not apply to private civil suits. The court has not yet ruled on the motion.

Takeaways: The *Motorola* decision is one of the first to provide an in-depth analysis of the extraterritorial scope of the DTSA and may provide a roadmap for other courts, as well as support to plaintiffs seeking extraterritorial damages in future cases (assuming the decision survives). Of course, the significance of the quantum and nature of the U.S. contacts remains a determinative issue. *See, e.g.*, *ProV Int'l Inc. v. Lucca*, No. 8:19-CV-978-T-23AAS, 2019 WL 5578880, at *3 (M.D. Fla. Oct. 29, 2019) (holding that a plaintiff could not maintain a DTSA claim for misappropriation where the amended complaint contained no allegation that the defendants either acquired or used the alleged trade secrets in the U.S.).

E. Damages, Jury Verdicts, and Fees

1. *Title Source, Inc. v. HouseCanary, Inc.*, No. 04-19-00044-CV, 2020 WL 2858866 (Tex. App. June 3, 2020) (not released for publication)

Background: Title Source, Inc. ("TSI," now known as "Amrock") provides title insurance, property valuations, and settlement services in real estate transactions. HouseCanary, Inc. is a real estate analytics company.

Starting in 2014, HouseCanary agreed to provide certain proprietary software and analytics to TSI. To that end, the parties executed a series of agreements by which they agreed, among other things, not to "develop, manufacture, produce, and/or distribute any software or business system derived from or which otherwise uses any of the [other party's] Confidential Information." *Title Source, Inc.*, 2020 WL 2858866, at *1-2. Unbeknownst to HouseCanary, and despite repeated assurances by TSI, TSI was developing its own valuation models based on HouseCanary's data.

The parties' relationship began deteriorating in 2016. Following HouseCanary's refusal to sign a second amendment to the parties' licensing agreement – which would have required HouseCanary to send all of its underlying formulas and analytics to TSI and removed all restrictions (on TSI) on reverse engineering HouseCanary's data and creating derivative products – TSI sued HouseCanary for breach of contract and fraud. HouseCanary countersued for breach of contract, fraud, unjust enrichment, quantum meruit, and later added a claim for trade secret misappropriation in violation of the Texas Uniform Trade Secrets Act ("TUTSA").

The jury found in HouseCanary's favor on its trade secret misappropriation, fraud, and breach of contract claims, and rejected each of TSI's affirmative claims. Judgment of nearly $740 million entered against TSI.

TSI moved for a new trial, which the trial court denied. TSI appealed.

Holding and analysis: On appeal, the Court of Appeals of Texas, San Antonio, found that the lower court's jury instruction, which asked the jury to determine whether TSI misappropriated HouseCanary's trade secrets based on a theory of either "use" or "acquisition," improperly contained multiple liability theories that were not supported by the evidence.

With respect to the *acquisition theory* instruction – which tracked relevant language in TUTSA[1] – the appellate court first found that there was no evidence that TSI acquired the trade secrets through bribery or espionage and, therefore, they should have been omitted from the "improper means" definition that was submitted to the jury.

Still focused on the *acquisition theory* instruction, the court also found that the "breach or inducement of a breach of a duty to maintain secrecy, to limit use, or to prohibit discovery of a trade secret" language should have been omitted. The court held that, under the plain language of TUTSA, "TSI needed to acquire the trade secrets *as a result of* the alleged breaches to support a misappropriation finding." *Id.*, at *10 (citing TEX. CIV. PRAC. & REM. CODE § 134A.002(3)(A)) (emphasis in original). As a result, the court reasoned that "[a] post-acquisition breach of a confidentiality or non-disclosure agreement . . . is irrelevant to the method by which [TSI] *obtained* access to the trade secrets in the first instance and thus [could not] support an improper means finding as a matter of law." *Id.* (emphasis added; internal quotations omitted).

The court determined that the inclusion of the erroneous jury instructions constituted harmful error, requiring a new trial. It therefore reversed the trial court's judgment on HouseCanary's TUTSA claim and remanded the claim for a new trial.

The court also found that, to the extent that TSI's fraud claim was based on an assertion that TSI misappropriated HouseCanary's trade secrets, those allegations were preempted by TUTSA. The court therefore reversed the court's judgment on HouseCanary's fraud claim and remanded that for a new trial as well.

[1] Both TUTSA and the jury instruction define "improper means" as including "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, to limit use, or to prohibit discovery of a trade secret, or espionage through electronic or other means." *Id.*, at *9 (citing TEX. CIV. PRAC. & REM. CODE § 134A.002(2)).

