Table of Contents

2

Trade Secret

To understand why the law protects trade secrets,[1] it helps to understand why people keep trade secrets. Consider the the story of Greek fire, a semi-legendary superweapon of the middle ages. Apparently invented sometime in the 7th century, it was a kind of pre-modern napalm. Ancient and medieval chroniclers describe it as a burning liquid with the remarkable property that it couldn't be extinguished with water, making it a truly fearsome weapon against wooden ships. In the words of one 13th-century account:

> This was the fashion of the Greek fire: it came on as broad in front as a vinegar cask, and the tail of fire that trailed behind it was as big as a great spear; and it made such a noise as it came, that it sounded like the thunder of heaven. It looked like a dragon flying through the air.

In the 8th century the Byzantines used it to drive off Arab invasions, and they were still using it six centuries later. They recognized that the military edge that it provided was useless if their enemies acquired the secret of making it. Thus, they kept the details closely guarded. Only a few people knew the secret process to prepare it; soldiers who used it in battle didn't know how it was made. The Byzantines guarded it so closely, in fact, that knowledge of how to make it fire disappeared with the Byzantine Empire. The story goes that when the Fourth Crusade sacked Constantinople in 1204, the secret vanished in the chaos. The Empire never recovered, politically or militarily. We still don't know today how Greek fire was made.[2]

1. The leading trade secret treatises are Roger M. Milgrim & Eric Bensen, Milgrim on Trade Secrets (2021); Louis Altman & Malla Pollack, Callmann on Unfair Competition, Trademarks, and Monopolies (2021); Melvin F. Jager, Trade Secrets Law (2021).
2. It still happens. A material code-named FOGBANK was used in W76 nuclear weapons. FOGBANK's composition was classified. So was its use. And so was the

Greek fire, as depicted in the Madrid Skylitzes, a 12th-century illuminated manuscript

This story illustrates three central lessons about secrets:

- Information gives a competitive advantage.
- That advantage can depend on secrecy.
- But secrecy is costly.

These facts are enough to justify the *practice* of trade secrecy; businesses keep secrets because there are things they don't want competitors to know. But they are not enough by themselves to justify trade secret *law*. At least four justifications rub elbows in the cases and commentary. Two are familiar from the previous chapter, and two are new:

- **Contracting**: Legal protection for trade secrets, like NDAs and patents, is a mechanism to resolve Arrow's Information Paradox. Trade secret law helps make it possible to negotiate for the disclosure of secret information.
- **Innovation**: Keeping secrets safe gives companies incentives to invest in creating valuable information in the first place.
- **Arms Race**: Unless trade secrets received legal protection, companies would inefficiently overinvest in self-help to protect them, and other companies would inefficiently overinvest in stealing them.
- **Competition**: Trade secret law deters unethical business practices and encourages companies to compete with each other fairly.

Doctrinally, trade secret law has deep common-law roots as a branch of "unfair competition" law. The older Restatement (First) of Torts reflects this common-law heritage. Over time, it has become more statutory and

process for making it. In 2000, a program to extend the service life of the existing stock of W76 warheads ran into trouble when it was discovered that the government no longer knew how to make FOGBANK. Most of the records of the manufacturing process had been discarded or destroyed, and most of the people who worked on it had retired.

more federal. The Uniform Trade Secrets Act (UTSA) has been adopted in some form by 47 states, and the modern Restatement (Third) of Unfair Competition generally parallels the UTSA. The federal Economic Espionage Act of 1996 (EEA) criminalized an important subset of trade secret misappropriation,[3] and the 2016 Defend Trade Secrets Act (DTSA) added a federal civil cause of action and an important seizure remedy.[4]

A Subject Matter

Not every secret is a *trade* secret. When one fifth-grader asks another to cross her heart and hope to die before revealing a bit of gossip about a mutual friend, this is not the kind of secret the courts will take an interest in. Trade secret law has traditionally policed this line using an ***economic value*** requirement. In the words of the Restatement (Third): "A trade secret is any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable ... to afford an actual or potential economic advantage over others."[5]

1 Economic *Value*

There are actually two subtly different things going on in here. One of them is quantitative. The information must be "sufficiently valuable," which suggests that there is some threshold of value: information can be worth more or less, and only information worth more than 400 quatloos (or some other arbitrary value) can qualify as a trade secret. This is a ***threshold test***: information needs to clear a minimum level of something (value, creativity, fame, etc.) to be protectable.

The economic-value threshold could in theory serve a significant screening function, keeping the courts out of chump-change disputes. In practice, however, the threshold of value is so low it rarely matters. Quoth the Restatement (Third), "It is sufficient if the secret provides an advantage that is more than trivial."[6] When a plaintiff believes that a secret has sufficient value to be worth suing over, the courts almost never second-guess that belief.

2 *Economic* Value

The other way to look at this test is qualitative. Only information with an "economic" value that "can be used in the operation of a business" counts, which suggests that information with only non-economic value does not. This is a ***categorical test***: certain kinds of information are protectable, and certain other kinds are not.

3. Economic Espionage Act (1996) [hereinafter EEA].
4. Defend Trade Secrets Act (DTSA), 18 U.S.C..
5. Restatement (Third) of Unfair Competition § 39 (1995).
6. *Id.* § 39 cmt. e.

The Flag Building in Clearwater, Florida, which serves as Scientology's "spiritual headquarters"

Dennis Erlich holding a press conference

There was a time when the courts took an even narrower view: trade secrets were secret formulas, manufacturing plans, and other information about how to do something physically better. Customer lists, prospective marketing plans, and other information about the business side of the business weren't proper trade secret subject matter. That time has long since passed, and the Restatement (Third) takes a very broad view: trade secrets can relate either to "technical matters" or to "business operations."[7] The UTSA refers broadly to "information, including a formula, pattern, compilation, program, device, method, technique, or process."[8]

But there still is an outer limit here: information with no nexus to business is not a *trade* secret. The cases here are not many, but they are illuminating. Consider *Religious Technology Center v. Netcom On-Line Communications Services, Inc.* ("*RTC*"), in which the Church of Scientology sued Dennis Erlich, a dissident former minister who had posted various of its internal documents on the Internet.[9] The documents described in detail the highest and most secret doctrines of the Church and its belief system, and had typically been shared only with high-ranking Church officials and the innermost circle of initiates. The Church "considers it sacrilegious for the uninitiated to read its confidential scriptures," and Scientologists believe that exposure to this material can be dangerous, even fatal, for those who are unprepared.

