

## 2019 Trade Secrets Mid-Year Review: Global Developments in Trade Secrets

AUGUST 20, 2019

The increased focus on protecting trade secrets by individuals, governments, and law enforcement agencies in the United States and abroad has continued during the first half of 2019. Following up on our [2018 Trade Secrets Year in Review](#), Winston & Strawn's Global Privacy & Data Security Task Force has assembled a list of trends and interesting developments involving trade secrets that have occurred around the globe in the last six months. This list also identifies our observations and predictions for the remainder of 2019.

### UNITED STATES

#### ***DOJ's Continued Focus on Theft Involving Chinese Entities and Actors***

Consistent with the aims identified by the Department of Justice (DOJ) when it announced the [China Initiative](#) in November 2018, during the first half of 2019, prosecutors have initiated and resolved a handful of criminal trade secrets cases involving Chinese entities and actors or theft undertaken for the benefit of Chinese entities and actors. For example, in January 2019, a [grand jury indicted two affiliates of Huawei Technologies](#) (Huawei), one of the world's largest communications equipment manufacturers, for stealing trade secrets from a competitor company. On February 14, 2019, [the Department of Justice obtained an indictment against former Coca-Cola scientist Xiaorong You](#) of Lansing, Michigan and Liu Xiangchen of Shandong Province, China for conspiring to steal trade secrets regarding the expensive and difficult-to-develop formulations for bisphenol-A-free (BPA-free) coatings used to line soda cans. On February 25, 2019, a [jury in Chicago, Illinois convicted an employee](#) of a cast-iron manufacturing firm on seven counts of trade secret theft. The employee was found guilty of stealing the trade secrets in order to supply them to his new Chinese employer. In late April, [federal prosecutors in New York unsealed a 14-count indictment](#) that charges a former engineer of an American power company and a Chinese businessman with conspiring to commit economic espionage and to steal trade secrets for the benefit of the government of the People's Republic of China (PRC) and other entities owned or controlled by the Chinese government. Winston predicts that DOJ will continue to pursue criminal cases to combat the theft of trade secrets that benefit Chinese entities and actors.

#### ***Trade Secrets Cases Dismissed on Timeliness Grounds***

In several recent decisions, courts in the United States have dismissed trade secrets claims on timeliness grounds. For example, on April 4, 2019, the Eighth Circuit Court of Appeals affirmed summary judgment in favor of Iowa Parts, a company that allegedly used intellectual property owned by a competitor, CMI Roadbuilding (CMI), concluding that CMI failed to timely assert a claim because the statute of limitations clock under the Defend Trade Secrets Act (DTSA) started to run after CMI was put on notice that its trade secrets were misused by Iowa Parts. See *CMI Roadbuilding, Inc. v. Iowa Parts, Inc.*, 920 F.3d 360 (8th Cir. 2019). Similarly, a court in the Northern District of California dismissed a plaintiff's claim under the California Uniform Trade Secrets Act (CUTSA) as untimely. The court reasoned that because the plaintiff asserted a theory of misappropriation by acquisition—meaning that the defendant misappropriated the trade secrets at the time it acquired them pursuant to the non-disclosure agreement executed in 2011—the plaintiff was on notice that the defendant acquired its trade secrets, and it failed to bring a claim within the four-year statute of limitations period.

### ***Recent Cases Demonstrate that Plaintiffs Must Allege that Trade Secret Theft Occurred After May 11, 2016 to Constitute Predicate Acts Under RICO***

The DTSA is an enumerated predicate act under the civil Racketeer Influence and Corrupt Organizations (RICO) Act. Thus, plaintiffs can assert claims under RICO alleging a conspiracy “through a pattern of racketeering activity” and a violation of the DTSA may constitute one or more of the underlying claims.

