Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

January 27, 2023

An Introduction to Trade Secrets Law in the United States

Trade secrets—a form of intellectual property comprising many kinds of confidential information—are widely considered to be important assets for U.S. companies and the U.S. economy as a whole, with examples as varied as search engine algorithms and soft drink formulas. Congress and the states have enacted laws to protect trade secrets, and federal and state courts see a steady stream of trade secrets cases, with more than a thousand filed annually in U.S. district courts in recent years.

Although historically protected mostly by state law, trade secrets have more recently come under the protection of federal civil and criminal laws. Members proposed several bills concerning trade secrets in the 117th Congress, largely in an effort to address the potential risk of trade secret theft by foreign governments and agents. This In Focus provides an overview of how trade secrets are defined and protected under U.S. law and discusses selected legislation introduced in the 117th Congress.

What Are Trade Secrets?

Legal Definition

State and federal laws generally provide that trade secrets may encompass many types of information, including formulas, patterns, compilations, programs, devices, methods, techniques, and processes. To constitute a trade secret, such information must meet two criteria:

- *First*, the information must derive economic value from not being known or "readily ascertainable" by other persons. In other words, a trade secret derives its value—for instance, giving its owner a competitive advantage—from the fact that others cannot easily discover it.

- *Second*, the owner must keep the information secret using measures that are reasonable under the circumstances. Such protective measures may involve, for example, restricting access to the information to specific individuals on a "need-to-know" basis, including limiting physical access to company facilities and files; requiring employees to sign nondisclosure agreements; and securing computer networks.

Differences Between Trade Secrets and Patents

Trade secrets may include, but are not limited to, the types of inventive discoveries that are eligible for U.S. patent protection. For example, the inventor of a new type of manufacturing equipment—or a new way to use such equipment—might have a choice either to apply for a patent on the invention or to maintain it as a trade secret. One advantage of patent protection is that, unlike trade secrets, a patent gives its owner a monopoly that competitors cannot legally circumvent by reverse-engineering or independently discovering the invention. On the other hand, patents require public disclosure of the invention and expire after a certain time—typically, about 20 years—whereas trade secrets may be maintained indefinitely.

Trade secrets may also encompass certain financial or business information that is not patentable, such as supplier lists. The relatively broad scope of potential trade secret (as compared with patent) protection may have taken on greater importance in light of a line of Supreme Court decisions that further restricted the types of inventions that may be patented, including in the software and biotechnology fields. *See* CRS Report R45918, *Patent-Eligible Subject Matter Reform: Background and Issues for Congress*.

What Laws Protect Trade Secrets?

Trade secrets are protected by a combination of state and federal laws, which prescribe a combination of civil and criminal penalties for trade secret "misappropriation"—the improper acquisition, disclosure, or use of a trade secret.

State Laws

State laws generally allow trade secret owners to sue and obtain damages or injunctive relief for trade secret misappropriation. In most states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, these civil suits are governed by the Uniform Trade Secrets Act (UTSA), a statute first published in 1979 and then enacted, with some variation, on a state-by-state basis. The only states that have not yet adopted UTSA are North Carolina, which has enacted a similar statute, and New York, where trade secret misappropriation claims are governed by common law.

Although state courts generally have jurisdiction over UTSA claims, plaintiffs may file certain UTSA lawsuits in U.S. district courts. As with many other kinds of civil suits, plaintiffs may file standalone UTSA claims in federal court if the requirements for "diversity jurisdiction" are met—i.e., the plaintiff and defendant are citizens of different states, and the lawsuit seeks more than $75,000 in damages. A defendant also has the right to "remove" (i.e., transfer) such a lawsuit from state to federal court if the diversity jurisdiction requirements are met and the defendant is not a citizen of the forum state.

Defend Trade Secrets Acts

In 2016, Congress passed the Defend Trade Secrets Act (DTSA) to create a new civil right of action for trade secret misappropriation under federal law. DTSA does not replace state laws such as UTSA, but rather creates a parallel right for plaintiffs to file trade secret misappropriation lawsuits in federal court if "the trade secret is related to a product or service used in ... interstate or foreign commerce."

Supporters contend that DTSA has improved protection for trade secret owners by providing easier access to federal courts and authorizing expedited seizure of property to retrieve stolen trade secrets in some circumstances.

Some critics argue that DTSA is largely duplicative of UTSA and that it has failed to achieve national uniformity in trade secrets law. For example, federal courts have disagreed on whether DTSA authorizes them to restrain employees from taking new positions that would allegedly result in the "inevitable disclosure" of their former employers' trade secrets, reflecting a split in various states' laws. This issue may have new salience given the January 2023 notice of proposed rulemaking by the Federal Trade Commission (FTC) that would ban most non-compete agreements. *See* CRS Legal Sidebar LSB10905, *The FTC's Proposed Non-Compete Rule*.

