JONES DAY | One Firm Worldwide®

WHITE PAPER

July 2020

Mid-Year Review of Key Global Trade Secret Developments

A trade secret is any information used in one's business that derives independent economic value from being kept secret. Unlike patents, trade secrets are protected indefinitely for as long as they remain a secret. In the United States, the enactment of the Defend Trade Secrets Act ("DTSA") in 2016 has made trade secrets an increasingly attractive form of intellectual property for businesses hoping to protect their innovations. And in other jurisdictions, developments such as Germany's Company Secret Act and recent amendments to China's Anti-Unfair Competition Law are similarly refining trade secret laws.

This *White Paper* summarizes and explains recent noteworthy decisions in trade secret law and updates around the world in the first half of 2020. Each of these decisions has meaningful implications for trade secret owners, defendants, and practitioners alike.

TABLE OF CONTENTS

UNITED STATES

Courts Continue to Refine Trade Secret Misappropriation Standards

***Advanced Fluid Systems, Inc. v. Huber*, Nos. 19–1722, 19–1752, 2020 WL 2078298 (3d. Cir. Apr. 30, 2020)**

The Third Circuit recently recognized a trade secret misappropriation claim by a party *possessing*, but not *owning*, the trade secret. Advanced Fluid Systems, Inc. ("AFS") sued its former employee, Kevin Huber, and several competitors for trade secret misappropriation. Huber allegedly stole confidential information from AFS, first for the benefit of an AFS competitor, Livingston and Haven, LLC ("Livingston"), and then for a company Huber created, Integrated Systems and Machinery, LLC ("Integrated").[1] After a Pennsylvania district court found in favor of AFS at the summary judgment stage, Huber, Livingston, several Livingston employees, and Integrated (together, "Appellants") appealed.[2]

Appellants argued, in part, that AFS's misappropriation claim must fail because AFS did not "own" the asserted trade secrets.[3] In fact, ownership of the confidential information at issue was explicitly spelled out in a contract between AFS and another party, the Virginia Space Flight Authority ("Authority"). All materials generated under the contract were to be deemed "work for hire" and the Authority's "exclusive property."[4]

The Third Circuit found Appellant's argument unpersuasive. It noted that "while ownership of the sort traditionally associated with real or personal property is *sufficient* to maintain a trade secret misappropriation claim. . ., it is not a *necessary* condition."[5] Indeed, the relevant language of Pennsylvania's Uniform Trade Secrets Act ("PUTSA") lacks any ownership requirement whatsoever.[6] A plaintiff "need only demonstrate *lawful possession* of a trade secret," not ownership in its traditional sense, to maintain such a claim.[7] Implementing a *per se* ownership requirement for misappropriation claims "is flawed since it takes account neither of the substantial interest that lawful possessors of the secrets have in the value of that secrecy, nor of the statutory language that creates the protection for trade secrets while saying nothing of ownership as an element of a claim for misappropriation."[8]

***Compulife Software Inc. v. Newman et al.*, No. 18–12004, No. 18–12007, 2020 WL 2549505 (11th Cir. May 20, 2020)**

According to the Eleventh Circuit, using bots to webscrape a publicly available database may constitute trade secret misappropriation under Florida's version of the Uniform Trade Secrets Act ("FUTSA") and the federal DTSA.[9]

Plaintiff Compulife Software, Inc. ("Compulife") and defendants are direct competitors in a niche industry: generating live insurance quotes.[10] Compulife's main product is a "Transformative Database" containing up-to-date information on many life insurers' premium-rate tables. Although Compulife's database is based on publicly available information, it cannot be replicated without a confidential method and formula.[11] Compulife sells access to this database to life insurance agents, and also provides free access to consumers through its website.[12] When an individual gets a quote from the website, the site automatically refers that individual to an insurance agent who pays to partner with Compulife.[13]

Defendants also operate life insurance quote websites. Defendants' products function similarly to—and, in some cases, are copied from—Compulife's database and website.[14] In addition to copying portions of Compulife's source code (which is undisputed), defendants also allegedly hired a hacker to run automated queries on Compulife's website. These hundreds of thousands of queries "scraped" data from Compulife's database to use as the basis for generating quotes on defendants' own websites.[15]

Compulife filed suit in the Southern District of Florida alleging, among other claims, that defendants misappropriated a trade secret by scraping data from Compulife's website.[16] Finding against Compulife on its misappropriation claim, the district court magistrate judge held that, while the underlying Transformative Database is a trade secret, the individual quotes are not.[17] Thus, Compulife's FUTSA and DTSA claims alleging misappropriation of these quotes "necessarily fail[ed]."[18]

On appeal, the Eleventh Circuit reversed. It found that "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."[19] While "[t]he magistrate judge was correct to conclude that the scraped quotes were not *individually* protectable trade secrets because each is readily available to the public, . . . that doesn't in and of itself resolve the question whether, in effect, the database *as a whole* was misappropriated."[20]

The Eleventh Circuit did not opine whether trade secret misappropriation actually occurred. It "merely clarif[ied] that the simple fact that the quotes taken were publicly available does not *automatically* resolve the question in the defendants' favor."[21] As such, the appellate court remanded the trade secret misappropriation claim to the district court.

To Resolve Discovery Issues and Abuses, Courts Order Third-Party Examination of Source Code and Enter Default Judgment for Spoliation

***Tesla, Inc. v. Guangzhi Cao*, Case No. 19–cv–01463 (N.D. Cal. May 27, 2020)**

A California federal court ordered a Chinese self-driving car company to allow a neutral third party to examine its source code and logs in a trade secret misappropriation case initiated by Tesla, Inc. ("Tesla").