Takeaways: Practitioners must take care to appropriately tailor their jury instructions to the applicable law and evidence presented in the case, and the failure to do so may have severe consequences.

2. *Insurent Agency Corp. v. Hanover Ins. Co.*, No. 16CV3076LGSJLC, 2020 WL 86813 (S.D.N.Y. Jan. 8, 2020), *report and recommendation adopted sub nom. Insurent Agency Corp. v. Hanover Ins. Grp., Inc.*, No. 16 CIV. 3076 (LGS), 2020 WL 1080774 (S.D.N.Y. Mar. 6, 2020)

Background: Insurent Agency Corporation (and a related company) (together, "Insurent") brought a host of claims against The Hanover Insurance Company ("Hanover") and two others, including, *inter alia*, state and federal claims for trade secret misappropriation. Hanover eventually prevailed on all asserted claims, some on motions to dismiss and others on summary judgment. (The claims against the other parties were settled.) Afterward, Hanover moved to recover its attorneys' fees under the Copyright Act, the Lanham Act, and the DTSA. Agreeing that Hanover was the prevailing party, the magistrate judge considered whether there was a basis for recovering fees under each statute.

With respect to Hanover's request under the DTSA – which grants courts discretion to award reasonable fees to the prevailing party on a showing that the claim was made in bad faith – the magistrate judge found that the summary judgment record did not indicate that Insurent's DTSA claim was meritless or brought for improper purposes. Specifically, although Insurent failed to establish that Hanover knew of the trade secrets, or acquired them through improper means or used them, Insurent's claim only "failed as a matter of *proof*." *Insurent Agency Corp.*, 2020 WL 86813, at *9 (emphasis in original). The record did not "demonstrate that it was wholly without merit and brought in bad faith." *Id.*

Specifically, the magistrate judge found that, at the time the claim was filed, Insurent's belief that the trade secrets had been misappropriated appeared to be reasonable. The judge also found that the fact that Insurent's DTSA claim survived summary judgment against other defendants, when considered in context of the relationship between Hanover and the other defendants, weighed in Insurent's favor. The magistrate judge accordingly recommended that the court deny Hanover's request to recover fees under the DTSA. Hanover objected to the magistrate judge's report and recommendation.

Holding and analysis: The United States District Court for the Southern District of New York adopted the magistrate judge's report and recommendation, holding that there was "no basis to find Plaintiffs acted in bad faith in bringing a trade secrets misappropriation claim against Hanover." *Insurent Agency Corp.*, 2020 WL 1080774, at *4.

The court found that, although Hanover claimed that it "undertook an exhaustive investigation of its own files to confirm that it neither possessed nor used any of Plaintiffs' trade secrets – and informed Plaintiffs of the same[,]" that did not establish that Insurent's claim had no good faith basis, as "a plaintiff is not required to withdraw a claim . . . merely because the defendant asserts that it conducted an internal search and found no evidence of plaintiff's claims . . . ." *Id.* The

court further held that "[i]t was not unreasonable for Plaintiffs' attorneys to believe that facts supporting the claim might be established following discovery" and "nothing in the record demonstrates that [the claim] was wholly without merit." That the trade secret claim survived Hanover's motion to dismiss further supported denial of Hanover's request for fees.

Takeaways: As the magistrate judge in *Insurent* recognized, neither the legislature nor the courts have defined "bad faith" under the DTSA. The court therefore applied the Second Circuit's definition of "bad faith" as applied in other contexts to require a showing that Insurent's claim was meritless *and* brought for improper purposes. Within this framework analysis, that a defendant ultimately prevails in defending against the claim is not sufficient, standing alone, to warrant recovery of fees under the DTSA. As the court stated, "The question is whether a reasonable attorney could have concluded that facts supporting the claim *might be* established." *Id.* (emphasis in original).

F. Criminal Liability Under the Economic Espionage Act ("EEA"): *United States v. O'Rourke,* 417 F. Supp. 3d 996 (N.D. Ill. 2019), *appeal dismissed*, No. 19-3179, 2019 WL 8631809 (7th Cir. Nov. 14, 2019)

Background: Robert O'Rourke was a metallurgical engineer and salesperson for Dura-Bar, an Illinois-based manufacturer of specialized iron bars. After accepting a position as vice president of research and development with Hualong, a Chinese competitor, O'Rourke resigned from his position at Dura-Bar. On the Sunday before his last day at work, O'Rourke entered Dura-Bar's facility and downloaded more than 1,900 documents from Dura-Bar's network onto his personal hard drive. Shortly after, Dura-Bar management discovered O'Rourke's unauthorized taking and contacted law enforcement. O'Rourke was arrested by the U.S Customs and Border Patrol as he attempted to board a flight to China. The hard drive with the stolen documents was found in his checked luggage. O'Rourke was charged with 13 counts of theft and attempted theft of trade secrets in violation of 18 U.S.C. § 1832(a).

