IN-DEPTH

Trade Secrets

USA

LEXOLOGY

Trade Secrets

EDITION 1

Contributing Editor

Wil Rao

McAndrews, Held & Malloy Ltd

In-Depth: Trade Secrets offers a detailed examination of trade secret law across key jurisdictions. Each chapter addresses core principles of trade secret law, recent legislative changes, significant cases, and practical strategies for protecting trade secrets and handling claims.

Generated: November 1, 2024

USA

Rocco Screnci and **Wil Rao**
McAndrews, Held & Malloy Ltd

Summary

Introduction

Trade secret law in the United States should be at the forefront of the agenda for all businesses. Trade secret protection and enforcement are complex and legally nuanced areas, and each requires much more than a light-touch legal assessment.

This chapter explores some of the recent, key developments in trade secret protection and enforcement. As one recent development, in federal litigation, trade secret law received some needed clarity about the geographic reach – specifically, the scope of available protection domestically and abroad – of the Defend Trade Secrets Act (DTSA),[1] which governs federal trade secret law. Another development is that trade secrets damages law was further complicated by an appellate court that cut off damages that some other courts had held available for trade secret misappropriation.

Outside the US courts, the Federal Trade Commission (FTC) proposed regulations to impose an unprecedented, nationwide mandate on businesses banning employee non-compete agreements; however, the courts put the brakes on that agency overreach by preventing the FTC from enforcing the nationwide mandate, which has, at least for now, forestalled the consequences that the mandate would have had on the US economy.

In view of these recent developments, this chapter provides additional insight into and a review of the legal and practical considerations relevant to protecting commercially sensitive information in the United States.

Year in review

Many significant trade secret cases have been decided in the past year. They have addressed various issues both at the federal and state courts. At the federal level, the DTSA marked its eighth year in force. It has reshaped litigation options for trade secret owners in the US courts. There has been a steady annual filing of trade secret claims in federal court (which does not require diversity of litigants for jurisdiction).

The DTSA's relatively recent enactment means that the courts' analysis of it is still in its infancy. Over the past year, a number of 'hot topics' in US trade secret law have arisen, including the topics of monetary damages, injunctive relief, trade secret identification and adequacy of pleadings.

The most popular venues for DTSA litigation are the Northern District of Illinois, the Southern District of New York and the Central District of California.[2] In total, 10 federal district courts located in just seven states were responsible for nearly 40 per cent of all federal trade secret cases filed between 2021 and 2023.[3]

Cases

Foreign sales may be recoverable damages under DTSA

A major development over the past year involves a company's ability to protect its trade secrets both within and outside the United States under the DTSA. In *Motorola v. Hytera*,[4] the Court of Appeals for the Seventh Circuit addressed the extraterritorial scope of the DTSA.

In *Motorola*, 'a large and blatant theft of trade secrets' was alleged to have occurred via Motorola's Malaysian servers by China-based Hytera. In advancing its theft, Hytera poached several engineers from Motorola who, upon their departure from Motorola, downloaded thousands of technical documents and pieces of source code for digital mobile radios from Motorola's Malaysian servers. Hytera then used the trade secrets contained in the stolen documents to develop and sell their own competing radio products.

Following a three-month jury trial, a jury awarded US$765 million in damages for trade secret misappropriation and copyright infringement. The district reduced the damages award to US$543.7 million, denied a permanent injunction and awarded an ongoing royalty on products adjudicated at trial. These damages included compensatory damages for conduct (e.g., sales) that happened outside the United States.

On appeal and cross-appeal, the parties challenged the district court's damages award and denial of permanent injunction. One of the central issues on appeal was whether the DTSA could apply to conduct that occurred outside the United States.

On appeal, the Seventh Circuit ruled in favour of Motorola, concluding that the DTSA's plain language contemplates foreign misappropriation of trade secrets and, therefore, rebuts the presumption against extraterritoriality. It found that the DTSA applies to trade secret misappropriation that occurs abroad if there is a sufficient connection to the United States. To this end, the Court focused on the text of the statute, which allows for the extraterritorial application of the DTSA so long as an 'act in furtherance of the [misappropriation]' happened within the United States.

The above means that defendants can be held liable for trade secret misappropriation abroad if an act perpetuating misappropriation happened within the United States. Because Hytera sold and promoted its radios within the United States, it acted in furtherance of its worldwide misappropriation of Motorola's trade secrets. This decision strengthens trade secret protection in the United States by ensuring that trade secret owners are compensated for not just harm suffered within the United States, but wherever the plaintiff suffered injury.

Avoided costs damages are not available in the Second Circuit under DTSA

Another notable development in US trade secret law involves what components of a trade secrets damages claims are recoverable – specifically, whether the 'avoided costs' of the defendant for not developing trade secrets on its own are recoverable. In *Syntel v. TriZetto*-,[5] the court concluded that avoided costs are not recoverable under the DTSA.

The dispute involved trade secret owner TriZetto, which develops software, and Syntel, with whom TriZetto had subcontracted to support its software users for software updates and implementation. As part of the subcontract agreement, Syntel agreed to forgo soliciting its own clients in exchange for an annual payment from TriZetto. During the relationship, TriZetto shared its trade secrets with Syntel to better service TriZetto's software. But after

the subcontracting agreement ended, Syntel continued using TriZetto's trade secrets to service Syntel's client base in violation of the parties' agreement.

A jury awarded TriZetto US$285 million in compensatory damages for the misappropriation. The award was based on an avoided costs theory: it reflected what TriZetto spent to develop the trade secrets, which are costs that Syntel avoided by not developing its own trade secrets.