Tesla sued former engineer Guangzhi Cao, alleging he downloaded Tesla's Autopilot-related source code before joining autonomous vehicle start-up Xiaopeng Motors Technology Company Ltd. ("XMotors") in early 2019.[22] During discovery, Tesla subpoenaed third-party XMotors to produce "(i) [XMotors'] autonomous driving source code. . .; (ii) certain source-code related logs; (iii) forensic images of workplace computers used by various XMotors employees. . .; (iv) forensic images of workplace computers used by individuals who are not employees of XMotors; and (v) confidential documents produced by XMotors in response to [a] . . . criminal investigation involving an individual formerly employed by XMotors."[23] XMotors moved to quash Tesla's subpoena, calling it "a fishing expedition" at best, and at worst, "nothing more than an attempt to gain competitive advantage or to simply harass a competitor."[24]

The Northern District of California disagreed with XMotors, at least with respect to some of Tesla's requests. The court ordered XMotors to produce the requested source code and source code logs, as the "information is relevant to Tesla's claim that Cao disclosed Tesla's trade secrets to XMotors."[25] Recognizing the confidential nature of the source code, the court instructed Tesla and XMotors to meet and confer "regarding whether a neutral third party should examine the source code in the first instance."[26]

The court also ordered XMotors to produce the requested forensic images of its laptops and work computers, except those belonging to nonemployees. And it further granted XMotors's motion to quash with respect to the pending criminal investigation documents, noting that the relevance of the grand jury materials to Tesla's claims against Cao was "speculative and tenuous."[27]

***WeRide Corp. v. Huang*, No. 18–cv–07233, 2020 WL 1967209 (N.D. Cal. Apr. 24, 2020)**

According to a Northern District of California court, the failure to adequately preserve electronically stored information ("ESI") in a trade secrets litigation can lead to case-ending sanctions.

In another autonomous vehicle case, *WeRide Corp. v. Huang*, plaintiffs WeRide Corp. and WeRide Inc. (collectively "WeRide") sued Zhong Zhi Xing Technology Co. Ltd. ("ZZX"), AllRide.AI, Inc. ("AllRide"), WeRide's former CEO Jing Wang, and WeRide's former Director of Hardware Kun Huang alleging trade secret misappropriation of its autonomous vehicle source code.[28] WeRide filed its original complaint in November 2018 and then moved for a preliminary injunction one month later.[29] In March 2019, the court granted the motion for preliminary injunction as to Huang and AllRide.[30] The preliminary injunction specifically prohibited the enjoined parties 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 are related to WeRide's confidential material or information, or AllRide's source code.[31]

In August 2019, the parties were scheduled to appear for a discovery conference to resolve multiple motions to compel filed by WeRide. On the eve of the conference, AllRide's counsel notified the court that in mid-June 2019, it discovered it failed to disable an auto-delete setting on its email server.[32] This oversight led to a companywide destruction of emails predating mid-March 2019.[33] After a court-ordered investigation into the extent of the document destruction, WeRide moved

for sanctions against the defendants based on the spoliation of evidence.

The court found that AllRide's "staggering" spoliation of evidence—including a mass destruction of emails, deleted email accounts, and wiped laptops—demonstrated both willfulness and bad faith. And it greatly prejudiced WeRide's ability to establish its claims for trade secret misappropriation.[34] The court thus issued "terminating sanctions" against AllRide and AllRide's CEO, Wang, striking their answers and entering defaults against them.[35] Finding defendant Huang also "spoliated critical evidence," the court similarly issued terminating sanctions against him.[36]

District Court Examines Extraterritoriality of the DTSA

***Motorola Solutions, Inc. v. Hytera Communications Corp.*, 1:17–cv–1973, 2020 WL 967944 (N.D. Ill. Jan. 31, 2020)**

In one of the first cases to explicitly analyze the DTSA's extraterritorial reach, an Illinois district court confirmed the DTSA allows private litigants to pursue claims of misappropriation that occur outside of the United States if there is some conduct that occurs domestically in furtherance of the theft.

Plaintiff Motorola Solutions, Inc. ("Motorola") sued several Hytera entities (collectively, "Hytera") in the Northern District of Illinois, asserting trade secret claims under both the DTSA and Illinois Trade Secret Act.[37] In essence, Motorola alleged that: (i) Hytera hired three engineers away from Motorola's Malaysian office; (ii) those engineers stole and brought with them thousands of Motorola's confidential documents; and (iii) Hytera used those documents to develop a state-of-the-art digital radio functionally indistinguishable from Motorola's radios.[38] Hytera then sold those radios worldwide, including in the United States.[39]

In a motion to preclude Motorola from relying on extraterritorial damages, Hytera argued, in part, that neither the DTSA nor Illinois Trade Secret Act has extraterritorial effect, so all damages should be limited to only domestic applications of the respective statutes.[40] The court disagreed with respect to Motorola's DTSA claim. Recognizing that the DTSA does not contain an explicit reference to extraterritorial conduct, the district court interpreted the DTSA in light of "the statute as a whole."[41] Specifically, the court relied on Section 1837 of the Economic Espionage Act—an extraterritorial provision that, prior to the enactment of the DTSA, covered only criminal proceedings.[42] It noted: "The biggest indicator that Congress did intend for the private right of action of the DTSA to apply extraterritorially is the fact that Section 1837 refers broadly to 'this chapter,' which includes within it [the DTSA's] Section 1836."[43]