At trial, O'Rourke did not dispute that he had taken the materials without permission but, rather, that they were not trade secrets and that he did not believe them to be trade secrets at the time of taking. The jury found O'Rourke guilty of seven counts of theft and attempted theft of trade secrets. He was sentenced to a year and a day of prison and fined $100,000.[2]

O'Rourke moved for a new trial, arguing, *inter alia*, that the government should not have been allowed to prosecute O'Rourke on both attempt and substantive charges, and that several of the jury instructions were variously wrong and insufficient.

Holding and analysis: The United States District Court for the Northern District of Illinois denied O'Rourke's motion for a new trial.

[2] *See* "Businessman Sentenced to a Year in Prison for Stealing Employer's Trade Secrets While Planning New Job in China" (2019), https://www.justice.gov/usao-ndil/pr/businessman-sentenced-year-prison-stealing-employer-s-trade-secrets-while-planning-new ("DOJ Press Release on O'Rourke Sentencing," last visited Aug. 11, 2020).

In so doing, the court rejected O'Rourke's argument that section 1832 allows for a violation based on attempt only "when a defendant tries and fails to misappropriate *actual* trade secrets." *O'Rourke*, 417 F. Supp. 3d at 1002 (emphasis added). Citing to Third Circuit law (finding that the common law legal impossibility defense did not apply to EEA violations), the court found that EEA violations based on attempt "do not require proof that a trade secret exists" but rather only that "the individual *taking* the information at issue believed that information to be a trade secret." *Id.* (emphasis in original). Accordingly, the court stated, "[I]f the jury concluded that O'Rourke believed a document was a trade secret when he took it, he is guilty for attempted theft even if the document ultimately was not a trade secret . . . ." *Id.* at 1003.

Concerning the substantive charges of theft, the court rejected O'Rourke's argument that section 1832 should be read to require that a defendant know that the information he is taking *actually* constitutes a trade secret in order to assign criminal liability, as courts have held is required under section 1831 (criminalizing economic espionage to benefit a foreign government, instrumentality, or agent). As the court noted, "§ 1831 differs in one key respect: it criminalizes knowingly stealing or communicating a *trade secret*, not, as § 1832 does, knowingly stealing or communicating *such information*." *Id.* at 1005 (emphasis in original). Finding that the difference in language "changes what the word 'knowingly' modifies," the court held that section 1832 requires only that a "defendant know that he is stealing . . . the information described in § 1839 as a trade secret—that is, information owned by another that the owner has taken reasonable measures to keep secret and that derived independent economic value from not being known to or ascertainable by the general public." *Id.* Section 1832 does not require a defendant to know that what he is stealing is actually a trade secret. Based on this analysis, the court held that it did not err when it instructed the jury that it must find that O'Rourke "knew or believed that the information constituting the trade secret was proprietary information, meaning belonging to someone else who had an exclusive right to it." *Id.* at 1004

Takeaways: Criminal liability based on the attempted theft of a trade secret may exist under section 1832 of the EEA, even where the information taken by the defendant is not a trade secret, if the defendant believed it to be a trade secret at the time of taking. Moreover, the substantive offense of theft does not require a showing that the defendant knew – at the time of taking – that the information was actually a trade secret but, rather, only that it was information that is defined as a trade secret under section 1839.

It also bears noting that *O'Rourke* is yet another example of the federal government's continuing crackdown on economic espionage, particularly in cases involving Chinese competitors or the Chinese government.[3] Indeed, in the government's sentencing memorandum in *O'Rourke*,

[3] *See* DOJ Press Release on O'Rourke Sentencing; *see also*, *e.g.*, "US ratchets up China tensions, closing Houston consulate" (2020), https://apnews.com/ffc84d09363ba0a1a0e6db3c05bb8322 (last visited Aug. 11, 2020); "Harvard University Professor Indicted on False Statement Charges" (2020), https://www.justice.gov/opa/pr/harvard-university-professor-indicted-false-statement-charges (last visited Aug. 11, 2020); "Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax" (2020), https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking (last visited Aug. 11, 2020); "Chinese Citizen Convicted of Economic Espionage,