The *spiritual* value of the Church's secrets is not quite the same as the *economic* value demanded by trade-secret law. But the court found a way. Religious and non-profit corporations, like their for-profit cousins, can do business, even if the accumulation of profits is not their ultimate aim. Just as they can own and use real estate for churches and offices, they can own and use information. Is this a *competitive* advantage? It is true that organized religions claim to answer to a different standard

7. *Id.*
8. Uniform Trade Secrets Act § 1.4 (1985) [hereinafter UTSA].
9. Religious Tech. Ctr. v. Netcom On-Line Commc'ns Servs., Inc. ("*RTC*"), 923 F. Supp. 1231 (N.D. Cal. 1995).

than marketplace success.[10] But they do compete with each other for worshippers, and for donations. Like a public-radio station offering a tote bag as an incentive to become a member, Scientology offers initiation into life-changing secret knowledge. That was enough of a competitive value for the court in *RTC*.

B Ownership

It is clear, uncontroversial, and unsurprising that the essential requirement for owning a trade secret is ***actual secrecy***: the information must not be widely known.

> "Trade secret" means information . . . that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use . . .[11]

This concept does triple duty. It defines when information is a trade secret at all, it makes priority a non-issue between multiple competitors with the same secret, and it allocates ownership within collaborations.

1 Actual Secrecy

All information is secret in the sense that some people know it and other people don't. And all information is public in the sense that everyone could discover it on their own, given enough time and effort. So the test that information is secret when it is "not . . . generally known to, and not . . . readily ascertainable by proper means by, other persons" asks *how many* people know the purported secret, and *how hard* it would be for the others to discover it.

Consider *Amoco Production Co. v. Laird*. John Clendenning, a geologist at Amoco, recommended that it commission a aerial microwave radar survey of a 13,000-square-mile area in Michigan, Ohio, and Indiana at a cost of $150,000.[12] The surveys indicated the likely presence of oil at two sites, but the estimated yield was beneath Amoco's threshold for commercial viability. A frustrated Clendenning sent a fax of a road map with the sites circled to his former neighbor William Laird, who was an oil entrepreneur. Amoco later decided to go ahead with the project, only to discover that Laird had already leased the sites. Litigation ensued.

10. Compare Acts 8:20 ("But Peter said unto him, Thy money perish with thee, because thou hast thought that the gift of God may be purchased with money.") with Abrams v. United States, 250 U.S. 616, 630 (Holmes, J.) ("[T]he best test of truth is the power of the thought to get itself accepted in the competition of the market.")
11. UTSA, *supra* note 8, § 1(4).
12. Amoco Prod. Co. v. Laird, 622 N.E.2d 912, 914 (Ind. 1993).

One of Laird's arguments was that the locations of the sites was not protectable as a trade secret because it was "readily ascertainable" by others. After all, anyone could look at (publicly available) U.S. Geological Survey data and commission their own (commonly used) aerial microwave radar survey and learn exactly what Amoco did.

But this argument is wrong, and the court rejected it. Anyone could have paid $150,000 to carry out a survey, but only Amoco did. Laird was free to commission his own survey, but he was not free to free-ride on Amoco's. The result would have been different if if Amoco had published the results of the survey in a scientific journal, or if a microwave survey cost $15 instead of $150,000. These differences would have made the location of the oil reserves "readily ascertainable."

Note also that to be secret, information must not be known to or ascertainable by *competitors*: "other persons who can obtain economic value from its disclosure or use." The general public is not able to read microwave radar survey data and know what it means, and most of us are not in a position to sink oil wells, either. But we are not the relevant audience. Amoco's competitors are other oil companies and independents like Laird, the survey gave Amoco a leg up on them, and they are the ones who would have to spend $150,000 on a survey and who know what to do with the results.

In addition to being a subject-matter case, *RTC* offers another look at when information is actually secret. Erlich argued, unsuccessfully, that the documents had already been made public, and so were no longer secret. For one thing, they had been filed as a declaration in another Scientology-dissident case, *Church of Scientology Int'l v. Fishman*,[13] and court filings are generally matters of public record. But while the *RTC* court agreed that full public accessibility would destroy trade secrecy, it noted that the *Fishman* court had promptly sealed the filing. If the filings had been widely copied during the period before they were sealed, then that would end their secrecy; but the fact that they *could have been* copied would not by itself put an end to their trade-secret status. This pragmatic approach is typical of trade-secret law.

2 Priority

Actual secrecy also resolves priority questions by allowing multiple independent parties each to have a trade secret in the same information. There is no requirement that a trade secret be unique; more than one person can have the same information and each has a valid and independent trade secret provided the other requirements are met. Thus, trade secret does not generally raise difficult issues about which of several competing claimants developed the information first. Regardless of the order, both

13. Church of Scientology Int'l v. Fishman, No. 91-6426 (C.D. Cal. 1994).

Syndrome explains trade secrets

parties have protectable trade secrets in the information. If Laird had commissioned his own microwave survey, he would have had his own independent trade secret in the locations of the oil fields, and Amoco would have had a trade secret too. This logic breaks down only when the information is so "generally known" that it fails to qualify as a trade secret at all.

3 Collaborations

Actual secrecy also helps resolve questions of allocating ownership within collaborations. Two or more people working together can jointly own a trade secret.[14] Companies are a particularly common way to organize information ownership. The general default rule of agency and employment law is that the employer owns any valuable information created by employees in the scope of their employment, even if it results from the "application of the employee's personal knowledge or skill."[15] This default can be broadened or narrowed by contract. Thus, for example, an employer and employee can agree that the employee will own some or all of the information they create on the job.

Some employees use their employer's facilities to develop their own ideas, e.g., coming in after hours to use workshop tools, or running compute-intensive machine-learning models on the employer's computers. If these inventions relate to the employer's business, then the employer receives a ***shop right***. The employee owns the information, but the employer has an irreovocable, nonexclusive, royalty-free license to use it.

On the other hand, some employers attempt to claim ownership by contract of information created by employees during or even after their term of employment, regardless of whether it was part of their job duties.

14. "Three may keep a secret, if two of them are dead." Benjamin Franklin, *Poor Richard's Almanack*, July 1735.
15. Restatement (Third) of Unfair Competition, *supra* note 5, § 42 cmt. e.

