

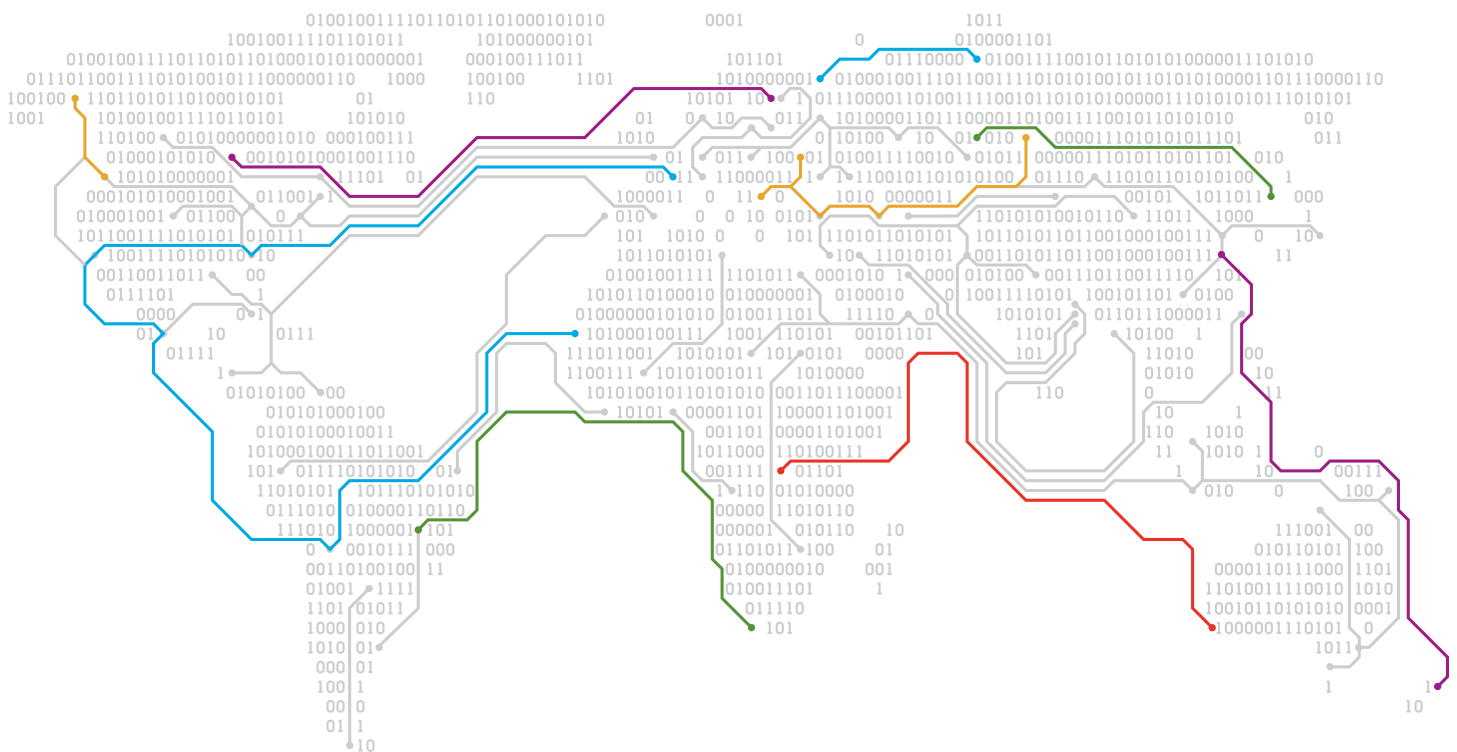
# 2018 Trade Secrets Year in Review

## Top 10 Takeaways in Trade Secrets



2018 was rife with notable legal developments in the trade secrets space as individuals, governments, and law enforcement agencies in the United States and abroad placed heightened attention on the protection of trade secrets.

**Winston & Strawn's Global Privacy & Data Security Task Force** has assembled a top 10 list of notable developments and trends that occurred over the past year relating to trade secret protection, as well as our observations and predictions for 2019.



# 1 Rising Trade Secret Litigation

---

On July 18, 2018, *Lex Machina* released the **Trade Secret Litigation Report 2018**. Among other interesting statistics, the Report found that since the Defend Trade Secrets Act (DTSA) was passed in the spring of 2016, the number of civil trade secrets cases filed in federal and state courts in the United States has increased by 30%. We expect that this statistic will continue to rise, suggesting that private litigants will continue to use the protections provided under the laws in the United States to protect their trade secrets.