The appeals court vacated the jury's damages award and held that avoided costs are not available under the DTSA. It explained that, although the DTSA allows for unjust enrichment damages, those damages must only be awarded after examining the other factors in the case, like the nature and extent of the misappropriation and the adequacy of other remedies. Because the jury assigned lost profits damages of US$8.5 million and the trial court enjoined further use of TriZetto's trade secrets, the appeals court reasoned that the avoided costs were inappropriately punitive rather than compensatory and, therefore, forbidden under the DTSA.[6]

This decision is significant for several reasons. First, it eviscerated a massive damages verdict for the trade secret owner by leaving TriZetto without compensatory damages (although TriZetto still walked away with US$285 million in punitive damages and an additional US$15 million in attorneys' fees).[7] Second, and more importantly, it created tension among the US appellate courts on whether avoided costs are recoverable for trade secret misappropriation. So far, the other courts that have weighed in on the issue have generally concluded that avoided costs are recoverable for trade secret misappropriation, making it evident that the *Syntel* decision is an outlier.[8]

Recognising this appellate court disagreement allows trade secret owners (and their plaintiff's counsel) to appreciate there are risks of not being awarded substantial avoided costs damages based on where the suit is brought, and that the split in authority might lead to an unfavourable outcome in a jurisdiction where the trade secret owner has favourable authority. As a result, trade secret owners should factor in available damages in deciding where to file suit for trade secret misappropriation.

Preliminary injunction grants require careful balancing

In *Insulet v. EOFlow*,[9] the Federal Circuit reversed the district court's preliminary injunction involving wearable insulin pump technology.

Insulet launched its Omnipod insulin pump in 2006. In 2011, defendant EOFlow began developing it EOPatch insulin pump. Nearly a decade after Insulet's launch and around the time of former employees of Insulet joining EOFlow, EOFlow received regulatory approval in South Korea. In 2023, Medtronic was reported to have interest in acquiring EOFlow. Insulet sued EOFlow in response to the Medtronic reports, alleging trade secret misappropriation under the DTSA.

The district court issued a preliminary injunction. In reversing the injunction, the Federal Circuit found that the district court's equitable determination granting the preliminary injunction failed to consider, or properly consider, in its balance, among other things, the three-year statute of limitations, a suitable definition and scope of the asserted trade secrets, the existence of misappropriation, the extent of reasonable measures taken,

whether patent filings publicly disclosed the trade secrets and whether the trade secrets could be reverse engineered.

State court damage awards remain sizeable and trade secrets need a definition

In *Zunum Aero v. Boeing*,[10] a in federal district court jury awarded Zunum Aero over US$90 million on Zunum Aero's trade secret and tortious interference claims, which the court reduced to US$71.9 million to account for Zunum Aero's failure to mitigate approximately US$20 million in damages.

Zunum Aero is an electric aircraft start-up company. It claimed that investor Boeing and a Boeing venture arm, Horizon X, misappropriated its trade secrets related to hybrid-electric and all-electric aircraft technology. Throughout the case, the parties disputed the identification and definition of the asserted trade secrets. The district court drafted its own definitions for the jury after Zunum Aero offered a 550-page compilation and Boeing offered an unsuitably vague definition.

Need for sufficient trade secret definition and scope

In *Alifax Holding v. Alcor Scientific*, the Federal Circuit concluded that Alifax's 'signal acquisition' trade secret was not 'describe[d] . . . with sufficient detail', nor was 'its proper scope'.[11] It also reinstated the jury's verdict finding misappropriation of Alifax's 'conversion algorithm' trade secret, but it remanded for a new trial on damages.[12]

The trade secrets involved instruments for automating blood sample analysis for inflammation diagnosis. Alifax alleged that its former president of research development was hired by the defendant Alcor Scientific and thereby obtained Alifax's trades secrets. Alifax alleged that Alcor's access to the trade secrets allowed it to launch a competing automated blood sample instrument like Alifax's. The alleged trade secret misappropriation claim was under the Rhode Island Uniform Trade Secrets Act.

At trial, the judge at the charge conference struck the signal acquisition trade secret because there was no support for it being a trade secret. At the charge conference, the court struck the alleged signal acquisition trade secret from the jury verdict form, determining that there was no recorded evidence to support its status as a trade secret. The jury found misappropriation of the conversion algorithm and awarded US$6.5 million in damages.

The judge granted a motion for a new trial on damages, finding the jury verdict was against the clear weight of the evidence. Alifax appealed, arguing, among other things, that the district court erred in withholding the signal acquisition trade secret from the jury. The Federal Circuit disagreed.

Record-setting damages verdict overturned on appeal

In *Pegasystems v. Appian*,[13] the Court of Appeals of Virginia set aside Pegasystems's US$2 billion verdict for trade secret misappropriation. Pegasystems and Appian are both software developers that offer software platforms that other companies use to build complex applications to automate business processes.

A jury found that Pegasystems misappropriated five features of Appian's software platform and awarded just over US$2 billion in damages. To arrive at the number, the jury was instructed that Appian simply needed to prove how much Pegasystems made in sales, while Pegasystems bore the burden of proving how much of those sales were not attributable to misappropriation.[14] That instruction made it so every Pegasystems sale – even sales for product lines not accused of misappropriation – was presumably a result of the misappropriation unless Pegasystems could prove otherwise.[15]

On appeal, the Court of Appeals of Virginia vacated the verdict and held that the damages instruction was legally flawed because it wrongly placed the burden of proving proximate cause on Pegasystems. This means that, on remand, Appian will need to prove how many of Pegasystems's sales are attributable to the misappropriation.[16]

Another noteworthy aspect of this case was the court's discussion of Appian's identification of its trade secrets. At trial, Appian spent nearly three days and over 800 transcript pages to have its expert spell out precisely which software functionalities were trade secrets and how Pegasystems incorporated them into its technology.[17] This satisfied Appian's duty to identify its trade secrets with enough detail to inform the jury of their scope.

More interestingly, however, Appian identified as trade secrets information that Pegasystems exposed about Appian's weaknesses and how competitors could exploit them. To this end, Appian showed the jury exhibits of Pegasystems' marketing materials that revealed the flaws in Appian's software.[18] That, too, was enough to satisfy Appian's burden to identify its trade secrets with adequate specificity.

Bar for sufficiency of a trade secret definition must be met

In *Equate Media v. Suthar*, the Ninth Circuit concluded that the plaintiffs sufficiently identified the trade secrets, reversing the district court's grant of judgment as a matter of law and ordering that the jury verdict be reinstated.[19] The trade secrets involved marketing data, source code and confidential pricing information. The complaint construed it as:

> (1) Plaintiffs' Marketing Data, including [Google] Keywords, Themes, and Conversion Rates that Plaintiffs have gathered over 15 years, (2) proprietary source code developed by Plaintiffs that created multiple systems working together that allowed Plaintiffs to run their online business, and (3) confidential customer and pricing information.[20]

At trial, a jury decided for the plaintiffs, awarding US$1.4 million to Equate Media. After trial, however, the district court granted judgment as a matter of law in the defendants' favour, concluding that the plaintiffs had not clearly identified any trade secrets. In reversing, the Ninth Circuit concluded that the trade secret owner 'presented sufficient evidence to permit the jury to conclude that they possessed trade secrets in Google ad data'.[21] Following the reversal, the district court entered an injunction in March 2024 that prevents the defendant from disclosing or otherwise using the trade secrets.