These provisions are enforceable in theory but can be litigation quagmires in practice. The Restatement (Third) explains:

> In some situations, however, it may be difficult to prove when a particular invention was conceived. The employee may have an incentive to delay disclosure of the invention until after the employment is terminated in order to avoid the contractual or common law claims of the employer. It may also be difficult to establish whether a post-employment invention was improperly derived from the trade secrets of the former employer. Some employment agreements respond to this uncertainty through provisions granting the former employer ownership of inventions and discoveries relating to the subject matter of the former employment that are developed by the employee even after the termination of the employment. Such agreements can restrict the former employee's ability to exploit the skills and training desired by other employers and may thus restrain competition and limit employee mobility. The courts have therefore subjected such "holdover" agreements to scrutiny analogous to that applied to covenants not to compete. Thus, the agreement may be unenforceable if it extends beyond a reasonable period of time or to inventions or discoveries resulting solely from the general skill and experience of the former employee.[16]

C Procedures

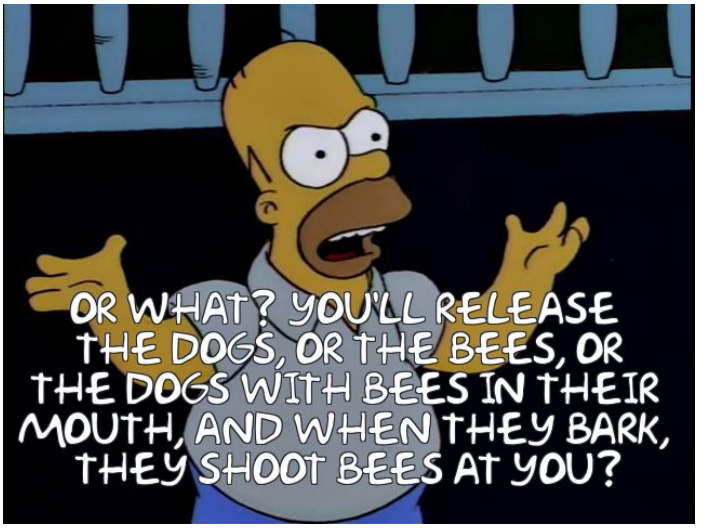
There is no requirement that the owner of a trade secret register it as one with a government agency, or take other formal steps. Instead, the only procedural prerequisite to having a valid trade secret is making ***reasonable efforts*** to preserve its secrecy.

1 Reasonable Efforts

The UTSA provides that to be a trade secret, information must be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[17] Such efforts can involve a mixture of physical security like locks and guards, digital security like password policies and firewalls, confidentiality agreements, and compartmentalization of knowledge. Here is a summary of one company's precautions:

> RAPCO stores all of its drawings and manufacturing data in its CAD room, which is protected by a special lock, an alarm system, and a motion detector. The number of copies of sensitive information is kept to a minimum; surplus copies are shredded. Some information in the plans is coded, and few people know the keys to these codes.

16. *Id.* § 42 cmt. g.
17. UTSA, *supra* note 8, § 1(4)(i)(i).



Reasonable efforts? (*The Simpsons* S5E18, "Burns' Heir")

> Drawings and other manufacturing information contain warnings of RAPCO's intellectual property rights; every employee receives a notice that the information with which he works is confidential. None of RAPCO's subcontractors receives full copies of the schematics; by dividing the work among vendors, RAPCO ensures that none can replicate the product.[18]

It is always possible to imagine even stronger efforts. (Indeed, the reasonableness of the owner's efforts will only be at issue in cases where they have failed.) But the test is "reasonable" efforts, not perfect security:

> This makes it irrelevant that RAPCO does not require vendors to sign confidentiality agreements; it relies on deeds (the splitting of tasks) rather than promises to maintain confidentiality. Although, as Lange says, engineers and drafters knew where to get the key to the CAD room door, keeping these employees out can't be an ingredient of "reasonable measures to keep the information secret"; then no one could do any work. So too with plans sent to subcontractors, which is why dissemination to suppliers does not undermine a claim of trade secret.[19]

Security is costly. Fences and firewalls cost money. They also make it harder for people to do their jobs, by keeping useful information under wraps. What is reasonable under the circumstances reflects a tradeoff between the costs and benefits of increased security.

But this leaves a puzzle. Why require reasonable efforts at all, given

18. United States v. Lange, 312 F.3d 263, 266 (7th Cir. 2002).
19. *Id.*

that they are costly? Why isn't the test simply efforts sufficient to maintain actual secrecy? Here are some possible theories:

1. Reasonable efforts are evidence of economic value. Businesses will not bother to make an effort to keep their weekly break-room donut orders secret, because this information is of no meaningful use to competitors.
2. Reasonable efforts are evidence of actual secrecy. The fact that papers are kept under lock and key helps show that they are not widely available.
3. Reasonable efforts are evidence of misappropriation. (This one takes a little more thought to see.) If documents are not normally shared with subcontractors, it is less likely that a rival obtained them innocently from a subcontractor on a job site.
4. Reasonable efforts provide fair notice to potential defendants. If papers are stamped "CONFIDENTIAL," employees who handle them know they are dealing with information the company considers proprietary.
5. The reasonable-efforts requirement makes owners take reasonable efforts. Otherwise, they will be tempted to rely on expensive lawsuits when cheap five-dollar padlocks could have prevented the problem in the first place. Trade-secret law helps those who help themselves.[20]

Which of these strike you as persuasive?

2 Term

Trade secrets have no term limits; they can endure indefinitely. As long as the requirements to have a trade secret in the first place continue—economic value, actual secrecy, and reasonable efforts—so do the owner's trade-secret rights. As a result, trade secrets tend to end when they become either less-widely or more-widely known.

On the one hand, some trade secrets disappear without a trace because the information in them is no longer useful to the owner and so it no longer bothers to invest in keeping track of that information. (In the extreme case, when a business fails, it no longer bothers to invest in keeping track of anything.) As papers are shredded or old files deleted, they are forgotten entirely.

Other trade secrets disappear because they stop being secret. As technologies are reinvented, or leaked, or voluntarily disclosed, what used to be closely held becomes widely known. Ideas diffuse through

20. This list is adapted from Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174 (7th Cir. 1991) (Posner, J.).

an industry, and no one in the industry has a protectable trade secret in them.