Therefore, the court held the DTSA may apply extraterritorially in a private cause of action if either of the requirements of Section 1837 is met.[44] In this case, the court applied the "act in furtherance" requirement, limiting the circumstances under which the DTSA applies to those with a nexus to the United States.[45] The court found that the requirement had been met by Hytera's advertisement, promotion, and marketing of the products embodying the stolen trade secrets in the United States.[46] Therefore, Motorola was free to "argue for extraterritorial damages resulting from the misappropriation, but only those damages that occurred after the effective date of the [DTSA]—May 11, 2016."[47]

SCOTUS to Define "Exceeds Authorized Access" Under the Computer Fraud and Abuse Act

***United States v. Van Buren*, 940 F.3d 1192 (11th Cir. 2019), *cert. granted*, 2020 WL 1906566 (Mem.) (U.S. Apr. 20, 2020)**

The U.S. Supreme Court has agreed to review the Computer Fraud and Abuse Act ("CFAA") in order to resolve a federal circuit split about the scope of statute.[48] The CFAA makes it a federal crime to "access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] information from any protected computer."[49] Under the Act, to "exceed[] authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[50] These provisions present a recurring question on which appellate courts are openly divided: Does a person who is authorized to access information on a computer for *certain* purposes violate the CFAA if he or she accesses the same information for an *improper* purpose?[51]

The Eleventh Circuit seems to think so. In the underlying case, defendant Van Buren was a police sergeant who used his access as an officer to search an official license plate database in exchange for money.[52] He was convicted under the provisions of the CFAA detailed above. Appealing the conviction, Van Buren argued he did not violate the CFAA because he did not "exceed[] authorized access" under the

statute.[53] Indeed, he accessed only databases he was authorized to use, even though he did so for an improper reason.[54] Recognizing that other circuits reject its line of reasoning, the Eleventh Circuit upheld Van Buren's conviction. Because Van Buren accessed the database for "inappropriate reasons," the appellate court affirmed the lower court's holding that he "exceed[ed] authorized access" under the statute.[55]

Van Buren then petitioned the Supreme Court, noting the circuit split surrounding the proper interpretation of the CFAA provisions.[56] The Court granted the petition to determine "[w]hether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) of the [CFAA] if he access the same information for an improper purpose."[57]

While the *Van Buren* case does not directly involve trade secrets, the Court's interpretation of the CFAA will have implications in this sector. Although primarily a criminal statute, the CFAA also includes a private right of action allowing a person who is injured by a CFAA violation to sue for damages or equitable relief.[58] And many cases involving the CFAA arise out of trade secret disputes where a defendant uses authorized credentials to obtain computer access to sensitive company information.

Sixth Circuit Finds Default Judgment of Willful and Malicious Trade Secret Misappropriation Not Dischargeable in Bankruptcy Proceeding

***In re Hill*, 957 F.3d 704 (6th Cir. 2020)**

The Sixth Circuit affirmed that a state court's default judgment of "willful and malicious" trade secret misappropriation against a debtor is not dischargeable in a Chapter 7 bankruptcy proceeding. In that case, Aaron Hill and other principals of First Meridian Mortgage Corp. ("First Meridian") agreed to sell First Meridian to CMCO Mortgage, LLC ("CMCO"), where the former principals would build and manage an internet division.[59] More than a year later, Hill received an offer of employment from CMCO's competitor, Peoples Bank, which he accepted. CMCO thereafter terminated Hill, alleging that he breached his contract, provided trade secrets to Peoples Bank, and unlawfully recruited CMCO employees.[60] CMCO then sued Peoples Bank and Hill on a variety of theories, including trade secret misappropriation.[61]

Peoples Bank originally paid for Hill's legal representation, but after settling all claims with CMCO, it notified Hill that it would no longer fund his representation. Hill eventually proceeded *pro se* but "generally declined to participate in the action."[62] "Most importantly, Hill failed to attend the pretrial conference. . . , resulting in the state court granting CMCO's motions for sanctions and entry of a default judgment on the claims set forth in its complaint."[63] As a part of its findings of fact, the state court noted that "Hill's actions . . . were willful, intentional, in bad faith, egregious, and done with malice."[64] Hill then failed to appear for the damages trial, and the state court entered a money judgment against him in the amount of almost $3.5 million in compensatory damages.[65]

Between the damages trial and the entry of final judgment in favor of CMCO, Hill filed a chapter 7 bankruptcy petition in the U.S. Bankruptcy Court for the Western District of Kentucky. CMCO filed a proof of claim in the bankruptcy court, which lifted the automatic stay with respect to the money judgment.[66] CMCO then filed an adversary proceeding against Hill, seeking a determination that the debt owed by Hill to CMCO was nondischargeable. Specifically, 11 U.S.C. § 523(a)(6) recites that an individual debtor is *not* discharged from any debt "for willful and malicious injury by the debtor to another entity."[67] Because the state court found Hill's misappropriation "willful" and "done with malice," CMCO argued the $3.5 million judgment was not dischargeable under § 523(a)(6). The bankruptcy court granted CMCO's motion on collateral estoppel grounds.[68] Hill appealed to the district court, which affirmed, and then to the Sixth Circuit.