Information and belief allegations can be sufficient

In *Ahern Rentals v. EquipmentShare*, Ahern Rentals alleged, on 'information and belief', that the defendant competitors misappropriated its trade secrets involving the construction rental industry.[22] Its complaint was dismissed by the district court. The district court held that that allegations that are pleaded only on information and belief are insufficient.

The Court of Appeals for the Eighth Circuit reversed the holding. It concluded that 'the district court erred by summarily rejecting [plaintiff's "information and belief"] allegations' and explained that such allegations are permissible if they are 'based on information that is within the possession and control of the defendant or are supported by sufficient factual material that makes the inference of culpability plausible'.[23]

Proof of ownership requires proffers from which jury can reasonably infer ownership

In *Highland Consulting v. Soule*, the Eleventh Circuit affirmed the district court's denial of the defendant's motions for judgment as a matter of law, or alternatively for a new trial on this ground.[24] The Eleventh Circuit rejected the defendant's claim that the plaintiff failed to establish trade secret ownership and explained that the plaintiff stamped trade secret documents with its marketing name, and the trade secret owner's testimony regarding those documents allowed a jury to reasonably infer that the plaintiff owned the trade secrets, notwithstanding that the plaintiff's foreign affiliates were using the trade secrets contained in the documents. The misappropriation claim was made under DTSA, and the jury awarded damages of US$1.2 million.

Lack of reasonable measures when unrestricted emails sent

In *Pauwels v. Deloitte*, the Second Circuit affirmed the district court's dismissal of the plaintiff's claims for failing to adequately protect his trade secrets.[25] Pauwels contended that the 'Pauwels Model' was a trade secret.[26] While the Pauwels did control distribution of Pauwels Model spreadsheets to the defendant and secured some oral agreement to keep the information confidential from the defendant, the Second Circuit explained that the complaint failed to set forth any reasonable measures to protect the spreadsheets, such as password protection or encryption or otherwise labelling the spreadsheet.[27]

There was no evidence of non-disclosure agreements; there were only asserted oral arrangements. However, there was evidence that Pauwels sent the Pauwels Model spreadsheets in an unrestricted manner to individuals at the defendant and without any assurance to maintain the secrecy of the information. In short, there were no legal obligations restraining the defendant from disclosing the spreadsheets.

Employee's sending of trade secrets via personal email is unauthorised use

In *TWC Concrete v. DeCarlo*, the district court issued a temporary restraining order against the defendant DeCarlo and did so after concluding that DeCarlo's act of sending trade secret information to his personal email, in violation of employment, is by itself unauthorised use of a trade secret.[28] At issue was the plaintiff's financial statement.

The financial statement included confidential customer names, contract values, budget information and estimate costs of contract. The court found that information derived independent economic value from not being generally known or readily ascertainable by a

competitor, and that reasonable measures to maintain secrecy were adequate – measures that included limited distribution to persons who signed non-disclosure agreements.

Defendants early access to asserted trade secrets necessary to fair defence

In *Jane Street v. Millennium*, the district court compelled the disclosure of the asserted trade secrets before the disclosure of the trade secrets during the normal course of responding to discovery (e.g., interrogatory responses).[29] Jane Street asserted its option trading trade secrets that were alleged to have been misappropriated under the DTSA and New York trade secret law by ex-employees and the ex-employee's new employer. The trade secrets involved an options-trading strategy for India.[30]

The defendant, before answering, requested a particularised trade secret disclosure. The plaintiff refused. It indicated it would provide the information in response to interrogatory responses. The court also refused to limit the disclosure to 'attorneys' eyes only' as the plaintiff requested, and it allowed disclosure to the individual defendants and designated in-house counsel. The court's reasoning was that not allowing the disclosure would fail to give defendants fair notice.[31] It would deprive them of their ability 'to adequately defend the company' and impinged on their outside counsel's ethical obligation to inform and advise their clients.[32]

Non-compete agreements

Total Quality Logistics v. Leonard

In *Total Quality Logistics v. Leonard*, the Ohio Twelfth District Court of Appeals reversed the trial court's denial of the plaintiff's motion for summary judgment that Leonard breached her non-compete agreement.[33] The Court held that, where a non-compete agreement is needed to protect an employer's legitimate interest, it will be upheld in Ohio.[34] To this end, the Court explained that an agreement restricting competition is reasonable as long as it has a reasonable scope to protect the former employer, is not an undue hardship on the former employee and does not injure the public interest.[35] The defendant had left the plaintiff, joined a competitor and solicited the plaintiff's customers for the competitor. At the time, the defendant was on administrative leave from the plaintiff.

Administrative agency actions

Non-compete agreements are a common tool used by businesses to protect potential disclosure of trade secrets.

In 2023, the Biden administration, through the FTC, proposed a ban on non-compete clauses in employment contracts, which would take effect in 2024.[36] The justification of the ban was to increase job mobility and enhance competition in the labour market.

The FTC-proposed rule was quickly challenged in court. Challenges to the rule often centred around arguments that the rule overstepped the FTC's regulatory authority.

On 20 August 2024, a federal district court enjoined the FTC from enforcing the rule banning non-compete clauses.[37] The court held that the rulemaking exceeded the

FTC's authority. The decision means that, for now, employers may continue to enforce non-compete clauses under existing laws and contractual terms. The ongoing legal battles will determine whether the FTC's ban will eventually go into effect or be significantly modified.

Securing trade secret protection

Trade secrets are protected in the United States by federal legislation – the DTSA – and on a state-by-state basis. Fortunately, there are few differences between federal- and state-level trade secret protections because the federal trade secret legislation was modelled after the Uniform Trade Secrets Act (UTSA), which almost all 50 states have enacted in some form.[38] For the sake of brevity, this section focuses on federal trade secret law but identifies important differences with state law.