D Infringement: Prohibited Conduct

The essence of trade secret misappropriation is to ***acquire*** a protected secret through ***improper means***, or to ***use*** or ***disclose*** a secret that was acquired through improper means or by "accident or mistake".[21]

1 Improper Means

The UTSA defines improper means to be "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means."[22] The Restatement (Third) uses a similar list, but adds the catchall "other means either wrongful in themselves or wrongful under the circumstances of the case."[23] These definitions can be roughly divided into two types of wrongful conduct. On the one hand there is ***espionage***, which often involves theft, trespass, or computer hacking. On the other hand there is ***breach of confidence***, which often involves violating a promise to keep someone else's secrets. It is tempting to to conclude that "improper means" consist of torts (espionage) and breach of contract (breach of confidence), but this equation is a little too pat.

a Espionage

E.I. du Pont de Nemours & Co. v. Christopher
431 F.2d 1012 (5th Cir. 1970)

This is a case of industrial espionage in which an airplane is the cloak and a camera the dagger. The defendants-appellants, Rolfe and Gary Christopher, are photographers in Beaumont, Texas. The Christophers were hired by an unknown third party to take aerial photographs of new construction at the Beaumont plant of E. I. DuPont de Nemours & Company, Inc. Sixteen photographs of the DuPont facility were taken from the air on March 19, 1969, and these photographs were later developed and delivered to the third party.[24]

21. UTSA, *supra* note 8, § 1; Restatement (Third) of Unfair Competition, *supra* note 5, § 40.
22. UTSA, *supra* note 8, § 1(1).
23. Restatement (Third) of Unfair Competition, *supra* note 5, § 43.
24. [Ed: "The appearance of the airplane at such an opportune moment [may have] suggested to DuPont that some kind of inside leak had tipped off the photographers (or their client) to the opportunity." Edmund Kitch, *The Law and Economics of Rights in Valuable Information*, 9 J. Legal Stud. 683 (1980).]

Modern view of the Beaumont methanol plant (now owned by OCI)

DuPont subsequently filed suit against the Christophers, alleging that the Christophers had wrongfully obtained photographs revealing DuPont's trade secrets which they then sold to the undisclosed third party. DuPont contended that it had developed a highly secret but unpatented process for producing methanol, a process which gave DuPont a competitive advantage over other producers. This process, DuPont alleged, was a trade secret developed after much expensive and time-consuming research, and a secret which the company had taken special precautions to safeguard. The area photographed by the Christophers was the plant designed to produce methanol by this secret process, and because the plant was still under construction parts of the process were exposed to view from directly above the construction area. Photographs of that area, DuPont alleged, would enable a skilled person to deduce the secret process for making methanol. DuPont thus contended that the Christophers had wrongfully appropriated DuPont trade secrets by taking the photographs and delivering them to the undisclosed third party.

The Christophers argued both at trial and before this court that they committed no "actionable wrong" in photographing the DuPont facility and passing these photographs on to their client because they conducted all of their activities in public airspace, violated no government aviation standard, did not breach any confidential relation, and did not engage in any fraudulent or illegal conduct. In short, the Christophers argue that for an appropriation of trade secrets to be wrongful there must be a trespass, other illegal conduct, or breach of a confidential relationship. We disagree.

One may use his competitor's secret process if he discovers the process by reverse engineering applied to the finished product; one may use a competitor's

process if he discovers it by his own independent research; but one may not avoid these labors by taking the process from the discoverer without his permission at a time when he is taking reasonable precautions to maintain its secrecy. To obtain knowledge of a process without spending the time and money to discover it independently is improper unless the holder voluntarily discloses it or fails to take reasonable precautions to ensure its secrecy.

In the instant case the Christophers deliberately flew over the DuPont plant to get pictures of a process which DuPont had attempted to keep secret. The Christophers delivered their pictures to a third party who was certainly aware of the means by which they had been acquired and who may be planning to use the information contained therein to manufacture methanol by the DuPont process. The third party has a right to use this process only if he obtains this knowledge through his own research efforts, but thus far all information indicates that the third party has gained this knowledge solely by taking it from DuPont at a time when DuPont was making reasonable efforts to preserve its secrecy. In such a situation DuPont has a valid cause of action to prohibit the Christophers from improperly discovering its trade secret and to prohibit the undisclosed third party from using the improperly obtained information.

In taking this position we realize that industrial espionage of the sort here perpetrated has become a popular sport in some segments of our industrial community. However, our devotion to free wheeling industrial competition must not force us into accepting the law of the jungle as the standard of morality expected in our commercial relations. Our tolerance of the espionage game must cease when the protections required to prevent another's spying cost so much that the spirit of inventiveness is dampened. Commercial privacy must be protected from espionage which could not have been reasonably anticipated or prevented. We do not mean to imply, however, that everything not in plain view is within the protected vale, nor that all information obtained through every extra optical extension is forbidden. Indeed, for our industrial competition to remain healthy there must be breathing room for observing a competing industrialist. A competitor can and must shop his competition for pricing and examine his products for quality, components, and methods of manufacture. Perhaps ordinary fences and roofs must be built to shut out incursive eyes, but we need not require the discoverer of a trade secret to guard against the unanticipated, the undetectable, or the unpreventable methods of espionage now available.

In the instant case DuPont was in the midst of constructing a plant. Although after construction the finished plant would have protected much of the process from view, during the period of construction the trade secret was exposed to view from the air. To require DuPont to put a roof over the unfinished plant to guard its secret would impose an enormous expense to prevent nothing more than a school boy's trick. We introduce here no new or radical ethic since our ethos has never given moral sanction to piracy. The marketplace must not deviate far from our mores. We should not require a person or corporation to take unreasonable precautions to prevent another from doing that which he

ought not do in the first place. Reasonable precautions against predatory eyes we may require, but an impenetrable fortress is an unreasonable requirement, and we are not disposed to burden industrial inventors with such a duty in order to protect the fruits of their efforts. "Improper" will always be a word of many nuances, determined by time, place, and circumstances. We therefore need not proclaim a catalogue of commercial improprieties. Clearly, however, one of its commandments does say "thou shall not appropriate a trade secret through deviousness under circumstances in which countervailing defenses are not reasonably available."

Having concluded that aerial photography, from whatever altitude, is an improper method of discovering the trade secrets exposed during construction of the DuPont plant, we need not worry about whether the flight pattern chosen by the Christophers violated any federal aviation regulations. Regardless of whether the flight was legal or illegal in that sense, the espionage was an improper means of discovering DuPont's trade secret.