## 2 Increased Focus on Theft Involving Chinese Entities

---

On November 1, 2018, the United States Department of Justice (DOJ) announced the creation of the **China Initiative** that aims to combat economic espionage and the theft of American trade secrets perpetrated by Chinese actors. Consistent with this recent policy pronouncement, in 2018, DOJ both initiated and resolved a number of criminal cases against defendants with ties to China, including cases involving alleged theft of anti-cancer technology from **GlaxoSmithKline**, alleged theft of **GE Aviation technology**, and theft allegedly accomplished in part by **hiding data in a photograph**. As companies

continue to grapple with cross-border trade secret issues, **Winston predicts** greater reliance on the ITC as a forum for litigation cross-border trade secret rights.

---

**Trade secrets, by definition, are given legal protection** because they are comprised of information that creates economic value.

---

## 3 Large Damages Claims, Verdicts, and Settlements

---

The damages sought and obtained in many trade secret cases in 2018 were very high. For example, there was a \$245 million settlement in a California-based dispute regarding alleged misappropriation of self-driving technology trade secrets. In a Texas lawsuit, a real estate valuation company, HouseCanary, alleged that title insurance company, Title Source (now Amrock), misappropriated HouseCanary's intellectual property to create competing software. After a seven-week trial, the jury sided unanimously with HouseCanary and awarded the company a \$706.2 million verdict. In California, a jury awarded the U.S. branch of a Dutch semiconductor maker, ASML, \$223 million in its suit against a local rival, XTAL, for misappropriating trade

secrets, and ASML was also ordered to pay an additional \$1.2 million to compensate AMSL for its investigation expenses. In a government-driven action, the DOJ pursued a wind turbine manufacturer, Sinovel Wind Group Co. Ltd., for stealing trade secrets from American Superconductor (AMSC), a Massachusetts-based company, with a claimed loss of at least \$800 million, 700 jobs, and \$1 billion in shareholder equity. Sinovel secretly downloaded AMSC source code and used it on Sinovel-commissioned turbines. Still pending is a suit brought in August against a major big-box chain, alleging \$2 billion in damages related to alleged illegal use of intellectual property in food freshness technology.

## 4 Significant Media Attention

---

With the rise of trade secret cases, and the damage that companies can suffer from theft, it is not surprising that trade secret cases and trends have been highlighted in the media. For example, Corporate Counsel published an article titled, "Why Trade-Secret Theft Prosecutions vs. China are Trending: Lawyers Explain"; *Reuters* published an "Exclusive" that "German prosecutors

charge Chinese-born engineer in industrial espionage case"; and *The Wall Street Journal* published an article titled "How China Systematically Pries Technology from U.S. companies"; and *The New York Times* covered various trade secret cases including in an article titled "Chinese Officer Is Extradited to U.S. to Face Charges of Economic Espionage."

# 5 Implementation of the EU Trade Secret Directive



Because the European Union's Trade Secret Directive was required to be implemented by all member states by June 9, 2018, many (but not yet all) EU countries took significant steps to implement and to begin enforcing trade secret laws in 2018. While the EU Trade Secret Directive's definition of a trade secret closely mirrors the definition in the federal DTSA and requires companies to take proactive measures to protect their information, the individual countries' implementations of the directive can differ from the DTSA, such as by providing broader protections for whistleblowers and by not providing an ex parte seizure remedy.

# 6 Near Universal Adoption of the UTSA by States

In August, Massachusetts became the 49th state in the United States to adopt a version of the **Uniform Trade Secrets Act (UTSA)**. Massachusetts's trade secret statute codifies many aspects of existing common law while making protections clearer and allowing cost shifting and the recovery of attorneys' fees if a plaintiff brings a theft of trade secrets lawsuit in bad faith.



## 7 Courts Pushing on the “Reasonable Measures” Required to Protect Trade Secrets

A handful of courts, interpreting state trade secrets laws and the DTSA, dismissed theft of trade secrets claims because the victim-company failed to take reasonable measures to protect their purported trade secrets. For example, the **Eleventh Circuit affirmed** a district court's grant of summary judgment in favor of a defendant because the plaintiff failed instruct the defendant to secure company information on his personal devices, allowed the defendant to access information after he refused to sign a confidentiality

agreement, and failed to mark information as confidential. Additionally, another district court summarily dismissed a case brought by a company against a former employee, finding that no reasonable jury could find the requisite misappropriation under the DTSA because, in contravention of corporate policy, the information taken by the defendant was not marked as a trade secret or confidential.