On appeal, Hill contended, in part, that collateral estoppel did not apply because he was denied an opportunity to be heard. But the appellate court disagreed, noting that "Hill had his opportunity to litigate the claims against him but instead chose not to appear."[69] Indeed, "Kentucky courts will apply preclusive affect (sic) to default judgments such that they are considered 'actually litigated' for the purposes of collateral estoppel."[70] After reviewing the other elements of collateral estoppel, the court affirmed that Hill's debt to CMCO was the result of "willful and malicious injury" such that Hill is precluded from arguing his debt is dischargeable in bankruptcy.[71]

Reasonable Royalty Damages and Attorneys' Fees

***Ajaxo, Inc. v. E*Trade Financial Corp.*, 261 Cal.Rptr.3d 583 (Cal. Ct. App. 2020)**

In the newest addition to a 20-year saga between Ajaxo and E*Trade, a California appellate court affirmed the lower court's denial of a reasonable royalty to Ajaxo for trade secret misappropriation.[72] Thus, despite prevailing on the merits, Ajaxo was unable to recover damages. The dispute arose in 1999 when Ajaxo offered to license its wireless trading platform to E*Trade. After numerous discussions between the parties, a mutual nondisclosure agreement, and several Ajaxo technology demonstrations, E*Trade declined to license Ajaxo's software.[73] Shortly thereafter, E*Trade entered into an agreement with a different wireless vendor, Everypath, Inc. ("Everypath"). Everypath worked with E*Trade to develop and implement wireless trading technology "almost identical to" Ajaxo's platform.[74]

Ajaxo sued E*Trade and Everypath in October 2000, asserting trade secret misappropriation and breach of contract claims. In the first trial, Ajaxo relied on an unjust enrichment measure of damages for its misappropriation claim.[75] The trial court granted a partial motion for nonsuit on the issue, however, finding that Ajaxo had presented insufficient evidence of unjust enrichment by E*Trade and Everypath.[76] Due to the nonsuit, the jury declined to award damages on the trade secret claim, even though it found both E*Trade and Everypath liable for trade secret misappropriation.[77] The trial court also denied Ajaxo's claim for injunctive relief. Ajaxo appealed and the appellate court reversed and remanded, holding the trial court erred in granting a nonsuit for the misappropriation claim.[78]

In the remanded trial, the jury again awarded no damages for the trade secret claim. The jury found E*Trade's benefit from the misappropriation to be vastly outweighed by its expenses in achieving the benefit, resulting in no net damages to Ajaxo. Ajaxo then asked the court to award reasonable royalties under California's UTSA ("CUTSA"), which provides that "[i]f neither damages nor unjust enrichment caused by misappropriation are provable, the court may order payment of a reasonable royalty for no longer than the period of time the use could have been prohibited."[79] The trial court denied the request, finding that Ajaxo's unjust enrichment claim *was* "provable," making a royalty award unavailable. Indeed, Ajaxo *had* proven unjust enrichment damages, just with no net amount recoverable.[80]

Ajaxo appealed again, and the appellate court reversed the second trial court's ruling.[81] In so holding, the appellate court noted "[t]o refuse to consider a reasonable royalty where liability had been proven but the defendant had not made a profit would ignore the fact that a defendant might achieve nonpecuniary benefits from stealing a trade secret."[82] Accordingly, "where a defendant has not realized a profit or other calculable benefit as a result of his or her misappropriation of a trade secret, unjust enrichment is *not provable* within the meaning of [the CUTSA]."[83] The appellate court thus remanded for an evaluation of Ajaxo's reasonable royalty claims.

On remand in September 2015, the third trial court found that Ajaxo failed to prove it was entitled to an award of royalties from E*Trade.[84] According to the court, Ajaxo's royalty theory was "excessive," not reasonable, and not tethered to E*Trade's misappropriation.[85] Further, the court noted Ajaxo "acted with unclean hands in destroying evidence during the pending litigation."[86] (Ajaxo's CEO allegedly destroyed a hard drive containing confidential source code with a hammer during one of the earlier trials.)[87] Such evidence, E*Trade's expert testified, was necessary in order to identify the trade secret and to apportion its value in a reasonable royalty inquiry.[88]

Ajaxo initiated its third appeal, but this time, the appellate court affirmed the trial court's decision. The panel noted: "We find nothing erroneous or contradictory in the trial court's application of apportionment principles to the reasonable royalty analysis," adding that there is "ample support in the record for these findings. Ajaxo's contention that the trial court erred in considering E-Trade's 'unclean hands' or spoliation arguments because they were rejected at other points in the litigation is without merit."[89] The appellate court also ruled that Ajaxo misinterpreted its remand orders to the trial court. The CUTSA does not—as Ajaxo argued—*guarantee* recovery "of a royalty where actual losses and unjust enrichment are not provable" but provides only that the court "*may*" do so.[90] The court ultimately affirmed the trial judge's decision to award no damages.

***Insurent Agency Corp., et al. v. The Hanover Insurance Co., et al.*, No. 16–cv–3076, 2020 WL 86813 (S.D.N.Y. Jan. 8, 2020)**
To succeed on a motion for attorneys' fees under the DTSA, the Southern District of New York required the prevailing party to establish that the claim was wholly without merit.