Questions

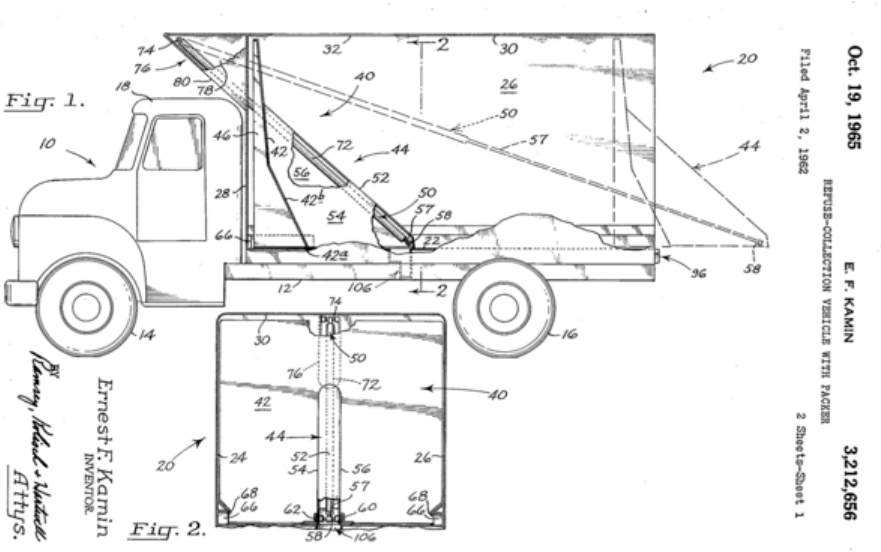
1. Look back at the four theories to justify trade secrets law at the start of the chapter. Which of them are most consistent with the court's reasoning in *Christopher*?
2. It is the present day and your client is a major petrochemical company. It wants to learn as much as possible about a competitor's methanol plant, which is about to start construction. The client has proposed (a) flying a plane over the construction site, as in *Christopher*; (b) flying a five-pound drone 300 feet in the air above a public road adjacent to the site; and (c) buying commercially available satellite photos of the site. What is your advice?

Cases of accident or mistake are usefully thought of as espionage-adjacent. Stealing deal documents from an airplane seatmate's briefcase is acquisition through improper means, but reading through documents they left behind when they deplaned is acquisition through mistake.

b Breach of Confidence

Turn now to the other prong of improper means, breach of confidence. *Kamin v. Kuhnau* is reasonably representative.[25] After a career as a knitting-mill mechanic, Ernest Kamin got into the garbage collection business in 1953. It was a fertile time for garbage-truck innovations, and Kamin soon had ideas about how to use hydraulic cylinders to lift garbage containers to the truck and compress garbage once inside. In

25. Kamin v. Kuhnau, 374 P.2d 912 (Or. 1962).



One of Kamin's garbage-truck designs

1955, he struck a deal with Richard Kuhnau to use Kuhnau's machine shop to experiment with truck designs and build prototypes.

The experiment was a success. By the summer of 1956, Kamin was taking orders for garbage trucks made to his improved design. Kuhnau set up another company to manufacture the trucks for Kamin. But after the first ten trucks, Kuhnau broke off the relationship in October 1956 and started making trucks on his own with a very similar design. Kamin sued, arguing that Kuhnau had misappropriated Kamin's trade secrets.

If Kamin and Kuhnau had explicitly contracted for nondisclosure, this would be an easy case. Indeed, there would be no need to invoke trade secret law; as in *Apfel*, contract law would suffice. But, like so many other business partners, they neglected the IP terms in their contracts. If Kuhnau had been Kamin's employee, this would also be an easy case. Employment law imposes a duty of loyalty on employees, and they breach that duty by using the employer's trade secrets for their own benefit.[26] But at no point did Kamin have the kind of direct control over the "manner and means" of Kuhnau's work that characterizes an employment relationship.[27] "Tenant" and "customer" are better descriptions of his role than "employer"; Kamin rented space from Kuhnau, and then purchased completed trucks from him.

But trade-secret law is willing to imply duties of confidentiality, not just as a matter of fact, but as a matter of law. To quote *Kamin*:

26. Restatement of Emp. L. § 8.01 (2015).
27. Restatement of Emp. L. § 1.01.

> It is not necessary to show that the defendant expressly agreed not to use the plaintiff's information; the agreement may be implied. And the implication may be made not simply as a product of the quest for the intention of the parties but as a legal conclusion recognizing the need for ethical practices in the commercial world. In the case at bar the relationship between plaintiff and Kuhnau was such that an obligation not to appropriate the plaintiff's improvements could be implied. Kuhnau was paid to assist plaintiff in the development of the latter's idea. It must have been apparent to Kuhnau that plaintiff was attempting to produce a unit which could be marketed. Certainly it would not have been contemplated that as soon as the packer unit was perfected Kuhnau would have the benefit of plaintiff's ideas and the perfection of the unit through painstaking and expensive experimentation. It is to be remembered that the plaintiff's experimentation was being carried on, not on the assumption that he was duplicating an existing machine, but upon the assumption that he was creating a new product.[28]

Another common setting in which breach of confidence is important is failed negotiations. The plaintiff has an idea, and would like the defendant's help in commercializing it, and the situation unspools just as in the idea-submission cases (e.g., *Desny* or *Apfel*) except that when the plaintiff sues on a trade-secret theory, the courts will often find misappropriation even when there is no explicit NDA. If it is clear to both parties that the disclosure is being made for the purpose of negotiation, trade-secret law will treat the negotiations as a confidential relationship and protect against unauthorized disclosure or use. Just as the espionage prong of improper means builds on tort law but does not feel compelled to track it exactly, so too does the breach-of-confidence prong build on contract law, but without getting tangled up in the niceties of contract doctrine.

2 Acquisition, Use, and Disclosure

The three verbs "acquire," "use," and "disclose" cover the lifecycle of information: you acquire it, you use it for your own purposes, and then you disclose it to others.