Assistant U.S. Attorney Shoba Pillay stated, "Theft of trade secrets is a serious offense with wide-ranging consequences to the victim companies and the United States economy . . . . A would-be insider thief must understand the consequences of stealing their employer's trade secrets in order to benefit competitors, particularly when those competitors are based in China."[4] Of course, the Department of Justice is not singularly focused on China, as we were recently reminded by the sentencing of Anthony Levandowski for trade secret theft related to Google's self-driving car program. Most recently in that case, Levandowski pled guilty, was sentenced to 18 months in prison, a three-year period of supervised release, and was ordered to pay a $95,000 fine and $756,499.22 to Waymo LLC in restitution.[5]

G. Computer Fraud and Abuse Act

1. *United States v. Van Buren*, 940 F.3d 1192 (11th Cir. 2019), *cert. granted*, 206 L. Ed. 2d 822 (Apr. 20, 2020)

Background: Nathan Van Buren was a police sergeant in Cumming, Georgia. In that role, he searched an official government license-plate database on behalf of a civilian, who paid him to run the search. As a result of his actions, Van Buren was convicted of one count of honest-services wire fraud and one count of felony computer fraud in violation of the CFAA.

Van Buren appealed his convictions to the Eleventh Circuit. Among other things, Van Buren argued that there was insufficient evidence to support his conviction for computer fraud.

Holding and analysis: The Eleventh Circuit held that, under binding circuit precedent, a jury could have found beyond a reasonable doubt that Van Buren committed computer fraud for financial gain.

The court first noted that, although Van Buren's appeal had been "styled as a sufficiency-of-the-evidence challenge," he was really asking the court to overturn the precedent established by its previous decision in *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010). *Van Buren*, 940 F.3d at 1207. In *Rodriguez*, the court interpreted the CFAA – which makes it a crime to "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] information from any department or agency of the United States" – to extend to instances in which a person *with* authority to access a computer nevertheless does so for *improper purposes*. 628 F.3d at 1263 (quoting 18 U.S.C. § 1030(a)(2)(B)).

Theft of Trade Secrets, and Conspiracy" (2020), https://www.justice.gov/opa/pr/chinese-citizen-convicted-economic-espionage-theft-trade-secrets-and-conspiracy (last visited Aug. 11, 2020); "Chinese National Who Worked at Monsanto Indicted on Economic Espionage Charges" (2019), https://www.justice.gov/opa/pr/chinese-national-who-worked-monsanto-indicted-economic-espionage-charges (last visited Aug. 11, 2020).

[4] DOJ Press Release on O'Rourke Sentencing.

[5] *See* "Former Uber Executive Sentenced to 18 Months in Jail for Trade Secret Theft from Google" (2020), https://www.justice.gov/usao-ndca/pr/former-uber-executive-sentenced-18-months-jail-trade-secret-theft-google (last visited Aug. 14, 2020).

In *Rodriguez*, a Social Security Administration ("SSA") employee accessed an SSA computer database to research information for personal reasons, in violation of agency policy. Rodriguez was convicted of computer fraud and appealed his conviction. On appeal, Rodriguez argued that he had not violated the CFAA because "he accessed only databases that he was authorized to use," although for improper purposes. *Id.* The Eleventh Circuit rejected Rodriguez's argument, holding that Rodriguez had "exceeded his authorized access and violated the [CFAA] when he obtained personal information for a nonbusiness reason." *Id.*

Citing to decisions in other circuits criticizing *Rodriguez*'s broad interpretation of the CFAA, Van Buren similarly argued that he should not be convicted under the CFAA because he was authorized to access the license-plate database, even though he did so for improper purposes. Van Buren having failed to identify binding precedent to support his position, however, the Eleventh Circuit applied the holding in *Rodriguez* and upheld Van Buren's conviction for computer fraud. *Van Buren*, 940 F.3d at 1208.

Van Buren petitioned the Supreme Court of the United States for a writ of *certiorari*, which the Court granted on April 20, 2020.

Issues on appeal and takeaways: The issue presented on appeal is "Whether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) of the Computer Fraud and Abuse Act if he accesses the same information for an unauthorized purpose." The Court's input on this issue is much needed, as it will – once and for all – resolve the current circuit split concerning whether the CFAA's language "exceed[] authorized access," should be extended to circumstances where access itself is authorized, but the purpose for access is not.

The Court's decision will have far-reaching implications as, among other things, it could potentially turn everyday activities, such as checking Facebook at work, into a felony. *Van Buren*, 940 F.3d at 1208 (discussing, *e.g.*, diverging decisions from the Second and Ninth Circuits).

2. *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019)

Background: hiQ Labs, Inc. ("hiQ") is a data analytics company that uses bots to scrape information from public LinkedIn profiles. Using a predictive algorithm, hiQ aggregates and analyzes that information to create "people analytics," which it then sells to businesses seeking to retain high-level talent and identify skill gaps in their workforces.