Definition of trade secret

Information must be commercially sensitive

The United States affords broad trade secret protection to commercially sensitive information. A trade secret can include 'all forms and types of financial, business, scientific, technical, economic, or engineering information'.[39] In effect, that definition can extend to virtually any commercially valuable information. Some courts have extended trade secret protection to the genetic information of agriculture or livestock.[40] Other common examples of information that usually qualify as trade secrets include secret recipes or formulas, internal pricing information and source code.

Not all commercially valuable information qualifies as a trade secret: to qualify as a trade secret, the information must meet two other requirements.

Economic value is derived from secrecy of information

The first requirement is that the information must 'derive[ ] independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information'.[41] In other words, the information itself is not inherently valuable; the value of a trade secret comes from its secrecy – 'from not being generally known' – and its difficulty to be learned through 'proper means'.

This means that well-known public information cannot qualify for trade secret protection. Information that is 'ascertainable through proper means' encompasses information that is indirectly revealed, such as by public disclosure of a related product or service. For example, while a device's blueprint might not be public knowledge, the device's design will not qualify as a trade secret if it can be reverse engineered and reproduced.[42]

At the same time, not all information that is technically available to the public is barred from qualifying as a trade secret. A classic example is a compilation of information (e.g., a customer list) that includes public information (e.g., addresses and phone numbers).

Because the hallmarks of a trade secret are that it is not readily ascertainable and provides a competitive advantage through its secrecy, courts examine how a compilation containing public information functions within a business and whether it could be easily recreated. With a customer list, for example, courts ask whether the customers on the list are readily ascertainable as prospective customers of the business's goods or services, or whether the compilation was uniquely generated from years of marketing and advertising efforts.-[43] Evidence of the latter indicates that the list could not be easily reproduced through proper means and is, therefore, more likely to receive trade secret protection.[44]

Reasonable measures have been taken to keep information secret

The second requirement for trade secret status is that the owner of the commercially valuable information 'has taken reasonable measures' to ensure it remains secret.[45] For measures to be reasonable, they need not be perfect. Although the reasonableness of any particular measures varies depending on the nature of the information and the industry,[46] some common best practices have emerged:

1. affixing stamps or labels to denote that a document is 'Confidential';
2. restricting access to documents either physically (e.g., lock and key) or digitally (e.g., password requirements); and
3. imposing confidentiality policies or requiring non-disclosure agreements before allowing access to commercially sensitive information.[47]

Nevertheless, there is no one-size-fits-all solution to ensuring adequate security. Courts evaluate reasonableness on a case-by-case basis and typically leave the ultimate determination for the factfinder – often a lay jury – to decide based on the costs and benefits of the particular security measures.

Another key consideration in deciding whether confidentiality measures are adequately reasonable hinges on the relationship between the parties. For instance, in cases where the parties have little to no pre-existing relationship or are engaged in an arm's-length transaction, binding non-disclosure agreements with all the relevant parties are typically required.

As an example, a recent case addressing this issue involved a business pitch for a financial services product to a third-party insurance company. Although the owner of the alleged trade secrets had entered into non-disclosure agreements with other third parties who set up the pitch meeting, it had not entered into a non-disclosure agreement with the insurance company to whom the pitch was directed.[48] As a result, the information was not kept adequately confidential to form the basis of a trade secret claim.[49]

Employment relationship

By contrast, the employer–employee relationship already imposes implicit duties on employees to act in their employer's interests, so courts often award trade secret protection to information disclosed to employees absent a binding non-disclosure agreement.[50] But as a recent case highlights, employers must still take some affirmative measure to keep the information safe from disclosure.

In *In re Island Industries*, the court of appeals affirmed the dismissal of a trade secret claim because the employer exclusively relied on the common law fiduciary duty of confidentiality.[51] Because the owner of the alleged trade secret must impose reasonable measures to preserve confidentiality, the owner cannot rely solely on a duty imposed by common law. If the employer had imposed minimal affirmative measures (e.g., company policy requiring confidentiality or limiting access to the information), the case likely would have been decided differently.[52]

In sum, the evaluation of reasonable measures varies depending on the totality of the circumstances in each case. At a minimum, reasonable measures require a sufficiently confidential relationship (whether by explicit agreement or implied at law) and some affirmative steps, such as a written policy or clear access restrictions, to preserve secrecy of the commercially sensitive information.

Measures to protect trade secrets

Duration of trade secret protection

While reasonable measures are a legal requirement for trade secret protection in the United States, businesses may want to consider implementing extraordinary measures to preserve their trade secrets, particularly because trade secrets are a valuable tool in a business's intellectual property arsenal.

Unlike patents and copyrights, trade secrets have no predetermined lifespan, meaning that they can last in perpetuity as long as they remain secret and commercially valuable. There are also no transactional costs associated with registering trade secrets with an administrative agency since trade secrets are not registered with or examined by the government. A well-guarded trade secret can often provide even stronger protection than patents (which can often be easily designed around), copyrights (which are often subject to online piracy) and trademarks (which must be vigorously policed and are often copied by knock-off products).

Departing employees

Trade secret owners may want to consider where their security measures are most vulnerable and how to strengthen those measures. One common scenario is when an employee with access to sensitive information leaves to work for a competitor. While requiring all employees to sign non-compete and non-disclosure agreements can help deter potential trade secret theft and strengthen any resulting legal claims if theft occurs, they still leave businesses susceptible to departing employees who either did not read or do not care to honour their agreements. Further, if non-compete agreements are banned entirely (as they already are in California), employers are at a bigger disadvantage in preventing trade secret misappropriation.

For these reasons, employers should consider implementing additional cybersecurity measures and offboarding policies when employees leave a company. These policies could include requiring prompt return of any company property, restricting access to

sensitive documents immediately upon learning of an impending departure and monitoring the departing employee's access to sensitive information.

Generative AI

Another nascent issue is the proliferation of generative artificial intelligence (AI). For example, use of generative AI has become prevalent for mundane tasks like writing emails. This can be dangerous because some generative AI is trained by using the inputs provided by a given user. As a result, someone who uses generative AI must be careful to ensure that no commercially sensitive information is used to prompt the AI output.

