

## When Trade Secret Litigation And Criminal Law Collide

By **Kenneth Notter** (March 25, 2026, 1:16 PM EDT)

On Jan. 29, a jury in the U.S. District Court for the Northern District of California returned a criminal conviction of an ex-Google engineer for trade secret theft and economic espionage in *U.S. v. Ding*. This epitomizes a long-running trend — the increasing convergence of trade secret litigation and white collar defense.

Trade secret litigation has traditionally been seen as a subspecies of intellectual property law with some employment law thrown in. Criminal prosecutions for trade secret theft or economic espionage were rare. This is no longer the case.

For the past decade, U.S. Department of Justice leadership under both parties has increasingly emphasized trade secret cases. And, even as the current DOJ has cut back on white collar enforcement in other areas, it has reaffirmed its commitment to trade secret enforcement.[1]

It is thus increasingly important for businesses and practitioners to understand how trade secret law and criminal law overlap, and to adjust accordingly.

### Legal Landscape

The Economic Espionage Act punishes two types of trade secret crimes: economic espionage and trade secret theft.

Economic espionage means misappropriating a trade secret with the intent or knowledge that doing so will benefit a foreign government or agent.[2] Trade secret theft means misappropriating a trade secret connected to interstate or foreign commerce with the intent or knowledge that the misappropriation will injure whoever owns the trade secret.[3]

Enacted in 2016, the Defend Trade Secrets Act dialed up the Economic Espionage Act's criminal penalties, increasing the statutory maximum prison sentence and adding economic espionage and trade secret theft as predicate offenses under the Racketeer Influenced and Corrupt Organization Act and money laundering statutes.[4]

Misappropriating trade secrets implicates a variety of other criminal laws too. Obtaining a trade secret through deceit could be charged as mail or wire fraud, for example.[5] Transporting or selling stolen trade secrets across state lines could be charged under the National Stolen Property Act.[6] And using a



Kenneth Notter

computer without authorization to obtain a trade secret could be charged under the Computer Fraud and Abuse Act.[7]

### **Increasing Criminal Enforcement**

Trade secrets are critical to the modern information economy. Yet it was not until 2014, in *U.S. v. Liew* before the Northern District of California, that a jury first convicted a defendant of economic espionage.[8]

For the last decade, though, the DOJ has made investigating and prosecuting criminal trade secret cases a priority.

Toward the end of the Obama administration, for example, the department's National Security Division released a strategic plan to increase enforcement of the Economic Espionage Act.[9]

That focus led to several high-profile trade secret prosecutions, such as *U.S. v. Xue* in the U.S. District Court for the Eastern District of Pennsylvania, which ended in multiple guilty pleas between 2018 and 2022.[10] And *U.S. v. Hailong* in the U.S. District Court for the Southern District of Iowa, which ended in a guilty plea for one defendant, Mo Hailong, in 2016 and dismissal for another defendant in 2015.[11] Both cases involved schemes to pass trade secrets from U.S. companies to China.[12]

The department's focus on trade secrets has only increased.

The first Trump administration, for instance, launched the China Initiative in 2018 to target trade secret theft linked to China. Though that program found mixed success in the courtroom and received substantial criticism,[13] the Biden administration launched its own strike force, resulting in a string of notable trade secret prosecutions.[14] And the second Trump administration has continued the trend, as seen by the February indictment in the Northern District of California of ex-Google engineers in *U.S. v. Ghandali* for allegedly stealing trade secrets to benefit Iran.

Even with the increasing focus on prosecuting trade secret cases, not every civil case merits criminal prosecution. At the federal level, prosecutors are more likely to indict cases that involve a foreign government, otherwise threaten national security or cause large-scale economic injury to the trade secret owner.[15]

In recent years, however, the department has increasingly prosecuted cases unconnected to foreign actors or national security.[16] The 2020 Northern District of California **conviction** of Anthony Levandowski, a former Uber executive, for stealing Google's trade secrets related to self-driving cars is the most high-profile example. But there are many others, such as the conviction last year of Varun Gupta — a former Intel Corp. engineer who allegedly shared trade secrets with Microsoft — in the U.S. District Court for the District of Oregon.[17]

Similarly, recent criminal cases have followed civil trade secret litigation that arguably fully remedied the misappropriation. For example, in 2022, the department indicted Hytera Communications in the U.S. District Court for the Northern District of Illinois for allegedly stealing Motorola Solutions' trade secrets years after Motorola prevailed at trial in 2020 in its civil suit in the Northern District of Illinois involving the same conduct.

Even so, it remains true that not every civil trade secret case is a criminal case in the making.

Prosecutors simply lack the time and resources to investigate every alleged trade secret misappropriation. And the higher burden of proof in a criminal case likely deters prosecutors from pursuing at least some, if not many, trade secret theft prosecutions. Cases involving foreign actors or inflicting massive harm to trade secret owners remain the most likely to attract prosecutors' attention.

## **Takeaways**

Businesses and practitioners need to adapt to the increasing overlap between trade secret litigation and criminal law. Here are a few things they can do.