In May 2017, LinkedIn Corporation sent hiQ a cease-and-desist letter, asserting that hiQ's scraping activities violated LinkedIn's User Agreement and demanding that hiQ refrain from accessing and copying data from LinkedIn's server. The letter asserted that any future access of that type by hiQ would violate, *inter alia*, the CFAA, the Digital Millennium Copyright Act ("DMCA"), and California statutory and common law. The letter also indicated that LinkedIn had "implemented technical measures to prevent hiQ from accessing, and assisting others to

access, LinkedIn's site, through systems that detect, monitor, and block scraping activity." *hiQ Labs, Inc.*, 938 F.3d at 992.

hiQ filed suit in the United States District Court for the Northern District of California, seeking injunctive relief and a declaratory judgment that LinkedIn could not lawfully invoke the CFAA, DMCA, or California law against it. hiQ also filed a request for a temporary restraining order, which the parties later agreed to convert to a motion for preliminary injunction.

The district court granted hiQ's motion and ordered LinkedIn to withdraw its demand letter, to remove any technical barriers to hiQ's access to LinkedIn's public profiles, and to refrain from putting in place any legal or technical measures that would block hiQ's access to the public profiles.

LinkedIn appealed to the Ninth Circuit.

Holding and analysis: The Ninth Circuit affirmed the preliminary injunction. In addressing LinkedIn's CFAA claim – which, if successful, would preempt hiQ's state law claims that provided the basis for its preliminary injunction – the court found that hiQ had "raised serious questions about whether LinkedIn may invoke the CFAA[.]" *Id.* at 1004.

The issue turned on whether hiQ's scraping and use of LinkedIn's data *after* it received the cease-and-desist letter from LinkedIn was "without authorization" in violation of the CFAA.

Implementing the traditional tools of statutory construction, the court found that the CFAA, which must be narrowly construed under the rule of lenity, was enacted to prevent computer hacking (which the legislature had previously analogized to breaking and entering) and therefore, where the information is generally accessible to the public (*e.g.*, without requiring a password), the operative CFAA language "without authorization" is inapplicable.

In particular, the court stated:

> In recognizing that the CFAA is best understood as an anti-intrusion statute and not as a "misappropriation statute," [*United States v. Nosal*, 676 F.3d 854, 857-58 (9th Cir. 2012)], we rejected the contract-based interpretation of the CFAA's "without authorization" provision adopted by some of our sister circuits.

Id. at 1000 (comparing prior Ninth Circuit decisions with decisions from the First and Eleventh Circuits). The court continued:

> For all these reasons, it appears that the CFAA's prohibition on accessing a computer "without authorization" is violated when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer. It is likely that when a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA.

Id. at 1003.

Agreeing with the district court that hiQ had established each of the elements required for a preliminary injunction, the Ninth Circuit affirmed the lower court's decision and remanded for further proceedings. *Id.* at 1005.

Takeaways and petition for writ of *certiorari*: The Ninth Circuit has again narrowly interpreted the CFAA, this time holding that it does not prohibit the scraping and use of data from public websites. However, the Ninth Circuit's opinion reflects a departure from the approach taken by the Eleventh Circuit and, arguably, First Circuit, which have held that violations of contractual restraints can give rise to a claim for unauthorized access under the CFAA. *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583-84 (1st Cir. 2001); *Rodriguez*, 628 F.3d at 1263.

On March 9, 2020, LinkedIn filed a petition for writ of *certiorari*, asking the Supreme Court to weigh in on the issue. The Court requested a response from hiQ, which hiQ filed on July 25. It has yet to be seen whether the Court will grant *certiorari*, use *Van Buren* (see above) as a vehicle to clarify the scope of the CFAA, or neither. In the meantime, the *hiQ* decision has been held out as one of the most important web scraping cases to interpret CFAA liability and is frequently cited by web scrapers defending the legality of their actions.

Notably, the Ninth Circuit left the door open on other possible theories of recovery for victims of data scraping, including state law trespass to chattels, copyright infringement, misappropriation, unjust enrichment, conversion, breach of contract, and breach of privacy. *hiQ Labs, Inc.*, 938 F.3d at 1004. Indeed, the Eleventh Circuit recently held that using bots to scrape a publicly available database may constitute trade secret misappropriation under the DTSA and Florida Uniform Trade Secrets Act. *See Compulife Software Inc. v. Newman*, 959 F.3d 1288, 1312, 1315 (11th Cir. 2020) (vacating in part lower court's decision where the magistrate judge "failed to consider the important possibility that so much of the Transformative Database was taken—in a bit-by-bit fashion—that a protected portion of the trade secret was acquired" and finding that "the simple fact that the quotes taken were publicly available does not *automatically* resolve the question [of misappropriation] in the defendants' favor.") (emphasis in original).