To prevent inadvertent disclosure of trade secrets when using generative AI, a good place to start is to ensure that employees understand and are adequately trained on a company's confidentiality policies. It is also important to update these policies and training materials to confront new technologies, such as identifying which programs are appropriate and for what uses.

Proving trade secret theft

But even all the above steps may not be enough to stop trade secret theft, as a crafty employee (or competitor) may begin funnelling sensitive information out of the company or to a competitor before announcing their departure for a rival company. When that happens, a business's task transforms from preventing theft to mitigating its consequences. The best way to do this is to have proof of what was stolen. Gathering evidence may include keeping track of what the employee accessed in the weeks or even months before joining a competitor.

Another way to help prove what the employee stole is by leaving 'fingerprints' in particularly sensitive algorithms, formulas and recipes, among other similar types of information. These fingerprints can be anything that helps uniquely tie the trade secret information to its source and, therefore, prevents any assertion that the information was generated independently through proper means. A common fingerprinting technique for software involves introducing innocuous errors (e.g., typos) into the source code. These errors should not affect how the code ultimately works and should ideally be hard to detect upon careful inspection, but their presence is compelling evidence that the information was stolen given that it is unlikely that both the trade secret owner and the alleged copier made the same mistake.[53]

Downsides of relying on trade secret protection

In implementing an effective intellectual property strategy, businesses should also be aware of the downsides of relying on trade secrets. Because trade secrecy is like Pandora's box – once information becomes public knowledge, trade secret protection is gone – businesses should leverage other forms of complementary intellectual property when appropriate. Patents, for example, are better suited to protect inventions that are easily reverse engineered or sufficiently mimicked by competitors. Copyrights can also prove particularly valuable for protecting software or creative materials, such as marketing plans.

Another downside to relying on trade secrets is that they can be harder to enforce because the United States prioritises public access to legal proceedings, lay juries and robust discovery procedures, all of which can lead to potential disclosure of trade secrets. For similar reasons, the lack of formal registration for, and consequences of, public disclosure of trade secrets makes buying, selling and licensing trade secrets harder than other forms of intellectual property.[54] For instance, simply pitching a product or service can lead to disclosure – and, therefore, destruction of trade secret protection – of the very information trying to be sold.[55] In these situations, it is crucial that the trade secret owner ensures that all parties present have signed a valid non-disclosure agreement before sharing any sensitive information.

Enforcement of trade secrets

When faced with potential theft of trade secrets, it is important that businesses act quickly but carefully. Sometimes trade secret misappropriation claims can be handled informally when the improper acquisition of information happened inadvertently, like when a departing employee forgets to return company property (e.g., a laptop computer) that contains sensitive documents. But other times informal resolution is unlikely or impossible. In those cases, having a litigation strategy in place at the start is crucial to success.

Businesses should consider what they want to accomplish in pursuing trade secret claims, how they can best do so and the potential problems they may encounter in pursuing a misappropriation claim. From there, the business can fine-tune its litigation strategy to best serve its interests. This section explores a few key decisions that businesses will need to make in protecting their trade secret rights.

Choice of court

The first major decision in any lawsuit is deciding where to sue. These decisions are particularly complicated in the United States because of the interaction between state and federal law and their respective court systems. State and federal laws operate within their own spheres of authority and have different scopes and sources. State laws apply within the boundaries of individual states, and each state has its own legal system, including its own legislature, judiciary and executive branch of government. Federal laws, by contrast, apply across the entire United States, and there is also a federal judiciary, legislative and executive branch.

Despite these differences, state and federal courts often have the authority to hear claims based on both federal and state law. This means that, depending on the circumstances, trade secrets can be brought in the courts of either system. And while state courts often share many similar rules and procedures with the federal courts, not all state courts are alike. Likewise, even though federal courts follow a uniform set of rules, the experience of individual judges varies wildly throughout the United States because of the regionality of certain types of litigation. For example, judges in federal courts located in California, Delaware, Illinois, New York and Texas are often more familiar with complex business litigation because many companies are incorporated or headquartered there

and, therefore, tend to file lawsuits in the federal courts responsible for those geographic regions.

Given that trade secret cases can be complex and intense, it is advisable to try filing a suit in a jurisdiction that can handle the intricacies of trade secret litigation. That said, the nuances of picking where to sue can be much more complicated than picking which court generally has more experienced judges, so it always helps to seek the advice of attorneys familiar with the day-to-day practice in each jurisdiction.

Choice of claim

The next major decision is deciding which claims to bring. In general, a state law claim requires that the alleged conduct occurred within the state. To bring a federal claim for trade secret misappropriation, however, the trade secrets must relate 'to a product or service used in, or intended for use in, interstate or foreign commerce'.[56]

This is a relatively low bar: products or services are involved in 'interstate or foreign commerce' if any part of the transaction crosses state or international lines.[57] In other words, businesses can bring federal trade secret claims if the allegedly misappropriated information relates to products or services sold in multiple states or countries.

Key differences between federal and state law

Other than the threshold difference between state and federal law on trade secret misappropriation, trade secret laws within the United States are relatively uniform. Even so, there are a few important distinctions worth considering when bringing a claim.

Civil seizure

Perhaps the most important difference is that federal law includes a civil seizure mechanism, while state law does not. This seizure mechanism lets a trade secret owner apply for a court order to seize the stolen information without giving the defendant notice or chance to oppose the seizure.[58] For that reason, civil seizure is exceedingly rare and should only be allowed in 'extraordinary circumstances' and to 'prevent the propagation or dissemination' of the stolen trade secrets.[59]

Because US courts are empowered to enter temporary restraining orders (which also enjoin defendants through a separate procedure in which the defendants cannot participate), the civil seizure remedy under federal law is generally reserved for when the defendant will not comply with court order, so the property must be seized to ensure its safekeeping.[60]

To succeed in seeking a civil seizure order, a plaintiff must also show that:

1. it will suffer immediate irreparable injury absent the seizure;
2. the potential harm outweighs the defendant's legitimate interests;
3. the information is a trade secret and will likely be misappropriated by the defendant;
4. the defendant has possession of any information or property to be seized; and
5. the property or information to be seized would likely be destroyed or concealed if the defendant were given notice of the position.[61]

Additionally, the plaintiff must describe the property to be seized with adequate particularity and refrain from publicising the request for seizure.[62]

Although these requirements are difficult to meet, a seizure order can be vital in securing a company's most sensitive information.