Two recent cases demonstrate that to survive a motion to dismiss, plaintiffs asserting RICO claims with violations of the DTSA as predicate acts must show that the theft of trade secrets occurred after the enactment of the DTSA. On February 28, 2019, a Pennsylvania federal court held that a plaintiff alleging violations of the civil RICO Act and using violations of the DTSA as the only predicate offenses must plead that two or more acts of trade secret theft occurred after May 11, 2016 to withstand a motion to dismiss. *Magnesita Refractories Co. v. Tianjin New Century Refractories Co., Ltd.*, 2019 WL 100623, at \*8 (M.D. Pa. Feb. 28, 2019). Similarly, in *Attia v. Google LLC*, 2019 WL 1259162, at \*3 (N.D. Cal. March 19, 2019), a court dismissed the plaintiff's complaint in part because it failed to allege that two or more predicate acts occurred after May 11, 2016.

### ***Recent ITC Case Demonstrates Why It May Become a More Popular Forum in Which Litigants May Choose to Pursue Cross-Border Trade Secrets Cases***

On February 28, 2019, the United States International Trade Commission (“ITC”) instituted an investigation into the botulinum toxin products manufactured by Korean Daewoong Pharmaceuticals Company Limited (Daewoong) and its California licensee, Evolus, Inc. (Evolus), after two courts in the United States dismissed theft of trade secrets cases filed by Medytox Inc. (Medytox) and Allergan entities. The ITC complaint filed by Medytox alleges that a former researcher printed out and emailed various confidential company documents, including reports, batch records, and test data, to his personal email account and took test samples of a toxin strain with him in a vial when he left the company in 2008. The complaint further alleges the researcher consulted for Daewoong and improperly used Medytox's stolen trade secrets, which enabled Daewoong to fast-track through years of research. Medytox pursued its trade secrets claims against Daewoong and Evolus at the ITC after the claims in its actions filed in Indiana and California were dismissed on *forum non conveniens* grounds and stayed pending the outcomes of litigation pending in South Korea. In dismissing Medytox's claims for *forum non conveniens*, the Indiana court found that certain conduct related to the theft occurred in Korea, outside of the court's jurisdiction.

This case is an example of how, when confronted with cross-border trade secrets issues, companies may increasingly rely on the ITC as part of their strategy to litigate these disputes. Winston predicts that the number of cases filed with the ITC that involve cross-border trade secrets theft will likely increase in coming months.

### ***Courts Still Pushing on the “Reasonable Measures” Requirement but Recent Case Suggests Confidential Markings May Not Be Outcome Determinative***

In 2018 and continuing in 2019, when interpreting the DTSA, numerous courts dismissed theft of trade secrets claims and denied injunctive relief because the victim-companies failed to take reasonable measures to protect their trade secrets. A handful of these rulings turned on whether the victim company adequately marked trade secrets as confidential. A recent decision, however, suggests that confidential markings in and of themselves may not be outcome determinative. In February 2019, a district court in Alabama denied a motion to dismiss theft of trade

secrets claims brought pursuant to the DTSA and the Alabama Trade Secrets Act, finding that the plaintiff company took “reasonable measures” to protect the purportedly stolen assets. See *S. Field Maint. & Fabrication LLC v. Killough*, No. 2:18-cv-581-GMB, 2019 BL 28443 (M.D. Ala. Jan. 29, 2019). Notably, the court found that the plaintiff company sufficiently plead that it took reasonable measures to protect its trade secrets even though it did not mark some of them as confidential. The court explained that the “analysis of the measures taken to protect secrecy is fact-specific” and, “under all the circumstances, if the employee knows or has reason to know that the owner intends or expects the information to be secret, confidentiality measures are sufficient.” The court reasoned that the company took adequate steps to protect its trade secrets because: (1) the non-marked information was contained on a password-protected, limited-access server; (2) the employee had signed a written acknowledgment of his obligation to keep sensitive business information confidential; and (3) the plaintiff had discussed with the employee the need to keep confidential the proprietary information in the documents at issue.

Winston expects that in the latter half of 2019, courts will continue to rule on motions on the pleadings and motions for summary judgment that center on the “reasonable measures” analysis. These cases will likely provide companies with additional guidance about how to take thoughtful and affirmative steps to implement policies, processes, and programs to protect their valuable trade secrets. Indeed, Winston predicts that reasonable measures risk assessments and compliance programs will become a focal point for companies looking to mitigate trade secret risks.