III. RECENT LEGISLATIVE DEVELOPMENTS IN NONCOMPETES[6]

For over 200 years, employee noncompetes have been governed by state law. And all but three (California, North Dakota, and Oklahoma) allow the use of noncompetes.

[6] The information in this section is summarized from FairCompetitionLaw.com, specifically, "Federal Noncompete Initiatives: When you can't convince the states, ask the feds" (2019), https://www.faircompetitionlaw.com/2019/12/24/federal-noncompete-initiatives-when-you-cant-convince-the-states-ask-the-feds/ (last visited Aug. 21, 2020) and "Senators Warren and Murphy Again Push the FTC to Regulate Noncompetes" (2020), https://www.faircompetitionlaw.com/2020/08/02/senators-warren-and-murphy-again-push-the-ftc-to-regulate-noncompetes/ (last visited Aug. 21, 2020).

Over just the past several years, bills to modify noncompete laws have been introduced in over 30 states. More than 20 of those states have enacted legislation modifying their laws, some strengthening enforcement, and others making enforcement harder. Instructively, while many of the states have recently considered banning noncompetes, *not a single state has done so*. Rather, each state has evaluated the diverse needs of its workforce and industries, and reached a balance of interests that it determined appropriate for its population. For example, in 2015, Hawaii banned the use of noncompetes for workers in the technology field. No other state has followed its lead.

Nevertheless, the debate over this traditional state-law issue has spilled over to the federal level – in Congress (at both the House and the Senate) and at the Federal Trade Commission ("FTC"). Much of the push for restrictions or a ban is premised on (1) the mistaken belief that Silicon Valley is the epicenter of tech because California bans noncompetes; (2) recent preliminary, inconclusive, and somewhat inconsistent studies, the nuances of which are ignored; (3) the mistaken belief that trade secrets laws and nondisclosure agreements provide adequate protections for trade secrets; (4) the mistaken belief that noncompetes prevent employees from using their general skill and knowledge; and (5) the prevalence of abuses in the use and drafting of noncompetes. When the mistakes are corrected and the issues put in context, a reasonable balance is one that (like the recommendations in the Obama Administration's "Call to Action"[7]) bans noncompetes for low-wage workers and medical professionals, requires advance notice if a noncompete will be required, limits the ability to rectify overly broad noncompetes after the fact, and provides a meaningful remedy for companies that attempt to rely on less restrictive alternatives.

Federal Noncompete Regulatory Efforts

Recent federal noncompete reform efforts can be traced back to three bills filed in 2015. The first (the "Mobility and Opportunity for Vulnerable Employees Act" or "MOVE Act"), filed by Senator Chris Murphy (D-CT) and co-sponsored by then-Senator Franken and Senators Elizabeth Warren (D-MA), Richard Blumenthal (D-CT), and Sheldon Whitehouse (D-RI), sought to prohibit the use of noncompetes for "low-wage employees." The other two were the "Limiting the Ability to Demand Detrimental Employment Restrictions Act," which was very similar to the MOVE Act, and the "Freedom for Workers to Seek Opportunity Act," which sought to ban the use of noncompetes for grocery store workers (*only*). None of these bills passed.

A few years later, in April 2018, Senators Elizabeth Warren (D-MA), Chris Murphy (D-CT), and Ron Wyden (D-OR) introduced the Workforce Mobility Act of 2018 (S. 2782) to impose a federal ban on the use of employee noncompetes. A companion bill was introduced in the House by Representatives Joseph Crowley (D-NY), Linda Sanchez (D-CA), Mark Pocan (D-WI), Keith Ellison (D-MN), Jerrold Nadler (D-NY), and David Cicilline (D-RI), who were later joined by Janice Schakowsky (D-IL), and Alan Lowenthal (D-CA). That legislative session ended without action on either bill.

[7] "State Call to Action on Non-Compete Agreements" The White House (Oct. 15, 2016), https://obamawhitehouse.archives.gov/sites/default/files/competition/noncompetes-calltoaction-final.pdf (last visited Aug. 21, 2020).

More recently, in January 2019, Florida Senator Marco Rubio introduced the "Freedom to Compete Act" to amend the Fair Labor Standards Act of 1938 (29 U.S.C. 201, *et seq*.) to ban noncompetes for most nonexempt workers. And, on October 17, 2019, Senators Chris Murphy (D-CT) and Todd Young (R-IN) filed the "Workforce Mobility Act" to ban the use of virtually all employee noncompete agreements.