Damages

The damages available for trade secret misappropriation can vary between state and federal law. For instance, in a recent decision, the federal appeals court responsible for the geographic region covering Connecticut, New York and Vermont interpreted federal law as precluding avoided-cost damages. Avoided-cost damages measure how much the defendant saved by stealing the trade secrets by looking at what it cost the plaintiff to generate them independently.[63]

In interpreting federal law as such, the court fractured from other courts that had interpreted various state trade secret laws to allow such damages.[64] This means that a federal claim brought in Connecticut, New York, or Vermont federal courts may face difficulty in evaluating the amount of damages appropriate for the misappropriation.

With that in mind, businesses faced with misappropriation that is hard to quantify in terms of dollars lost may want to consider looking elsewhere to bring misappropriation claims.

Level of protection

In some cases, state law may offer more protection than federal law. Under federal law, courts cannot stop (enjoin) a person from entering into an employment relationship.[65] But states that have enacted the UTSA do not share similar restrictions.[66]

In a similar vein, state laws generally provide a cause of action and remedy for threatened misappropriation under the 'inevitable disclosure' doctrine, but federal law does not.[67] The inevitable disclosure doctrine allows courts to enjoin individuals from employment with a competitor even absent a non-compete agreement or evidence of bad intentions from the departing employee in seeking competing employment.[68]

Inevitable disclosure cases generally involve individuals with high-ranking positions and intimate knowledge of commercially sensitive information that simply cannot be forgotten, who leave to work for direct rivals.[69] The logic is that, under those circumstances, it is practically impossible for the employee to refrain from using, directly or indirectly, their former employer's trade secrets to benefit their new company.[70]

Even though inevitable disclosure cases rarely prevail,[71] the ability to block employees from joining competitors after having years of access to confidential information can be a powerful tool in preventing misappropriation before it happens, which is uniquely possible under state laws.

Timing

Another important consideration at the onset of a trade secret case is timing. The reality is that trade secret cases are long, complex and often involve additional claims, such as for breach of contract or infringement of patents and copyrights. This reality is reflected in the data showing the timelines for major events in trade secret cases: for cases terminated between 2021 and 2023, the median case took 716 days – nearly two years – reach summary judgment, which is the point in the case, typically after discovery closes, when the court can resolve any dispositive issues of law based on the evidence viewed in the light most favourable to the non-moving party.[72]

The timeline for cases that make it to trial is longer still: the median case went to trial in just over 1,000 days (almost three years) after it was filed, and the longest time to trial for cases resolved between 2021 and 2023 was over eight years at a staggering 2,939 days from filing to trial.[73]

But even years of litigation in the trial court is likely not the end of a trade secret case as litigants have a right to appeal following disposition of the case at the trial court level. For appeals that were terminated between 2021 and 2023, the median time to termination was almost 10 months.[74] And depending on the outcome of that appeal, litigants may see themselves back in the trial court for a second round of summary judgment or trial.

And yet, despite these lengthy timelines, the median time to resolution for federal trade secret cases terminated between 2021 and 2023 was less than one year.[75] This suggests that most litigants favour early settlement rather than a protracted dispute.

Identification of trade secrets

Remedies play a key role in deciding where to sue and what claims to bring when facing trade secret misappropriation. But there are more issues that need to be addressed once a suit is filed.

One major legal issue present in many trade secret cases is the issue of identifying trade secrets. While courts do not require a precise identification of the trade secrets in the publicly filed complaint (as doing so would extinguish any trade secrets), they do require that plaintiffs describe its trade secrets with particularity during the discovery process. That detailed description is needed to give the defendant adequate notice of what it allegedly stole, to ensure that the information qualifies as a secret and to allow a jury to decide whether the alleged trade secrets were misappropriated by giving a precise description of their scope.

This can be a double-edged sword: too specific of a description may lead to public disclosure of the information (especially if the case goes to trial) and, therefore, abandonment of trade secret protections going forward; too general of a description may make it too hard to identify what was actually stolen. In a recent case, for example, the court struck a jury instruction identifying the alleged trade secret because the description lacked adequate detail and failed to identify the proper scope of the secret.[76]

Identifying trade secrets with adequate specificity is also important to preserve victories on appeal. In another recent case, an appeals court reversed a preliminary injunction for a similarly inadequate identification of trade secrets by the trial court.[77] There, the court enjoined an insulin pump maker from selling products that were allegedly developed using the plaintiff's trade secrets after four employees left the plaintiff to join the defendant

company.[78] But because the trial court defined those trade secrets to broadly include non-confidential sources of information (e.g., patents, which are public information), the appellate court found that the trial court abused its discretion in issuing a broad injunction that prevented otherwise completely lawful conduct.[79] This likely could have been avoided with a more careful identification of the relevant trade secrets, as there was seemingly evidence that the defendant's device incorporated information from highly confidential sources that likely qualify as trade secrets.[80]

Protective order

Finally, another important consideration when confronting trade secret litigation involves the protective order, which sets the rules on who has access to materials exchanged during discovery. Businesses on both sides of a case will often want as few people as possible to have access to sensitive information. But that is not always possible or practical, especially in cases involving complex, highly specialised information.

A recent case involving stock trading strategies illustrates this point. In that case, the plaintiffs wanted to restrict access of sensitive documents to only outside counsel for the defendant company, but the court allowed in-house counsel access to the documents because of the highly technical nature of the case.[81] In doing so, it found it persuasive that the defendant's in-house counsel were not involved with any 'competitive decision making' such that accessing the confidential information risked inadvertent use or disclosure of the sensitive information.[82]

By contrast, however, the court denied the defendant's request to allow a non-attorney 'business professional' access to the plaintiff's documents. Even though the court recognised that the defendant's attorneys may be unable to interpret some technical documents without someone else's technical assistance, it found that the plaintiff's interests outweighed any potential difficulties for the defendant because the defendant could retain an independent expert to help decipher any specialised information.[83]

A major takeaway here is that the court took careful steps to ensure that the defendant had adequate information to defend itself, but did not force the plaintiff to divulge sensitive information to a business person working for a rival, even though it meant that the defendant would need to bear some additional cost. As a practical matter, this case shows why having attorneys familiar with the technology at issue can provide value in communicating with a business's legal decision makers.