### ***Recent Cases Highlight the Importance of Forensic Evidence in Trade Secrets Cases***

Recent civil actions pursued in United States courts highlight the importance of preserving and pursuing the production of forensic evidence in theft of trade secrets cases. For example, in February 2019, a judge in North Carolina entered an injunction against a research and development chemist that worked for Ennis-Flint, citing forensic evidence of trade secrets theft. Namely, as cited by the court in its reasoning, forensic evidence showed that the chemist copied formulas from his laptop to a personal storage device and a personal cloud storage account. In May 2019, List Industries, LLC (List) filed a claim for trade secret misappropriation under Ohio law, alleging that a former employee (Umina) stole its trade secrets and gave them to Top Tier Storage Products, LLC. To prove its trade secret claim, List sought to forensically image the hard drive issued by List to Umina. At the request of List, the court ordered the defendants to capture and produce images of the laptop at issue.

Winston expects that electronic forensic evidence will be key in future trade secrets cases. When companies learn of potential theft of trade secrets, they should consider immediately directing a computer forensics vendor to preserve evidence of theft. Companies should also consider pursuing forensic evidence in discovery in trade secrets cases.

## **ASIA**

### ***Trade War Between the United States and China Keeps Trade Secrets in the News and Shines an International Spotlight on Intellectual Property Theft***

During the first half of 2019, the trade war between the United States and China escalated. The United States imposed tariffs on Chinese imports and it effectively barred United States companies from supplying China-based Huawei with telecom component parts. China responded and imposed tariffs on imports of American products. Huawei also responded and filed a lawsuit against the United States, asking a district court in Texas, the same court in which a jury recently found that Huawei stole CNEX Labs’ trade secrets, to declare the ban on parts unconstitutional.

One of the United States’ demands to end the trade dispute is that China take further measures to protect intellectual property and, specifically, to protect trade secrets. News outlets from Reuters, to the New York Times, the BBC, the South China Morning Post, and Xinhua have all written about the ongoing trade dispute and the issue of intellectual property protections in China. The press about the trade war has kept trade secrets in the news and has placed an international spotlight on intellectual property theft and the need for protection.

### ***China Revamps its Foreign Investments Law and Provides Additional IP Protections to Foreign Businesses***

On March 15, 2019, the National People's Congress (NPC), the highest legislative body of the PRC, approved a new Foreign Investment Law (FIL), which aims to promote foreign investment in China. The FIL will come into effect on January 1, 2020. The new FIL contains provisions that may provide to foreign investors additional intellectual property protections. For example, one provision requires Chinese government agencies and their officers to keep confidential all trade secrets belonging to foreign investors and foreign investment enterprises that they learn of during the course of their work. Government agencies and their officers may be penalized administratively, or possibly criminally, for divulging trade secrets. Additionally, in response to allegations made by foreign companies that, in exchange for the ability to operate in China, they have been required or pressured to disclose valuable intellectual property, the FIL expressly prohibits forced technology transfers.

The new FIL has been widely viewed as an olive branch to help China facilitate a resolution to the trade dispute with the United States. It may also be a sign of a cultural shift in China regarding intellectual property rights. We will closely monitor this issue going forward to determine to what extent courts in China enforce the FIL's provisions, whether and how the law impacts negotiations between Chinese actors and foreign companies, and whether the FIL's intellectual property protections help prompt more foreign companies to do business in the Chinese market.

### ***China Overhauls Anti-Unfair Competition Law***

Against the backdrop of the escalating trade war between China and the United States, the NPC promulgated revisions to the Anti-Unfair Competition Law (AUCL) to provide additional trade secrets protections. These revisions reflect the Chinese legislature's efforts to enhance trade secrets protections and to improve intellectual property protections for multinational companies that do business in China. The revisions change the AUCL in three principal ways. First, the scope of the definition of infringers under the AUCL was broadened to include not only business operators but also individuals and other entities, meaning that employees and former employees that steal trade secrets now fall under the ambit of the AUCL. Second, the revisions increased the amount of monetary compensation that a complainant may seek if a theft occurs. Finally, the revisions relaxed the burden of proof in trade secrets cases, requiring only that the complainant provide preliminary evidence that it took measures to protect its trade secrets and show that to a reasonable extent, its trade secrets have been infringed.