Congress: The House

Although no bill is presently pending before the House, on October 29, 2019, the United States House Committee on the Judiciary Subcommittee on Antitrust, Commercial, and Administrative Law held a hearing on "Antitrust and Economic Opportunity: Competition in Labor Markets."

Although a total of nine witnesses testified, the three who addressed noncompetes most directly and substantively were FTC Commissioner Noah Phillips, Dr. Evan Starr, and Dr. Robert Topel. Their testimony collectively and consistently established that, although sometimes abused, noncompetes, when used properly, serve legitimate purposes including "incentivizing investment in workers and protecting trade secrets – worthy goals in our increasingly knowledge-driven economy." In sum, the testimony made clear that a blanket ban can have serious unintended repercussions and, if any regulation is to be considered at the federal level, it needs to be a nuanced approach. As Commissioner Phillips explained, "[l]abor mobility [which might be affected to some extent by noncompetes] is a complex issue, and examining the inputs to it from both sides has a better chance of contributing to a thoughtful response that will improve the lot of American workers and the nation as a whole."

This concern is consistent with answers previously provided by FTC Chairman Simons to written questions from the Senate Committee on the Judiciary, in which Chairman Simons stated (as provided more fully, below), "In certain circumstances, narrowly tailored noncompete clauses can benefit competition. . . . Noncompete clauses also can encourage organizations to invest in employee training by reducing the risk that employees will take their new skills to a competitor."

No additional hearings have been announced. However, after finding consensus among the experts that noncompetes can be appropriate in some circumstances, Vice Chair Neguse suggested that the consensus path forward would be (as Dr. Starr suggested) to have the FTC commission a study to understand the full implications of noncompetes and craft a "surgical" solution, rather than a total ban.

Congress: The Senate

On November 14, 2019, the United States Senate Committee on Small Business and Entrepreneurship held a hearing on "Noncompete Agreements and American Workers."

The hearing started off and initially remained fairly moderate (including with Senator Rubio's framing of the issue and Senator Romney's questioning whether the issue even belongs at the

federal level). By the end, however, the focus of the hearing shifted toward a ban of all employee noncompetes.

The Federal Trade Commission

There have also been multiple recent efforts to push the FTC to regulate noncompetes (although one might question whether the FTC has the statutory power to address this issue).

These efforts appear to have arisen in response to an announcement by the FTC in June 2018 that it planned to "hold a series of public hearings on whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection enforcement law, enforcement priorities, and policy." Although the FTC did not at that time mention noncompetes, it did state that it was taking public comments through August 20, 2018.

Not surprisingly, the Open Markets Institute ("one of the most influential drivers of Democratic politics," according to Politico) submitted a statement urging the FTC to (among other things) "restrict or prohibit non-compete agreements that impair worker mobility and depress wages." A few weeks later (September 5, 2018), Congressmen Mark DeSaulnier (D-CA), Mark Pocan (D-WI), and Donald Norcross (D-NJ), and Congresswoman Debbie Dingell (D-MI) issued so-called "findings and policy recommendations," entitled, "The Future of Work, Wages, and Labor." The recommendations covered many topics (including labor unions, minimum wage, universal basic income, the government as an employer of last resort, wealth taxes, etc.) and called for (among other things) a ban of all noncompetes "in employment contracts, with exceptions for senior executives who possess trade secrets."

The next day (September 6, 2018), FTC Commissioner Rohit Chopra issued a written comment stating, "Given the paucity of private litigation challenging noncompete agreements as antitrust violations, the FTC might consider engaging in rulemaking on this issue. A rule could remove any ambiguity as to when noncompete agreements are permissible or not."

On October 3, 2018, the Senate Committee on the Judiciary submitted questions to FTC Chairman Simons. Chairman Simons responded on November 6, 2018. In one of his responses, Chairman Simons stated:

> In certain circumstances, narrowly tailored noncompete clauses can benefit competition. For example, noncompete clauses can protect against the disclosure or use of competitively sensitive information outside of an employer's organization. Noncompete clauses also can encourage organizations to invest in employee training by reducing the risk that employees will take their new skills to a competitor. That said, several private suits have alleged that overly broad employee restrictions can violate the antitrust laws.

In March 2019, seven Senators (Richard Blumenthal (D-CT), Ben Cardin (D-MD), Sherrod Brown (D-OH), Elizabeth Warren (D-MA), Edward Markey (D-MA), Chris Van Hollen (D-MD), and Amy Klobuchar (D-MN)) petitioned the FTC to ban noncompetes, calling them "these

insidious little clauses" and a "scourge . . . rigging our economy against workers." At about the same time, OMI once again – this time enlisting other advocacy organizations, labor unions, individuals, and academics – petitioned the FTC (in apparent coordination with the Senators), demanding the complete ban of noncompetes.