Acquisition itself is to obtain the information. What makes trade secret misappropriation distinctively wrongful is the improper means or unfair circumstances under which this acquisition takes place (as discussed above). If you acquire information properly, you are free to use and disclose it as you wish. Under the Restatement of Torts, only use and disclosure were actionable, and only folllowing a wrongful acquisition. The modern approach is simpler and cleaner. Although acquisition is often harmless by itself, it creates a high enough likelihood of subsequent harm

28. *Kamin*, 374 P.2d at 152—53.

through use or disclosure that it is made actionable. There is no good reason that Du Pont should have to wait for the Christophers to give their photographs to their client before it can sue them.

To *use* a trade secret is to exploit the information for commercial gain. This requires something more than bare possession, and something less than full commercialization. For example, merely possessing misappropriated construction diagrams for a widget smelter is not use, but following them to build a smelter is, even if the smelter is never operated to make widgets. There is a ***commerciality*** threshold here: purely personal uses are probably not actionable on their own. Most cases hold that to possess or use a product *made using* a secret is not to "use" the secret itself. As one court memorably put it:

> One who bakes a pie from a recipe certainly engages in the "use" of the latter; but one who eats the pie does not, by virtue of that act alone, make "use" of the recipe in any ordinary sense, and this is true even if the baker is accused of stealing the recipe from a competitor, and the diner knows of that accusation. . . . A coach who employs [a stopwatch] to time a race certainly makes "use" of it, but only a sophist could bring himself to say that coach "uses" trade secrets involved in the manufacture of the watch.[29]

To *disclose* a trade secret is to reveal the information to others. Disclosure can be private (the Christophers giving their photographs to their client) or public (Erlich posting the Scientology documents on the Internet). There is not a commerciality threshold for disclosure, as there was for use. Erlich had no profit motive for spilling Scientology's secrets, but the fact that he acted for principled rather than pecuniary reasons was no defense. Note that there are two kinds of harms here. One is that someone else might make unauthorized use of the information (e.g., the Christophers' client). The other is that the information might become no longer secret at all (e.g., the Scientology documents). Both are protected against, and both are part of the secret owner's measure of damages.

3 Intent

Generally speaking, liability for trade secret misappropriation requires that the defendant ***know or have reason to know*** that the information is a trade secret. Did the Christophers, strictly speaking, know that the layout of the methanol plant embodied trade secrets? Perhaps, perhaps not, but they certainly had reason to know, and that was enough.

There is a subtle timing issue here, because sometimes the knowledge that information is a trade secret arrives *after* the information itself. Think of a parts supplier who receives an email with their client's com-

29. Silvaco Data Sys. v. Intel Corp., 184 Cal. App. 4th 210, 224 (2010).

plete purchase-order database for the last quarter. If the recipient knows or has reason to know of the mistake, then the usual obligations attach. The supplier cannot undercut its competitors' prices or short their stock on the basis of what it learns. But other mistakes are harder for the recipient to spot.

Out of fairness, the UTSA says that if a recipient makes a "material change of position" before learning of the mistake, they are free of their trade-secret obligations.[30] Parties who have made substantial expenditures in the reasonable belief that the plans underlying their investment are not someone else's trade secret will not have the rug yanked out from under them retroactively. The Restatement (Third) accommodates a similar concern by saying that the recipient takes the information free and clear if "the acquisition was the result of the other's failure to take reasonable precautions to maintain the secrecy of the information,"[31] which sounds in reasonable efforts, rather than intent.

E Infringement: Similarity

The prohibition on misappropriation through improper means includes an implicit requirement that the information the defendant obtained or used is the *same* information the plaintiff claims as a trade secret. There will be cases in which the defendant discloses or uses information, but it is not derived from the plaintiff's secrets.

1 Substantial Similarity

Although the issue is rarely framed this way in trade-secret law, the test for similarity is the same as in copyright: ***substantial similarity*** between the plaintiff's and defendant's information.[32] Here is a typical holding from a case dismissing a trade-secret claim on the basis of no substantial similarity, *Big Vision Private, Ltd. v. E.I. Dupont De Nemours & Co.*:

> Quite simply, Big Vision cannot demonstrate that its recyclable banners are substantially similar to DuPont's. The parties do not dispute that DuPont's recyclable banner products are not made by either lamination or coextrusion. None of DuPont's recyclable banner products use the three-layer structures tested at the Trials, the range of $CaCO_3$ tested at the Trials, or "minimal" amounts of Entira (to the extent it has been defined), since DuPont's products either use 100% or 0% Entira. Furthermore, DuPont's recyclable banner products are not printable with solvent ink. Thus, to the extent Big Vision's trade

30. UTSA, *supra* note 8, § 1(2)(C).
31. Restatement (Third) of Unfair Competition, *supra* note 5, § 40(b)(4).
32. *See generally* Joseph P. Fishman & Deepa Varadarajan, *Similar Secrets*, 167 U. Pa. L. Rev. 1051 (2019).

> secret is discernible, DuPont's products implicate almost none of its elements.[33]

2 Proof of Copying

A recurring issue in IP areas that prohibit copying – as trade secret and copyright do – is proving that the defendant copied its information *from the plaintiff*. It is not trade secret infringement to independently come up with the same idea; indeed, it happens all the time. Unbeknownst to Kamin and Kuhnau, there were already hydraulic-press garbage trucks on the market in other parts of the country. This did not negate Kamin's trade secret. But if Kuhnau had seen one of those other trucks while on a business trip to Boston, it would not have been misappropriation for him to duplicate that truck – even if the design had coincidentally been close to Kamin's. Kuhnau infringed because he copied his design *from Kamin's* in breach of the duty of confidence he owed to Kamin.

Whether the defendant copied from the plaintiff is a factual question: either they did or they didn't. As such, proving copying is fundamentally an evidentiary question. Two kinds of evidence are particularly probative: proof that the defendant had ***access*** to the plaintiff's information, and proof that the defendant's information is ***similar*** to the plaintiff's. Access is relevant because it helps to make the theft story more plausible, and hence more likely. Similarity is relevant because it helps make the innocent alternative stories less plausible, and hence less likely.

For an example, consider *Grynberg v. BP, PLC*.[34] The plaintiff pitched ARCO on a variety of oil-development projects in Central Asia based on his research. Later, ARCO invested in two pipelines he proposed. He sued, alleging that ARCO had relied on his confidential research in pursuing these projects.