The changes to the AUCL demonstrate a potential shift in the intellectual property landscape in China. We will keep a close eye on this issue in the second half of 2019 to see whether companies doing business in China will seek protections from Chinese courts pursuant to the AUCL, giving the courts the opportunity to interpret and apply the law's new provisions.

### ***Taiwan Aggressively Pursues Theft of Trade Secrets Cases***

During the first half of 2019, authorities in Taiwan have continued to aggressively pursue trade secrets cases. In January, Taiwanese police arrested six individuals, including a retired, former employee of BASF Taiwan Ltd., for alleged breach of Taiwan's Trade Secret Act. Taiwan's Criminal Investigation Bureau suspected that a rival company conspired with the six individuals to funnel information to China. Also in January, Taiwanese prosecutors charged four former employees of Novatek Microelectronics Corp., a leading Taiwanese fabless chip design company, with violations of Taiwan's Trade Secrets Act. In May 2019, a criminal court in Taiwan sentenced Thomas Chien, a former top designer and vice president of Taiwanese smartphone manufacturer HTC, to seven years and ten months in jail for his role in a scheme to steal HTC's trade secrets. On June 18, 2019, another criminal court sentenced Chen Shih-Yu, a former employee of A-Lumen Machine Co. Ltd. (A-Lumen), to 18 months in prison and imposed a fine of NT\$2 million for misappropriating A-Lumen's trade secrets related to a UV optical film forming machine.

## **EUROPEAN UNION**

### ***Spain, Germany, Luxembourg, and Greece Pass Laws Implementing the EU Trade Secrets Directive***

During the first half of 2019, additional European Union (EU) member states implemented the EU's Trade Secrets Directive. In March, the Business Secrets Act went into effect in Spain and, in April, the Trade Secrets Act went into effect in Germany. Similarly, on April 1, 2019, Greece adopted Law 4605/2019, and, in June, Luxembourg adopted the Law of 26 June 2019, both of which implement the Trade Secrets Directive. The Spanish, German, Greek, and

Luxembourgish laws adopted the Trade Secrets Directive's reasonable measures requirement and for a secret to be protected under these laws, the owner must take steps to maintain the secret's confidentiality. None of these laws define what may constitute reasonable measures. However, the explanatory remarks to the German law provide some guidance. They explain that reasonable measures will be evaluated on a case-by-case basis and that physical protections, like access restrictions, and contractual mechanisms may be considered.

The laws implementing the EU's Trade Secrets Directive place a burden on companies to take active steps to protect their trade secrets. Winston predicts that reasonable measures risk assessments and compliance programs will increasingly become the focus of multi-national companies in Europe, and will likely spill over into litigation in the years to come. Companies should be cognizant of these new laws and should consider how best to protect their trade secrets.

### ***Prosecutors Announce Criminal Charges Against Four Individuals in Connection with Long-Running Investigation into the Theft of Business Secrets***

In connection with a years-long investigation, in January, the public prosecutor in Stuttgart, Germany announced criminal charges against four individuals for misappropriating trade secrets. The four individuals are former employees of KBA MetalPrint GmbH (KBA) who started a competing metal decorating company called Hebenstreit Metal Decorating GmbH (Hebenstreit). The individuals allegedly stole construction plans from KBA and used them to recreate KBA's printing presses and component parts for use at their new company. KBA hired private investigators to look into Hebenstreit and they found plans and drawings in the trash that bore KBA's mark. KBA filed a criminal complaint regarding the suspected theft of internal documents in 2013 and, since that time, the Stuttgart public prosecutor's office has also been investigating the matter. In 2015, police searched Hebenstreit's offices and, in 2017, two other former KBA employees were convicted and fined for stealing business secrets.

In recent years, the EU's adoption of the Trade Secrets Directive has highlighted the importance of protecting trade secrets. Just as Winston predicts that trade secrets issues are likely to spill over into civil litigation filed in the EU in the future, Winston anticipates also seeing a rise in the number of investigations into and prosecutions pursued against individuals and companies that misappropriate trade secrets. When companies doing business in the EU learn of potential theft, they should consider how and when to refer matters to law enforcement. Companies should also consider implementing proactive compliance measures to minimize risk and to protect their trade secrets when employees are terminated.