Plaintiffs Insurent Agency Corporation and RS Holdings Corporation (collectively "Plaintiffs") filed a single-claim complaint against The Guarantors Agency ("Guarantors") and its insurance carrier, The Hanover Insurance Company ("Hanover"). Plaintiffs alleged Hanover and Guarantors were using certain copyrighted legal agreements that appeared to be identical to those used by Plaintiffs in their own business.[91] After discovering that a former employee left to join Guarantors, Plaintiffs amended their complaint to add state and federal trade secret misappropriation claims.[92] Hanover eventually prevailed on all asserted claims—some on motions to dismiss and others on summary judgment.[93]

Hanover subsequently moved to recover attorneys' fees. Under the DTSA, a court *may* "if a claim of the misappropriation is made in bad faith, . . . award reasonable attorney's fees to the prevailing party."[94] Although the court recognized Hanover as a "prevailing party," it declined to award attorneys' fees.[95] In so holding, the court noted "the record d[id] not indicate that Plaintiffs' DTSA claim was meritless or brought for improper purposes." Instead, "Plaintiffs' trade secret misappropriation claim failed as a matter of *proof*."[96] Because Plaintiffs' claim was not "wholly without merit and brought in bad faith," Hanover's motion to recover attorneys' fees under the DTSA was denied.[97]

Trade Secret Enforcement at the ITC

The U.S. International Trade Commission ("ITC") has long been popular as a venue for patent litigants to seek to exclude entry of allegedly infringing goods into the United States based on 19 U.S.C. § 1337 (commonly known as § 337), which precludes importation of articles that infringe a valid patent or a valid registered copyright.[98] Similar provisions also protect trademarks, semiconductor masks, and boat hull designs, all of which possess domestic statutory protection.[99] However, because trade secret claims were historically creatures of common law, § 337 lacks a specific provision precluding importation of articles developed through theft of a trade secret. Nevertheless, the ITC has held since at least 1979 that the catchall provision of § 337(a)(1)(A)—which applies to any "*unfair methods of competition and unfair acts* in the importation of articles"—includes trade secret claims, and the Federal Circuit has upheld this determination.[100]

Despite this early establishment of jurisdiction, trade secret cases before the ITC have historically been rare: Only five cases were brought during the years 2000–2009 and only 12 during the years 2010–2018. But, as in other forums, the interest in litigating trade secrets claims before the ITC has risen sharply recently in the wake of passage of the DTSA: Six cases were filed in 2019 alone (although none so far in 2020). For this reason, a few points on the differences in the legal standards for trade secrets cases before the ITC may be of interest.

Notably, the "domestic industry" requirement of "significant investment" or "substantial employment" found in § 337(a)(2) does not apply to the catchall provision, which recites only "an industry in the United States." This more lenient requirement may be satisfied by domestic industries which demonstrate "significant investment" or "substantial employment," but may also be satisfied by a "more flexible 'realities of the marketplace' test."[101] Conversely, § 337(a)(1)(A) has an additional requirement not found in patent cases: that the effect of the importation be to, inter alia, "destroy or substantially injure" the industry in question. Injury may be shown based on either actual injury or threat of injury, and the inquiry is based on a substantive economic analysis.[102]

Lastly, unlike exclusion orders based on patent infringement, which generally continue in effect until the expiration of the patent, "the Commission bases the time period of a limited exclusion order [for trade secret infringement] on a 'reasonable research and development period' or an 'independent development time' for the trade secrets at issue."[103] In practice, this has yielded durations between five and 25 years.[104]

The DOJ Continues to Pursue Charges Under the Economic Espionage Act

In the first half of 2020, the U.S. Department of Justice ("DOJ") continued to pursue Economic Espionage Act ("EEA") charges as part of the China Initiative it announced in 2018. One of the Initiative's key goals is to "[i]dentify priority trade secret cases, ensure that investigations are adequately resourced, and work to bring them to fruition in a timely manner." To that

end, DOJ announced indictments in two high-profile theft of trade secrets cases with a nexus to China, and secured a significant prison sentence for a Chinese national in another.

***United States v. Zhiyong et al.*, 1:20–cr–00046 (N.D. Ga. 2020)**
On January 28, 2020, DOJ obtained a sealed indictment of four Chinese nationals (Wu Zhiyong, Wang Qian, Xu Ke, and Liu Lei) who are alleged to be affiliated with the Chinese military, in connection with one of the largest data breaches in U.S. history.[105] The indictment was unsealed on February 10, 2020. The defendants are alleged to have hacked into the computer network of Equifax, one of the three largest credit reporting agencies in the United States, and stolen proprietary data compilations that included the personal identifying information ("PII")—such as Social Security numbers, names/dates of birth, driver's license numbers, and credit card numbers—for approximately 45% of the U.S. population.[106] The defendants are also charged with conspiracy, theft, and attempted theft of trade secrets under the EEA. Notably, the attempt and conspiracy charges allow the government to secure a conviction without establishing the existence of a trade secret, as long as it can establish beyond a reasonable doubt that the defendants *believed* they were targeting trade secret information.[107]

Attorney General Barr characterized the breach as part of a "disturbing and unacceptable pattern" of state-sanctioned hacks of American computer systems and information, and the indictment as a warning to those countries who support such acts.[108] As long as all four defendants remain in China, however, it is difficult to predict whether or when they will have to answer these charges.