One potential difference between DTSA and UTSA is their extraterritorial reach (i.e., applicability to conduct outside the United States). A leading district court opinion held that, under DTSA, plaintiffs could recover damages for foreign acts of misappropriation so long as "an act in furtherance" of the misappropriation—such as marketing knock-off products at a trade show—took place in the United States. *See Motorola Solutions, Inc. v. Hytera Communications Corp.*, 436 F. Supp. 3d 1150 (N.D. Ill. 2020). By contrast, the court held that Illinois's UTSA did not reach such extraterritorial conduct. *See id.* A bill introduced in the 117th Congress, the Protect American Trade Secrets Act of 2021 (H.R. 4327), could have further expanded DTSA's extraterritorial scope by codifying that DTSA "shall apply to conduct occurring outside the United States and impacting United States commerce."

Section 337 of the Tariff Act of 1930

In addition to state and federal courts, trade secret owners may file certain misappropriation claims at the U.S. International Trade Commission (ITC) under Section 337 of the Tariff Act of 1930. *See* 19 U.S.C. § 1337. The ITC may issue injunctions to stop the importation of products that harm U.S. industry and are made using misappropriated trade secrets. The ITC may order such relief even if the acts of misappropriation take place outside the United States. *See* CRS In Focus IF12295, *An Introduction to Section 337 Intellectual Property Litigation at the U.S. International Trade Commission*; CRS Report RL34292, *Intellectual Property Rights and International Trade*. A bill introduced in the 117th Congress, the SECRETS Act of 2021 (S. 2067), would have created a separate procedure allowing the ITC to investigate and bar the importation of articles produced using trade secrets misappropriated "by a foreign agent or foreign instrumentality" on national security grounds.

Economic Espionage Act

The Economic Espionage Act of 1996 (EEA) made it a federal crime to misappropriate trade secrets for either foreign espionage or commercial purposes. Under this law, the crime of economic espionage consists of stealing a trade secret to "benefit any foreign government, foreign instrumentality, or foreign agent" and may be punished by fines on both individuals and organizations and prison sentences of up to 15 years. The crime of commercial theft consists of stealing a trade secret to "injure any owner of that trade secret" and may be punished by fines and prison sentences of up to 10 years.

The involvement of foreign governments or agents is a factor that the Department of Justice (DOJ) considers in deciding whether to file charges under EEA. For example, in January 2023 an ex-General Electric employee was sentenced to two years in prison for conspiring to steal the company's trade secrets regarding gas and steam turbines to benefit the People's Republic of China. DOJ has focused largely on addressing intellectual property theft and espionage by China's government and associated actors, although it has cautioned that this focus should not give the impression of intolerance or bias against Chinese people or chill legitimate academic and research collaborations.

Considerations for Congress

The 117th Congress considered several bills concerning trade secrets, including the two noted above (H.R. 4327 and S. 2067). Such bills largely addressed the perceived threat of misappropriation by non-U.S. persons. One such bill, the Combating Chinese Purloining (CCP) of Trade Secrets Act (S. 1245), stated that "China has expansive efforts in place to acquire United States technology, including sensitive trade secrets and proprietary information."

A number of bills introduced in the 117th Congress would have authorized penalties, including immigration restrictions, against non-U.S. persons who steal trade secrets. The CCP Act and the Stop Theft of Intellectual Property Act of 2021 (S. 1409) would have rendered aliens who violate EEA and certain other laws inadmissible and deportable under U.S. immigration law. Similarly, the Protecting American Intellectual Property Act of 2022 (S. 1294) would have denied or revoked U.S. entries and visas to individuals the President found to have knowingly engaged in, benefited from, or provided support to trade secret theft posing "a significant threat to the national security, foreign policy, or economic health or financial stability of the United States." That bill and the CCP Act also would have authorized several additional sanctions against foreign entities that misappropriate trade secrets, including trade restrictions, ineligibility for Export-Import Bank and other financial assistance, and exclusion of certain corporate officers from the United States.

Some bills from the 117th Congress also sought further fact-finding on trade secret misappropriation by other countries. The Countering Chinese Espionage Reporting Act (H.R. 7325) would have required the Attorney General to submit annual reports on efforts to counter "Chinese national security threats and espionage in the United States, including trade secret theft." Similarly, the CCP Act would have required the Attorney General to submit an annual report on trade secret misappropriation by foreign countries.

Looking ahead, Congress may also consider whether DTSA should be amended based on the federal courts' early years of experience deciding cases brought under this statute.

Christopher T. Zirpoli, Legislative Attorney

Disclaimer