Grynberg had ready evidence of access; he had met with ARCO to discuss these two pipeline routes. But ARCO's counter-story of no copying was also strong. It had well-documented proof that it had planned its investments using a mixture of publicly available resources and "data rooms" in which it compiled (and carefully logged) more detailed research. Grynberg tried to undercut this counter-story by showing that there were such detailed similarities between his proposal and ARCO's pipeline projects that they could only have been copied from him. But the court was unpersuaded:

> ARCO did eventually make investments in Tengiz and the Caspian pipeline, which were among the investments that Grynberg had endorsed and relayed information about. However ARCO also declined

33. Big Vision Priv., Ltd. v. E.I. Dupont De Nemours & Co., 1 F. Supp. 3d 224, 274 (S.D.N.Y.).
34. Grynberg v. BP, PLC, No. 06 Civ. 6494 (RJH) (S.D.N.Y Mar. 30, 2011).

> to pursue other investments Grynberg had advocated, such as the Karachaganak oil field also in the area of mutual interest. Moreover nothing about ARCO's investments bears the markers of the Grynberg information in such a way as to justify inferring the use of that information. It is not as if ARCO built wells at particular locations previously suggested by Grynberg, worked primarily through contacts developed by Grynberg, or tied its investments to Grynberg's numbers in a suspiciously similar way. Rather, an oil company chose to invest in one of the largest oil fields in the world, in a manner different from that envisioned by Grynberg at the time he developed his proposed consortium. That it did so is unsurprising and does not evince the kind of suspicious similarity present in [previous cases].[35]

This is the opposite of *Big Vision*. There, there were insufficient similarities between the plaintiff's products and the defendant's secrets, even though there may have been copying. Here, there were sufficient similarities, but they were the result of coincidence, not copying.

One last note. The kind of similarity needed to prove copying from the plaintiff is different from the kind of similarity needed to establish substantial similarity for misappropriation purposes. The former is evidentiary, the latter is substantive. Similarity to prove copying can be based on unprotected or trivial elements. A drafting error in the plaintiff's schematic diagrams that shows up in the defendant's product may be commercially insignificant but impossible for the defendant to explain away innocently. The drafting error proves copying, but other similarities will be needed to show substantial similarity.

F Secondary Liability

If a vice-president at MatrixCorp receives an email from someone calling themself Cypher offering to provide details of a computer graphics technology similar to one used by its competitor NeoCorp, can they take the deal? A moment's thought should suggest that the answer depends on how Cypher obtained the information. The general rule is that the obligation not to acquire, use, or disclose a trade secret obtained through improper means follows the secret downstream to subsequent parties as long as they know or have reason to know that the information reached them via an upstream misappropriation.[36] An email from a mysterious hacker is likely to put MatrixCorp on notice that the information was obtained by nefarious means.

35. *Id.* at 8.
36. UTSA, *supra* note 8, § 1(2).

G Defenses

The two most significant "defenses" to trade secret infringement are independent rediscovery and reverse engineering. I put "defenses" in quotation marks to emphasize that neither adds anything to the doctrines you have already seen. The defendant who establishes that she independently came up with the same information has actually defeated a crucial element of the plaintiff's case-in-chief: that the defendant stole the information *from the plaintiff*. Reflecting this, the Restatement simply excludes them from its definition of "improper means": "Independent discovery and analysis of publicly available products or information are not improper means of acquisition."[37] In addition, sometimes there are free-expression reasons or other important social policies to allow the disclosure of trade secrets.

1 Independent Rediscovery

Independent discovery needs little further discussion; it is nearly indistinguishable from ordinary research and development. In this context, "independent" means independently of the misuse of a trade secret. Thus it is allowable "independent" rediscovery to mount your own search for information that your competitor has, which you have learned the existence of through permissible means. For example, if they are selling 99.95% pure widgetium, it is permissible to infer that they have a secret process for purifying widgetium, conduct research, and develop a purification process.

On the other hand, it is not "independent" rediscovery to use improperly obtained secrets to guide your search. If your competitor's VP of engineering offers asks for a $100,000 bribe to tell you what *not* to try in your widgetium-purifying research, your next call should be to their head of security or the FBI, not to your own R&D division. True, they are not selling you the secret process itself. But they are still passing along a trade secret in breach of a duty of confidentiality, and there is no way to launder that breach into an "independent" discovery.

2 Reverse Engineering

Reverse engineering is conventionally defined as "starting with the known product and working backward to divine the process which aided in its development or manufacture."[38] Courts sometimes add that the "known product" must have been obtained lawfully: it is no defense to argue that you reverse engineered the widget-making-machine you stole from your competitor's factory.

37. Restatement (Third) of Unfair Competition, *supra* note 5, § 43.
38. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974).

RAPCO brake components

Why allow reverse engineering? For one thing, it reflects a policy of recognizing personal- property owners' rights over their things. If you buy it, you can break it down. In this sense, reverse engineering is trade secret's version of an exhaustion or first sale defense. If you buy a thing in the open market, you take it free and clear of any trade-secret rights.

Reverse engineering also promotes the same values as trade secret law itself. In the words of the Supreme Court, it is "an essential part of innovation" that "often leads to significant advances in technology."[39] It thus reflects a policy of balancing upstream and downstream innovation, limiting the former to promote the latter.

Remember that reverse engineering is a *defense* to infringement; the possibility of reverse engineering does not necessarily destroy the existence of a trade secret. Consider *United States v. Lange*.[40] Matthew Lange worked for Replacement Aircraft Parts Co., a/k/a RAPCO. As its name indicates, RAPCO made replacement airplane parts. Lange and others designed RAPCO's replacement parts by buying original parts, and then reverse engineering them:

> Knowing exactly what a brake assembly looks like does not enable RAPCO to make a copy. It must figure out how to make a substitute with the same (or better) technical specifications. Aftermarket manufacturers must experiment with different alloys and compositions until they achieve a process and product that fulfils requirements set by the Federal Aviation Administration for each brake assembly. Completed assemblies must be exhaustively tested to demonstrate, to the FAA's satisfaction, that all requirements have been met; only

39. Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 160 (1989).
40. United States v. Lange, 312 F.3d 263 (7th Cir. 2002).