***United States v. Tan*, 4:19–cr–00009–GKF (N.D. Okla. 2019)**
On February 27, 2020, Chinese national Hongjin Tan was sentenced to two years in prison for stealing trade secrets worth approximately $1 billion from his employer, Phillips 66. Tan had worked as a scientist on research and development of next-generation battery technologies for stationary energy storage applications, specifically flow batteries. He resigned in December 2018, claiming that he was returning to China to be with family and that he did not yet have a new job offer. The company reviewed Tan's computer activity and discovered that he had accessed and copied hundreds of files containing trade secret research and marketing information without permission to do so. A search of Tan's company laptop computer uncovered an employment agreement with a Chinese competitor of Phillips 66 that offered Tan a bonus for providing the Chinese company with certain information.[109]

In January 2019, Tan was indicted on one count each of unauthorized transmission, unauthorized possession, and theft of trade secrets, in violation of 18 U.S.C. § 1832(a)(1), (a)(2), and (a)(3).[110] In November 2019, Tan pled guilty to all three charges pursuant to a plea agreement.[111]

On February 27, 2020, District Judge Gregory Frizzell sentenced Tan to 24 months' imprisonment, three years of supervised release, $150,000 in restitution, and a $300 special assessment. Pursuant to the plea agreement, Tan also agreed to submit to deportation proceedings.[112]

GERMANY

Germany introduced its Company Secret Act (*Geschäftsgeheimnisgesetz*) ("Act") in April 2019. The Act was overdue because the underlying EU Directive 2016/943 required implementation by June 2018. Previously, trade secrets were typically protected in Germany only under brief provisions in the Act against Unfair Competition. The Act's definition of "trade secret": (i) permits a trade secret to be lawfully acquired by observation, study, disassembly, or testing of a product or object that has been made available to the public (i.e., so-called "reverse engineering"); and (ii) requires that reasonable steps have been taken to keep the information secret.

The Act introduced a specific type of litigation to resolve disputes on trade secrets (*Geschäftsgeheimnisstreitsachen*). Irrespective of the amount of controversy, these disputes are to be brought before the district courts (*Landgerichte*). Upon application by either party, the court can categorize certain information as "confidential," which in turn will oblige process participants (i.e., the parties and their lawyers, witnesses, and expert witnesses) to observe specific confidentiality obligations. In addition, court hearings may be nonpublic, which is very exceptional under German procedural law.

CHINA

Under China's general rules of evidence, the plaintiff has the burden to prove all elements of the offense. Coupled with the lack of a common law discovery system and strict rules on evidence collection by private parties, it has been challenging to pursue trade secret cases in China. However, China's recent legal reforms, including amendments to the Chinese Anti-Unfair Competition Law ("CAUCL"), have introduced changes that ease the burden on trade secret owners in misappropriation cases.

This section of the *White Paper* will first briefly examine several new Chinese laws and regulations and then review two recent trade secret cases that reveal how Chinese courts apply the reverse burden of proof.

The Chinese Anti-Unfair Competition Law

Burden of Proof

Under Article 32 of the CAUCL, "where the trade secrets owner provides prima facie evidence that he has taken confidential measures to protect the claimed trade secrets and that the trade secrets have been infringed, [then] the alleged infringer must prove that the trade secrets claimed by the owner do not constitute trade secrets." For information to be protected as a trade secret: (i) it must be nonpublic; (ii) it can bring economic benefits to the owner and is practical; and (iii) the owner must have adopted confidentiality measures to protect it. Hence, the defendant needs to prove that the claimed trade secret does not meet at least one of these three elements.

Article 32 also provides that "where the owner of the trade secrets provides prima facie evidence reasonably indicating that the trade secrets have been infringed and provides one of the following as evidence, the alleged infringer should prove that he has not infringed the trade secrets:

1. Evidence indicating that the alleged infringer had access to the trade secrets or had an opportunity to obtain the trade secrets and that the information used is substantially the same as the trade secrets; or
2. Evidence indicating that the trade secrets have been disclosed, have been used or are at risk of being disclosed or used by the alleged infringer."

Finally, Article 32 seems to allow trade secret owners to prove "access" using circumstantial evidence on "access", "opportunity to obtain" and "substantially the same" elements.

Infringers and Misappropriation Acts

Article 9 of the CAUCL specifies that obtaining another's trade secrets by means of electronic intrusion constitutes misappropriation. Also, under Article 9(4), "instigating, inducing, or aiding others in violation of confidentiality obligations to obtain, disclose, use or allow others to use trade secrets" constitutes misappropriation.

Under the amended CAUCL, the categories of infringers are expanded from business operators to include natural persons, legal persons, and unincorporated organizations.

Damages

The compensation for trade secrets misappropriation is prescribed to be the actual loss of the trade secrets owner or the gain reaped by the infringer. If the infringement is serious and in bad faith, the amount of compensation may be increased to more than one time, but less than five times, the loss suffered by the owner or the gain reaped by the infringer. If it is difficult to determine the loss suffered or the gain reaped, the amount of statutory damages can be up to RMB 5 million (about US$700,000, increased from RMB 3 million under the old law).

Evidence

The Provisions of the Supreme People's Court ("SPC") on Evidence in Civil Procedures ("New Evidence Rule") went into effect on May 1, 2020. The New Evidence Rule removed the requirements of notarization and legalization for most types of evidence formed outside of China. Only documents such as foreign official documents need to be notarized and legalized outside of China to be admissible in Chinese courts. The New Evidence Rule also specified the admissibility of electronic evidence. In addition, Articles 45–48 provide that a court can require the party who has control over certain evidence to submit the evidence, and if the party refuses without justification, it will bear the consequences. For example, in a trade secret misappropriation case, the court can request the defendant to submit books and accounts for assessing damages. If the defendant refuses without justification, the court should support the damage calculations put forward by the plaintiff.

Regulation for Criminal Enforcement Against Misappropriation

On June 17, 2020, the SPC and the Chinese Supreme People's Procuratorate jointly published the draft "Several Issues Concerning the Specific Application of Law for Handling Criminal Cases of Intellectual Property Infringement." The draft regulation clarifies the threshold for criminal prosecution of trade secret misappropriation, specifies possible confidential measures to protect evidence during trial, and provides sentencing guidelines. The draft regulation retains the threshold for initiating criminal prosecution requiring rights holders to prove that illegal income from the misappropriation exceeded RMB 500,000 (about US$70,000).