### ***Recent Legislation and Court Decision May Signal a Trend in Favor of Whistleblower Protections in Trade Secrets Cases***

In April, the EU Parliament approved a directive on the protection of persons reporting on breaches of Union law (Whistleblower Directive). The Whistleblower Directive applies to all companies with 50 or more employees and it encourages entities with less than 50 employees to adopt reporting mechanisms similar to those required for larger companies pursuant to the directive. The directive also reaffirms the whistleblower protections outlined in the Trade Secrets Directive and states that it and the Trade Secrets Directive should be considered complementary laws. The Whistleblower Directive references the Trade Secrets Directive's whistleblower exception, which states that the remedies available in trade secrets cases will not apply if the use or disclosure of the trade secret occurred because a person revealed misconduct, wrongdoing, or illegal activity if the person acted for the purpose of protecting the general public interest. The Whistleblower Directive also explicitly and affirmatively states that the disclosure of trade secrets in accordance with the conditions set forth in the Trade Secrets Directive is to be considered as allowed by EU law. Moreover, the Whistleblower Directive requires the authorities who receive disclosed trade secrets to ensure that the secrets are not used or disclosed for purposes other than what is necessary to follow up on or investigate allegations from whistleblowers.

In a recent court decision in Germany, a district court in Munich interpreted the whistleblower protections outlined in the Trade Secrets Directive and acquitted an individual after lower courts convicted him of inciting the disclosure of trade secrets by handing out leaflets that encouraged employees to report on employers involved in the illegal arms trade. In the decision, the court interpreted German law in light of the Trade Secrets Directive, even though it had not been implemented at the time that the court issued its decision. Looking at the interests of the individual and the company, and taking into account that the Trade Secrets Directive precludes actions against whistleblowers when

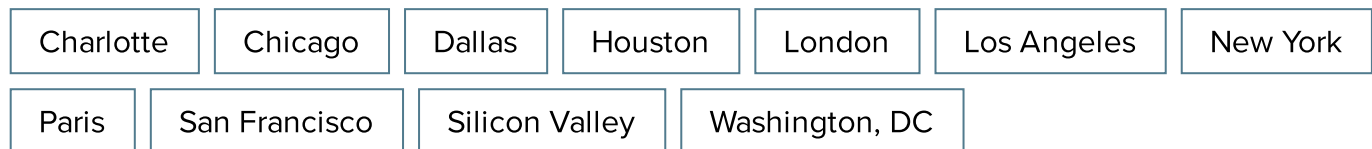
individuals act in the public interest to expose misconduct, the court found that the individual's behavior was exempted by the Trade Secrets Directive and that the individual could not be prosecuted for asking employees to expose illegal behavior.

The passage of the Whistleblower Directive and the recent case in Germany may signal a growing trend in favor of whistleblower protections in trade secrets cases in the EU. We will monitor the approval of the Whistleblower Directive during the second half of 2019, as well as court decisions in Germany and other member states, to see whether more individuals seek protection from courts in the EU after allowed disclosures of trade secrets.

10+ Min Read

---

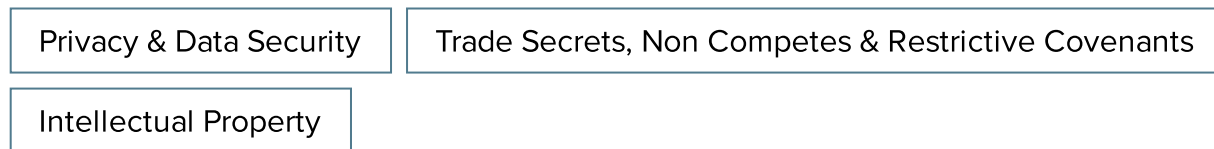
## Related Locations



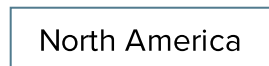
## Related Topics



## Related Capabilities



## Related Regions



## Related Professionals

---



Gino Cheng



Sara Susnjar



David Enzminger



Steven Grimes