Outlook and conclusions

Trade secret law in the United States is dynamic and often complicated, especially when addressing the various remedies available under state and federal law. While courts have blocked a federal ban on non-compete agreements, it remains to be seen whether that block will be permanent and how it will shape any future efforts for similar bans.

In the next few years, it is expected that there will be more US trade secret litigation, especially considering the rapid pace of globalisation with highly interconnected commerce, the willingness of employee talent to switch employers within the same or

similar industries, changes in eligibility of subject matter for patenting (e.g., in the United States), the digital revolution and recent decisions that, for example, allow victims of trade secret misappropriation to recover for damages suffered abroad if the misappropriation has adequate ties to the United States. The ever-changing and legally nuanced area of trade secrets over the past year is a reminder that all businesses should take a fresh look at what trade secrets they have and how they are protecting or will protect them.

Endnotes

1 Defend Trade Secrets Act of 2016 (DTSA). ^ Back to section

2 Trade Secret Litigation Report 2024, Lex Machina, at 8 (Sept 2024). ^ Back to section

3 Id. ^ Back to section

4 *Motorola Solutions, Inc. v. Hytera Commc'ns Corp. Ltd.*, 108 F.4th 458 (7th Cir. July 2, 2024). ^ Back to section

5 *Syntel Sterling Best Shores Mauritius Ltd. v. The TriZetto Group, Inc.*, 68 F.4th 792 (2d Cir. 2023). The Second Circuit encompasses Connecticut, New York and Vermont district courts. As a result, the decision is not binding but may be persuasive authority in other US circuit courts. ^ Back to section

6 Id. at 810–11. ^ Back to section

7 *Syntel Sterling Best Shores Mauritius Ltd. v. TriZetto Group, Inc.*, No. 15 CIV. 211 (LGS), 2024 WL 1116090 (S.D.N.Y. Mar. 13, 2024). ^ Back to section

8 See, e.g., *Salsbury Labs., Inc. v. Merieux Labs, Inc.*, 908 F.2d 706, 714-15 (11th Cir. 1990); *Epic Systems Corp. v. Tata Consultancy Servs., Ltd.*, 980 F.3d 1117, 1123, 1130 (7th Cir. 2020); *PPG Indus., Inc. v. Jiangsu Tie Mao Glass Co., Ltd.*, 47 F.4th 156, 162 (3d Cir. 2022). ^ Back to section

9 *Insulet Corp. v. EOFlow, Co. Ltd. et al.*, 104 F.4th 873, 881 (Fed. Cir. June 17, 2024). ^ Back to section

10 *Zunum Aero Inc. v. The Boeing Company*, 2024 WL 3816139 (W.D. Wash. June 4, 2024). ^ Back to section

11 Alifax Holding SpA v. Alcor Scientific LLC, 2024 WL 2932910, at *5 (Fed. Cir. June 11, 2024). ^ Back to section

12 Id. at *12. ^ Back to section

13 *Pegasystems Inc. v. Appian Corp.*, 904 S.E.2d 247 (Va. App. 2024). ^ Back to section

14 Id. at 261. ^ Back to section

15 Id. at 269–70. ^ Back to section

16 Id. at 274. ^ Back to section

17 Id. at 266–67. ^ Back to section

18 Id. at 267–68. ^ Back to section

19 *Equate Media, Inc. v. Suthar*, No. 22-55681, 2023 WL 7297328, at *1 (9th Cir. Nov. 6, 2023). ^ Back to section

20 Complaint at ¶ 127, *Equate Media, Inc. v. Suthar*, No. 221CV00314RGKAGR, 2022 WL 2824973 (C.D. Cal. June 22, 2022). ^ Back to section

21 Equate Media, Inc. v. Suthar, No. 22-55681, 2023 WL 7297328, at *1 (9th Cir. Nov. 6, 2023). ^ Back to section

22 Ahern Rentals, Inc. v. EquipmentShare.com, 59 F.4th 948 (8th Cir. 2023). ^ Back to section

23 Id. at 955. ^ Back to section

24 *Highland Consulting Grp. v. Soule*, 74 F.4th 1352 (11th Cir. 2023). ^ Back to section

25 *Pauwels v. Deloitte LLP*, 84 F.4th 171 (2d Cir. 2023). ^ Back to section

26 Id. at 177. ^ Back to section

27 Id. at 182–83. ^ Back to section

28 *TWC Concrete, LLC v. DeCarlo*, 2023 WL 4306121, at *5 (S.D. Ohio June 30, 2023). ^ Back to section

29 *Jane St. Grp. v. Millennium Mgmt.*, 2024 WL 3357005 (S.D.N.Y. July 10, 2024). ^ Back to section

30 Id. at *1. ^ Back to section

31 *Jane St. Grp. v. Millennium Mgmt.*, 2024 WL 2833114, at *2 (S.D.N.Y June 3, 2024). ^ Back to section

32 Id. ^ Back to section

33 *Total Quality Logistics, LLC v. Leonard*, 220 N.E.3d 225, 233 (Ohio App. 12th Dist. 2023). ^ Back to section

34 Id. at 232. ^ Back to section

35 Id. ^ Back to section

36 Non-Compete Clause Rule, 88 Fed. Reg. 3482 (proposed Jan. 19, 2023) (to be codified at 16 C.F.R. pts. 910 & 912). ^ Back to section

37 *Ryan, LLC v. Fed. Trade Commc'n*, No. 3:24-CV-00986-E, 2024 WL 3879954 (N.D. Tex. Aug. 20, 2024). ^ Back to section

38 Only two states have not enacted the Uniform Trade Secrets Act (UTSA): New York and North Carolina. See ' Trade Secrets Act', Uniform Law Commission. But even those states afford virtually identical trade secret protection to their UTSA-adopting counterparts and, by extension, the federal DTSA. See *Iacovacci v. Brevet Holdings, LLC*, 437 F. Supp. 3d 367, 380 (S.D.N.Y. 2020) (the elements of a claim for trade secret misappropriation under the DTSA and under New York law are 'fundamentally the same'); Joseph E. Root III & Guy M. Blynn, 'Abandonment of Common-Law Principles: The North Carolina Trade Secrets Protection Act', 18 *Wake Forest L. Rev.* 823, 831–48 (1982) (outlining the similarities and differences between the UTSA and the North Carolina Trade Secrets Protection Act). ^ Back to section