Recent Trade Secret Misappropriation Cases

***Hebi Reflective Materials Co., Ltd. v. Li Jianfa, Song Junchao, and Hebi Ruimingte Tech. Co., Ltd.* ((2018) Zui Gao Fa Min Shen No. 1273) (Decided Mar. 29, 2019)**

Six of the customers with whom the defendant Ruimingte traded in the northeast region of China were customers of the plaintiff Reflective. The SPC found that Song had participated in business activities such as changing the company registry information for Ruimingte. In addition, Ruimingte did not adduce any evidence that the six customers had approached Ruimingte, nor that the relevant customer information was obtained by its own work, so the SPC found that Ruimingte illegally misappropriated the customer information of Reflective. In this case, the SPC applied the "access to confidentiality information + substantial similarity – legitimate source" formula to determine whether there was trade secret misappropriation.

***Henan Zhongnianreke Industrial Energy Saving Co., Ltd. v. Henan Jiude Smart Devices Co., Ltd. and Gou* ((2019) Yu Zhi Min Zhong No. 450) (Decided Dec. 19, 2019)**

A former employee of the plaintiff used the plaintiff's confidential information (mainly customer lists) to trade with the plaintiff's customers after he was employed by the defendant. The Henan High Court found that: (i) the confidential customer information was substantially the same as that in the plaintiff's customer list; (ii) the employee had access to the confidential customer information while employed by the plaintiff and was in fact in contact with the confidential information when signing contracts with one customer in the list on behalf of the plaintiff; and (iii) there was no evidence proving the legitimate sources of the confidential information. The Henan High Court also followed the "access to confidentiality information + substantial similarity – legitimate source" formula to find trade secret misappropriation.

KEY TAKEAWAYS

Important reforms have placed trade secret owners on a more level playing field. Trade secret misappropriation litigation in China still faces other obstacles, including lack of a common law discovery system and strict rules on evidence collection by private parties. Even with the reforms, it is critical that trade secret owners carefully and meticulously prepare their cases.

CONCLUSION

This *White Paper* highlights recent noteworthy trade secret cases and updates in jurisdictions worldwide. In the United States, courts have provided insight into several topics, including ownership standards for misappropriation, the extraterritoriality of the DTSA, reasonable royalties and attorneys' fees in trade secret cases, the treatment of trade secret verdicts in bankruptcy, the Computer Fraud and Abuse Act, and the Economic Espionage Act. In Germany, the new Company Trade Secret Act provides a specific type of litigation to resolve disputes on trade secrets. And in China, recent updates to the CAUCL have introduced changes that ease the burden on trade secret owners in misappropriation cases.

LAWYER CONTACTS

Authors

Kelsey I. Nix
New York
+1.212.326.8390
knix@jonesday.com

Cheryl L. O'Connor
Irving
+1.949.553.7505
coconnor@jonesday.com

John A. Marlott
Chicago
+1.312.269.4236
jamarlott@jonesday.com

Georg Mikes
Frankfurt
+49.69.97263.939
gmikes@jonesday.com

Chiang Ling Li
Hong Kong
+852.3189.7338
chianglingli@jonesday.com

Haifeng Huang
Hong Kong/Beijing
+852.3189.7253/+86.10.5866.1216
hfhuang@jonesday.com

Marlee R. Hartenstein
Pittsburgh
+1.412.394.7257
mhartenstein@jonesday.com

ADDITIONAL CONTACTS

Emily J. Tait
Detroit
+1.313.230.7920
etait@jonesday.com

Randall E. Kay
San Diego
+1.858.314.1139
rekay@jonesday.com

Jonathan M. Linas
Chicago
+1.312.269.4245
jlinas@jonesday.com

Luke J. Burton, *Jiahui Sheng*, *Luke Song*, *and Albert Wang coauthored this* White Paper.

ENDNOTES

1 *Advanced Fluid Systems, Inc. v. Huber*, Nos. 19-1722, 19-1752, 2020 WL 2078298 at *2 (3d. Cir. Apr. 30, 2020).
2 *Id.* at *4.
3 *Id.*
4 *Id.* at *2.
5 *Id.* at *5 (emphasis added).
6 *Id.*
7 *Id.* (emphasis added).
8 *Id.*
9 Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (codified at 18 U.S.C. § 1836, *et seq.*)
10 *Compulife Software Inc. v. Newman et al.*, No. 18-12004, No. 18-12007, 2020 WL 2549505 at *1 (11th Cir. May 20, 2020).
11 *Id.*
12 *Id.* at *1–2.
13 *Id.* at *2
14 *Id.*
15 *Id.* at *4.
16 *Id.* at *5.
17 *Id.* at *16.
18 *Id.*
19 *Id.*
20 *Id.* (emphasis in original).
21 *Id.* at *17.
22 Complaint at 1, *Tesla, Inc. v. Cao*, Case No. 19-cv-01463 (N.D. Cal. March 21, 2019) (Dkt. 1).
23 Third Party XMotors's Motion to Quash at 2, *Tesla, Inc. v. Cao*, Case No. 19-cv-01463 (N.D. Cal. March 30, 2020) (Dkt. 44).
24 *Id.* at 7.
25 Order Re Pending Motions at 1, *Tesla, Inc. v. Cao*, Case No. 19-cv-01463 (N.D. Cal. May 27, 2020) (Dkt. 75).
26 *Id.*
27 *Id.*
28 *WeRide Corp. v. Huang*, No. 18-cv-07233, 2020 WL 1967209 (N.D. Cal. Apr. 24, 2020).