## 8 Employees Not Protecting Corporate Data



Numerous studies in 2018 found that employees, including CEOs and business leaders, admitted to taking and/or using company confidential information and that employees believed that their trade secrets were in the hands of a competitor. For

example, **Code42's 2018 Data Exposure Report**, which surveyed security, IT, and business leaders in the US, UK, and Germany, found that 72% of CEOs and 49% of business leaders admitted to taking intellectual property from their previous employers. Additionally, a report published by the **Ponemon Institute** found that 65% of the 634 IT security professionals surveyed believed that their companies' trade secrets were known to competitors, and 82% of respondents acknowledged that it was "likely" or "very likely" that high value company assets had been breached.

# 9 Protection for Trade Secret Whistleblowers

---

In 2018, for the first time, a **district court granted protection** to a whistleblower pursuant to the DTSA's immunity provision, dismissing the defendant's counterclaim and finding that the plaintiff in a discrimination case disclosed trade secrets "in confidence... to an attorney...solely for the purpose of reporting or investigating a suspected violation of law," as required by the DTSA.

---

**TIP:** Companies should be aware of the whistleblower protections provided by the DTSA when considering filing a claim based on disclosure.

---

# 10 Promotion of Cooperation with Law Enforcement

---

In a speech on October 1, 2018, FBI Director Christopher Wray stressed that it is of critical importance for companies to proactively protect trade secrets, including by cooperating with law enforcement after learning about potential theft. In 2018, coordination with law enforcement resulted in DOJ bringing criminal theft of trade secrets charges against a number of individuals, for example, in a case involving alleged theft of **GE Aviation's secrets** and a case involving alleged theft of drug manufacturer **Genentech, Inc.'s secrets**. Additionally, in December, the DOJ announced that it arrested a former Phillips 66 employee

for allegedly stealing the company's trade secrets after the company reviewed the employee's computer following his resignation and **referred the matter to law enforcement**.



## Looking Ahead

These notable legal developments of 2018 suggest that the number of trade secrets actions, both civil and criminal, is on the rise. We expect the number of both civil and criminal trade secret cases to rise again in 2019, with potentially double digit growth in criminal enforcement cases globally in the coming year. In parallel to this large uptick in trade secret cases, studies and first-hand experience suggest that many companies do not have adequate measures in place to protect their trade secrets or prevent the use of others' trade secrets within their

own organizations. That said, the legal developments of 2018, coupled with our own anecdotal experience, suggests that companies are beginning to view trade secret theft as a compliance risk (alongside FCPA, trade sanctions, fraud, and the like), and, as such, are beginning to implement programs and frameworks for proactively mitigating those risks across the enterprise. We expect that proactive protection will be a key focus for companies in 2019, both in the United States and abroad.

## Key Contacts



**Sheryl Falk**  
Partner, Houston  
+1 (713) 651-2615  
[sfalk@winston.com](mailto:sfalk@winston.com)



**Steve Grimes**  
Partner, Hong Kong and Chicago  
+852 2292 2138  
+1 (312) 558-8317  
[sgrimes@winston.com](mailto:sgrimes@winston.com)



**Shannon Murphy**  
Partner, Chicago  
+1 (312) 558-5285  
[stmurphy@winston.com](mailto:stmurphy@winston.com)

## About Winston & Strawn

Winston & Strawn LLP is an international law firm with 1,000 attorneys across 16 offices in Brussels, Charlotte, Chicago, Dallas, Dubai, Hong Kong, Houston, London, Los Angeles, Moscow, New York, Paris, San Francisco, Shanghai, Silicon Valley, and Washington, D.C. The exceptional depth and geographic reach of our resources enable Winston & Strawn to manage virtually every type of business-related legal issue. We serve the needs of enterprises of all types and sizes, in both the private and the public sector. We understand that clients are looking for value beyond just legal talent. With this in mind, we work hard to understand the level of involvement our clients want from us. We take time to learn about our clients' organizations and their business objectives. And, we place significant emphasis on technology and teamwork in an effort to respond quickly and effectively to our clients' needs.

Visit **[winston.com](http://winston.com)** if you would like more information about our legal services, our experience, or the industries we serve.

Attorney advertising materials. Winston & Strawn is a global law firm operating through various separate and distinct legal entities.