The Senators' letter and OMI's petition are both premised on the same mistaken assumptions permeating the noncompete debate overall (for example, the mistaken assumption that Silicon Valley resulted simply because noncompetes are banned in California), ignoring conflicting research and the significant potentially harmful unintended consequences of a potential ban. Perhaps most telling, however, the OMI petition goes so far as to seek to ban all noncompetes premised in part on the radical view that sharing other people's trade secrets may be justifiable. Specifically, the petition states, "Even accepting that firms principally use non-competes to protect their intangibles, information sharing is not a categorical 'evil' that state action should police at any cost. What is disparaged as free riding often is the broad dissemination of knowledge that contributes to economic growth and innovation." Such a position is directly at odds with the reasons Congress passed the Defend Trade Secrets Act of 2016.

On June 12, 2019, the FTC held "Hearing #14: Roundtable with State Attorneys General," during which, in response to a question about whether the FTC should look at noncompetes, Eric Newman (Chief Litigation Counsel for the Antitrust Division of the Washington State Attorney General's Office) responded, "Sure." He then elaborated on what Washington state had done, noting that Washington "just had a statute passed that made them illegal for low-wage workers and really up to $100,000 a year," and continued, "So I think that is a really effective way of getting in front of it obviously, is just outlawing it completely."

Joining the bandwagon on July 15, 2019, 18 state attorneys general – most of them from states that have made or considered moderate changes to their noncompete laws – also petitioned the FTC to investigate noncompetes.

By September 18, 2019, "[t]he Federal Trade Commission [had] deemed evidence on worker non-competes insufficient to justify a rulemaking, . . . but [determined that] the agency w[ould] continue to pursue action against such clauses." Thereafter, Chairman Simons was pushed by Senator Blumenthal to move forward on rulemaking. Specifically, in a series of written questions to and answers by Chairman Simons, Senator Blumenthal stated, "While non-compete agreements can help protect employers and incentivize investments in workers, too often they are used to stifle competition. I was disappointed to hear that the Commission found insufficient evidence in its literature review to justify a rulemaking. Nevertheless, I am glad that the FTC is hosting a workshop on this issue . . . and is seeking additional evidence to support a rulemaking."

On November 15, 2019, some of the same state attorneys general who submitted the July 15, 2019 public comments wrote a new, sterner letter. Four attorneys general (from Hawaii, Nevada, New Jersey, and New York) who signed the July 15 comments did not join in the new letter, though attorneys general from New Mexico, North Carolina, Oregon, Vermont, and Wisconsin (who had not been on the July letter) signed onto this new one. This newly constituted group summarily rejected (despite the studies to the contrary) the notion that noncompetes serve legitimate purposes and contended that nondisclosure agreements and trade secrets laws are

sufficient to protect trade secrets – a position that most trade secrets lawyers (who would be a beneficiary of the increased, costly litigation that would result) would dispute. In the end, these attorneys general called for the FTC to ban noncompetes – and to give them a timeline to complete the work.

On December 5, 2019, the FTC announced that it would be conducting a "Workshop on Non-Compete Clauses Used in Employment Contracts" on January 9, 2020.

Following the January 9 workshop, the FTC received 328 submissions answering several questions that the FTC had posed. Those submissions provided myriad varied perspectives, ranging from strong support for the FTC to claim authority and ban noncompetes to strong support to leave the regulation to the states.

More recently, a July 31, 2020, press release from Senator Elizabeth Warren's office reported by Framingham Source indicates that the issue has taken on a renewed urgency for Senators Warren and Murphy. According to the press release, Senators Warren and Murphy state, "The threat of non-compete agreements both during and after the economic crisis precipitated by the COVID-19 pandemic has put millions of workers in an untenable position. We urge the FTC to immediately move forward with its Commission Rule to restrict non-compete agreements, and we ask that the agency pursue emergency action to limit the enforcement of non-compete agreements during and after the COVID-19 public health emergency . . . ."

According to the press release, Senators Warren and Murphy premise their request on the (mistaken) assertion that "[n]on-compete agreements give employers undue power in the employer-employee relationship, allowing them to cut wages, decrease benefits, or subject workers to inhospitable environments without fear of their employees leaving for a competitor."

Senators Warren and Murphy requested a response no later than August 4, 2020. As of August 20, 2020, the FTC had not acted.