29 *Id.* at *2.
30 Order Granting In Part and Denying In Part WeRide's Motion for Preliminary Injunction, *WeRide Corp. et al. v. Huang, et al.*, Case No. 5:18-cv-07233-EJD (N.D. Cal. Apr. 1, 2019); *see also* Nix et al., "Mid-Year Review of Key Trade Secret Decisions" (May 2019).
31 *WeRide Corp.*, 2020 WL 1967209 at *2.
32 *Id.* at *3.
33 *Id.*
34 *Id.* at *9–11.
35 *Id.* at *9–12.
36 *Id.* at *15.
37 *Motorola Solutions Inc. v. Hytera Communications Corp.*, 1:17-cv-1973, 2020 WL 967944 at *5 (N.D. Ill. Jan. 31, 2020).
38 *Id.*
39 *Id.*
40 *Id.*
41 *Id.* at *8.
42 *Id.* at *9.
43 *Id.*
44 *Id.* at *12.
45 *Id.* at *11.
46 *Id.*
47 *Id.* at *12.
48 *See United States v. Van Buren*, 940 F.3d 1192 (11th Cir. 2019), cert. granted, 2020 WL 1906566 (Mem.) (U.S. Apr. 20, 2020).
49 18 U.S.C. § 1030(a)(2)(C).
50 *Id.* at § 1030(e)(6).
51 Petition for a Writ of Certiorari, *Van Buren v. United States*, No. 19-783 (Dec. 18, 2019), 2019 WL 6910424 at *1-3.
52 *Van Buren*, 940 F.3d at 1198.
53 *Id.* at 1208.
54 *Id.*
55 *Id.* at 1207–08.
56 Petition for a Writ of Certiorari, *Van Buren v. United States*, No. 19-783 (Dec. 18, 2019), 2019 WL 6910424.
57 *Id.*
58 18 U.S.C. § 1030(g).
59 *In re Hill*, 957 F.3d 704, 707 (6th Cir. 2020).
60 *Id.*
61 *Id.*
62 *Id.* at 708.
63 *Id.*
64 *Id.*
65 *Id.*
66 *Id.* at 708–709.
67 11 U.S.C. § 523(a)(6); *see also In re Hill*, 957 F.3d at 709.
68 *In re Hill*, 957 F.3d at 709.
69 *Id.* at 711.
70 *Id.* at 712.
71 *Id.* at 713–14.
72 *Ajaxo, Inc. v. E*Trade Financial Corp.*, 261 Cal.Rptr.3d 583 (Cal. Ct. App. 2020).
73 *Id.* at 592.
74 *Id.* at 592–93.
75 *Id.* at 593.
76 *Id.*
77 *Id.*
78 *Id.*
79 *Id.* at n.5.
80 *Id.* at 594.
81 *Id.* at 595.
82 *Id.*
83 *Id.* (emphasis added).
84 *Id.* at 605.
85 *Id.*
86 *Id.*
87 *Id.* at 616–17.
88 *Id.* at 603–04.
89 *Id.* at 615–17.
90 *Id.* at 611 (emphasis added).
91 *Insurent Agency Corp., et al. v. The Hanover Insurance Co., et al.*, No. 16-cv-3076, 2020 WL 86813 at *1 (S.D.N.Y. Jan. 8, 2020).
92 *Id.* at *1–2.
93 *Id.* at *2.
94 *Id.* at *8 (quoting 18 U.S.C. § 1836(b)(3)(D)).
95 *Id.* at *9.
96 *Id.*
97 *Id.*
98 *See* § 337(a)(1)(B).
99 *See* § 337(a)(1)(C), (D), (E); 15 U.S.C. § 1051 *et seq.* (trademarks); 17 U.S.C. § 901 *et seq.* (semiconductor masks); 17 U.S.C. § 1301 *et seq.* (boat hull designs).
100 *See TianRui Grp. Co. v. Int'l Trade Comm'n*, 661 F.3d 1322, 1326 (Fed. Cir. 2011) (emphasis added).
101 *TianRui*, 661 F.3d at 1336.
102 *See In the Matter of Certain Cast Steel Ry. Wheels*, USITC Inv. No. 337-TA-655 (Oct. 16, 2009); *In the Matter of Certain Rubber Resins*, USITC Inv. No. 337-TA-849 (June 17, 2013).
103 *Organik Kimya v. U.S. Int'l Trade Comm'n*, 848 F.3d 994, 1005 (Fed. Cir. 2017).
104 *Compare In the Matter of Certain Electric Fireplaces*, USITC Inv. No. 337-TA-791/826 (May 1, 2013) *with In the Matter of Certain Opaque Polymers*, USITC Inv. No. 337-TA-883 (Apr. 17, 2015).
105 Jody Godoy, *4 Chinese Military Members Charged with Equifax Hack*, Law360.
106 *Id.*
107 *See United States v. Liew*, 856 F.3d 585, 600-01 (9th Cir. 2017).
108 Department of Justice Press Release No. 20-157 (February 10, 2020).
109 *United States v. Tan*, Case No. 4:19-cr-00009 (N.D. Okla.), Dkt. No. 1, ¶ 7.
110 *Id.*, Dkt. No. 18.
111 *Id.*, Dkt. No. 149.
112 *Id.*, Dkt. No. 164 and 165.