### ***Educate employees about criminal risk.***

For businesses, the first thing to do is educate employees that stealing trade secrets is a crime. A 2013 Symantec study showed that most employees did not believe it was a crime to use a competitor's trade secrets.[18]

Beyond preventing potential violations, educating employees and implementing training may help a company show that it has taken the necessary reasonable measures to protect its trade secrets. It may also help qualify a business for cooperation credit with the DOJ in a criminal case.[19]

### ***React proportionately.***

Even as criminal enforcement increases, not every trade secret misappropriation should be treated as a potential criminal case. Low-dollar misappropriation involving domestic entities is unlikely to attract prosecutors' attention, so affirmatively disclosing misappropriation to the DOJ through one of its voluntary self-disclosure programs or spending time and energy to seek a criminal referral is likely to do more harm than good.

### ***Investigate foreign ties.***

Foreign involvement, more than anything else, can push a case from civil to criminal. Potential defendants must know whether the supposed misappropriation even arguably benefited a foreign government or other foreign entity. Knowing the answer is "no" can give businesses and practitioners more comfort that they are likely confronting only a civil case. And even if prosecutors do investigate, counsel can emphasize the lack of foreign ties as a reason against prosecution.

Conversely, knowing a case does implicate a foreign government or other foreign entity is just as important since it will color every strategic decision a potential defendant takes. For businesses whose trade secrets have been misappropriated, it is important to identify foreign involvement and the increased risk of criminal prosecution that comes with it because, if the government does indict, the company loses some control over potentially sensitive company information that the government must disclose to the defendant under the government's criminal discovery obligations.

### ***Act immediately.***

For potential plaintiffs, prompt action is essential given the relatively short three-year statute of limitations for many civil trade secret claims.[20] Plus, when the suspected misappropriation involves a former employee, businesses must immediately identify and secure the former employee's electronic devices before potential evidence is lost.

For defendants in civil or criminal cases, quick action is equally important. Securing electronic devices immediately can preserve powerful exculpatory evidence, for example, evidence that the defendant independently developed or lawfully obtained the information. And if the facts reveal substantial criminal liability, quick action to disclose the misconduct to the DOJ will help ensure eligibility for one of the department's self-disclosure programs, which condition leniency on prompt disclosure.[21]

## Conclusion

Trade secrets have never been more important. And with the government's growing appetite for criminal trade secret prosecutions, the stakes have never been higher. Businesses and litigants can and should adjust accordingly.

---

*Kenneth E. Notter III is a partner at MoloLamken LLP.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*

[1] See Memorandum from Matthew R. Galeotti, U.S. Dep't of Justice, Focus, Fairness, and Efficiency in the Fight Against White-Collar Crime (May 12, 2025), <https://www.justice.gov/criminal/media/1400046/dl?inline>.

[2] 18 U.S.C. §1831.

[3] 18 U.S.C. §1832.

[4] See 18 U.S.C. §§1956(c)(7)(A), 1961(1).

[5] 18 U.S.C. §§1341, 1343.

[6] 18 U.S.C. §§2314, 2315.

[7] 18 U.S.C. §1030.

[8] Richard S. Scott & Alan Z. Rosenstein, DOJ's Strategic Plan for Countering the Economic Espionage Threat, 64 United States Attorneys' Bulletin 1, 24 (2016), <https://perma.cc/4ZN5-BLQK> (noting United States v. Liew, 2014 WL 2586329 (N.D. Cal. June 9, 2014), was the first jury conviction under 18 U.S.C. §1831).

[9] See *id.*

[10] United States v. Xue, No. 2:16-cr-22 (E.D. Pa.).

[11] United States v. Hailong, No. 4:13-cr-147 (S.D. Iowa).

[12] See Jason C. Schwartz et al., 2016 Trade Secrets Litigation Round-Up, Bloomberg Law (Jan. 27, 2017).

[13] See U.S. Dep't of Justice, Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018, <https://shorturl.at/qZLyw>; Ryan Lucas, The Justice Department Is Ending Its Controversial China Initiative, NPR (Feb. 23, 2022), <https://shorturl.at/D3dUx>; Mike German, The "China Initiative" Failed U.S. Research and National Security. Don't Bring It Back, Brennan Center for Justice (Sept. 23, 2024), <https://shorturl.at/1vaWe>.

[14] See, e.g., Press Release, U.S. Dep't of Justice, Justice Department Announces Five Cases as Part of Recently Launched Disruptive Technology Strike Force (May 16, 2023), <https://tinyurl.com/39acry9n>.

[15] See Justice Manual § 9-59.100, U.S. Dep't of Justice (rev. 2020) (listing factors for prosecutors to consider when deciding whether to indict).

[16] See Janice W. Reicher, 3 Trends in Criminal Trade Secret Prosecution, Farella Braun + Martel, (Jan. 23, 2019), <https://tinyurl.com/3nhnwepk>.

[17] Maxine Bernstein, Former Intel Engineer Sentenced for Stealing Trade Secrets for Microsoft, Oregon Live (Aug. 12, 2025), <https://tinyurl.com/5ydn4653>.

[18] Symantec Study Shows Employees Steal Corporate Data and Don't Believe It's Wrong, Yahoo Finance (Feb. 6, 2013), <https://tinyurl.com/42dbc3kh>.

[19] U.S. Dep't of Justice, Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy (May 12, 2025), <https://tinyurl.com/bdyh9b94>.

[20] E.g., 18 U.S.C. §1836(d).

[21] U.S. Dep't of Justice, Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy (May 12, 2025), <https://tinyurl.com/bdyh9b94>.