39 18 U.S.C. § 1839(3). ^ Back to section

40 See, e.g., *TB Food U.S. LLC v. Am. Mariculture Inc.*, 2:17- cv-00009-JES-NPM (M.D. Fla. Aug. 1, 2022) (genetic information of shrimp qualified as trade secrets), rev'd on other grounds by, No. 22- 12936 (11th Cir. June 18, 2024). ^ Back to section

41 18 U.S.C. § 1839(3). ^ Back to section

42 See *Insulet Corp. v. EOFlow, Co. Ltd.*, 104 F.4th 873, 881 (Fed. Cir. 2024). ^ Back to section

43 See, e.g., Garvey v. Face of Beauty LLC, 634 F. Supp. 3d 84, 97 (S.D.N.Y. 2022). ^ Back to section

44 Id. ^ Back to section

45 18 U.S.C. § 1839(3)(A). ^ Back to section

46 *Rocket Pharms., Inc. v. Lexeo Therapeutics, Inc.*, No. 23-CV-9000, 2024 WL 3835264, at *5 (S.D.N.Y. Aug. 14, 2024) ^ Back to section

47 Id. ^ Back to section

48 *Novus Group, LLC v. Prudential Fin., Inc.*, 74 F.4th 424, 428-29 (6th Cir. 2023). ^ Back to section

49 Id. ^ Back to section

50 *In re Island Indus., Inc.*, No. 23-5200, 2024 WL 869858, at *3–4 (6th Cir. Feb. 29, 2024) (collecting cases). ^ Back to section

51 Id. at *3–4 (6th Cir. Feb. 29, 2024). ^ Back to section

52 Id. at *4 ('But unlike the cases referred to above, Sigma failed to allege the existence of its need-to-know policy in its complaint.'). ^ Back to section

53 See, e.g., *Motorola Sols., Inc. v. Hytera Commc'ns Corp. Ltd.*, 108 F.4th 458, 469-70 (7th Cir. 2024) ('Proof of the theft and copying included the fact that minor coding errors in Motorola's code appeared in exactly the same spots in Hytera's code.'). ^ Back to section

54 *Novus Group, LLC v. Prudential Fin., Inc.*, 74 F.4th 424 (6th Cir. 2023). ^ Back to section

55 See generally id. ^ Back to section

56 18 U.S.C. § 1836(b)(1). ^ Back to section

57 *Providence Title Co. v. Truly Title, Inc.*, 547 F. Supp. 3d 585, 598 (E.D. Tex. 2021). ^ Back to section

58 See 18 U.S.C. § 1836(b)(2). ^ Back to section

59 Id. § 1836(b)(2)(A)(i). ^ Back to section

60 Mission Capital Advisors LLC v. Romaka, No. 16 CIV. 5878 (LLS), 2016 WL 11517104, at *1 (S.D.N.Y. July 29, 2016). ^ Back to section

61 18 U.S.C. § 1836(b)(2). ^ Back to section

62 Id. § 1836(b)(2)(A)(ii)(VI) and (VIII). ^ Back to section

63 *Syntel Sterling Best Shores Mauritius Ltd. v. The TriZetto Group, Inc.*, 68 F.4th 792 (2d Cir. 2023). ^ Back to section

64 See, e.g., *Salsbury Labs., Inc. v. Merieux Lab'ys, Inc.*, 908 F.2d 706, 714–15 (11th Cir. 1990) (interpreting Georgia law); *Epic Sys. Corp. v. Tata Consultancy Servs., Ltd.*, 980 F.3d 1117, 1123, 1130 (7th Cir. 2020) (Wisconsin law); *PPG Industries, Inc. v. Jiangsu Tie Mao Glass Co., Ltd.*, 47 F.4th 156, 162 (3d Cir. 2022) (Pennsylvania law). ^ Back to section

65 18 U.S.C. § 1836(b)(3)(A)(i)(I). ^ Back to section

66 See UTSA with 1985 Amendments § 2(a). Some form of the UTSA has been enacted in 48 states. ^ Back to section

67 See Michael J. Garrison et al, ' A Proposed Framework for a Federal Inevitable Disclosure Doctrine unde
r the Defend Trade Secrets Act Doctrine under the Defend Trade Secrets Act', 72 *Buff. L. Rev.* 271, 297-324 (2024) (identifying jurisdictions that endorse the inevitable disclosure doctrine). ^ Back to section

68 See generally *PepsiCo v. Redmond*, 54 F.3d 1262 (7th Cir. 1995). ^ Back to section

69 Id. at 1269 (general manager responsible for a business unit with $500 million in annual revenues). ^ Back to section

70 PetroChoice LLC v. Amherdt, No. 22-CV-02347, 2023 WL 2139207, at *5 (N.D. Ill. Feb. 21, 2023) (plaintiffs must show that the defendant "could not operate or function" in their new role without relying on the trade secrets). ^ Back to section

71 See, e.g., id. ^ Back to section

72 See Lex Machina, at 16. Summary judgment is typically sought by defendants to dismiss claims when the undisputed evidence shows that the plaintiff's claim is legally deficient. ^ Back to section

73 Id. ^ Back to section

74 Id. ^ Back to section

75 Id. ^ Back to section

76 *Alifax Holding SpA et al. v. Alcor Scientific LLC et al.*, No. 22-1641, 2024 WL 2932910 (Fed. Cir. June 11, 2024). ^ Back to section

77 *Insulet Corp. v. EOFlow, Co. Ltd.*, 104 F.4th 873 (Fed. Cir. 2024). ^ Back to section

78 Id. at 877–78. ^ Back to section

79 Id. 881–83. ^ Back to section

80 Id. at 881 (describing the reasonable measures used to protect a set of information). ^ Back to section

81 *Jane St. Grp. v. Millennium Mgmt.*, 2024 WL 2833114, at *2 (S.D.N.Y. June 3, 2024). ^ Back to section

82 Id. ^ Back to section

83 Id. at *3. ^ Back to section

Rocco Screnci rscrenci@mcandrews-ip.com
Wil Rao wrao@mcandrews-ip.com

McAndrews, Held & Malloy Ltd