> then does the FAA certify the part for sale. For brakes this entails 100 destructive tests on prototypes, bringing a spinning 60-ton wheel to a halt at a specified deceleration measured by a dynamometer. Further testing of finished assemblies is required. It takes RAPCO a year or two to design, and obtain approval for, a complex part; the dynamometer testing alone can cost $75,000. But the process of experimenting and testing can be avoided if the manufacturer demonstrates that its parts are identical (in composition and manufacturing processes) to parts that have already been certified. What Lange, a disgruntled former employee, offered for sale [for $100,000] was all the information required to obtain certification of several components as identical to parts for which RAPCO held certification.[41]

Lange was arrested and charged under the federal EEA, which incorporates essentially the UTSA definition of "trade secret."[42]

In theory, anyone could do what RAPCO did: take an airplane part and reverse engineer it. Thus, Lange argued, the designs he offered for sale were not actually "secret" in the first place. This argument failed. The key is that RAPCO actually invested the time and money to do the hard work of reverse engineering, and Lange didn't. Just like a dry-cleaning equipment salesperson who picks up the phone and laboriously builds a list of dry cleaners in a large metropolitan area, or an oil-exploration firm that conducts geological surveys, RAPCO acquired valuable information that others lack. As long as its competitors do not have ready access to that information, it qualifies as a trade secret. Lange was trying to sell them a shortcut to what RAPCO learned through hard work, and it is precisely that shortcut that trade secret law tries to prevent. Others are free to reverse engineer RAPCO's parts (just as it itself did), but they are not free to bribe Lange for the details.

3 Freedom of Expression

Free-speech concerns also weigh on trade-secret cases. *RTC* is a case in point; Scientology was using trade-secret law to silence its critics. At a high level, there is a stronger First Amendment argument for being allowed to *disclose* a trade secret (which necessarily involves speech) than for for *acquiring* one (which is often illegal in other ways) or for *using* one (which looks like purely economic conduct). Indeed, there is Supreme Court caselaw suggesting there is a First Amendment right (at least for the press) to publish information of public concern, even if it was obtained improperly. In *Bartnicki v. Vopper*, an unknown party illegally wiretapped a telephone call bweteen teachers' union officials discussing

41. *Id.* at 265.
42. EEA, *supra* note 3, § 1839.

a threat to "blow off [the school board's] front porches."[43] The recording was mailed to a local activist, who gave it to a radio host, who played it on the air. The school board sued under the federal Wiretap Act and a state equivalent, which prohibited not just the interception of telephone communications (in trade secret terms, acquisition) but also the disclosure of intercepted communications.[44] The Supreme Court held that the activist and host were protected by the First Amendment:

> We think it clear that . . . a stranger's illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern. The months of negotiations over the proper level of compensation for teachers at the Wyoming Valley West High School were unquestionably a matter of public concern, and respondents were clearly engaged in debate about that concern.[45]

These First Amendment protections for disclosure, however, may not reach trade secrets. In *Bartnicki*, the Supreme Court withheld judgment about the "the application of [wiretapping laws] to disclosures of trade secrets or domestic gossip or other information of purely private concern."[46] And in *DVD Copy Control Ass'n, Inc. v. Bunner*, the California Supreme Court drew on that language in a trade-secret case against Andrew Bunner, who posted the code for a program, DeCSS, that would let users decrypt DVDs and copy them to their computers. The association that controlled the copy-protection on DVDs sued him for trade-secret misappropriation. The court upheld a preliminary injunction against Bunner, explaining that the injunction "burdens no more speech than necessary to serve the government's interest in encouraging innovation and development" and "merely applies this venerable standard of commercial ethics to a constitutionally recognized property interest in information."[47]

Still, courts do sometimes find ways internal to trade-secret law to avoid imposing liability on defendants making expressive disclosures. Bunner won on remand. The court there held that DeCSS was widely available online, so the horse was already out of the barn, and the plaintiffs had not shown that Bunner was the one who opened the barn door by posting it first.[48]

43. Bartnicki v. Vopper, 532 U.S. 514, 519 (2001).
44. 18 U.S.C. § 2511(1)(a), (1)(c).
45. *Bartnicki*, 532 U.S. at 535.
46. *Id.* at 533.
47. DVD Copy Control Ass'n, Inc. v. Bunner, 75 P.3d 1, 14 (Cal. 2003).
48. DVD Copy Control Ass'n Inc. v. Bunner, 10 Cal. Rptr. 3d 185 (Cal. Ct. App. 2004). Unsurprisingly, the DeCSS code is still available online. Similarly, in *RTC*, Erlich won because the documents might already have been public when he posted them, and Scientology couldn't prove that they weren't. The OT documents also remain widely available online.

4 Whistleblowing

In general, whistleblower laws protect employees (and sometimes others) from retaliation for complaining about illegal conduct, making it public, or bringing it to the attention of authorities. The details vary greatly and are based in different bodies of law, depending on the jurisdiction, the industry in question, the kind of misconduct, and the way in which the employee reports it. For example, employers may not fire or demote employees for reporting overtime violations or sexual harassment. An especially striking system is that the Dodd-Frank Wall Street Reform and Consumer Protection Act authorizes the Securities and Exchange Commission to award whistleblowers between 10 and 30 percent of the fines it recovers as a result of their reports—in some cases, tens or even hundreds of millions of dollars. The general policy of whistleblower laws is to *defeat* secrecy when it is being used to hide wrongdoing.

But is it a *trade* secret?

Enter trade secret law. Some information is a trade secret, but shouldn't be. Not only do companies use secrecy to hide unethical or illegal business practices, they sometimes use threats of trade secret litigation to keep anyone from spilling the beans. The DTSA created a whistleblower defense. Not only does it carve out whistleblowing from DTSA liability, it preempts *all* trade-secret liability for whistleblowers who meet its criteria.

> (1) An individual shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that—
>
> (A) is made—
>
> (i) in confidence to a Federal, State, or local government official, ei-

ther directly or indirectly, or to an attorney; and

(ii) solely for the purpose of reporting or investigating a suspected violation of law; or

(B) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal.[49]

Note that this defense only applies to disclosures; it does not protect the acquisition of trade secrets by improper means, or the use of improperly-obtained trade secrets.

Problems

Moe Syzslak preparing a Flaming Moe

Flaming Moe's Problem

Moe Szyslak is the owner of Moe's Tavern, where the specialty drink is a "Flaming Moe." Moe mixes the drinks in a back room, then sets them on fire in front of customers.

1. Representatives from Tipsy McStagger's Good-Time Drinking and Eating Emporium meet with Moe to discuss licensing the recipe. As part of the negotiations, Moe tells them how it's made. Tipsy's breaks off talks and starts selling its own version. ***What result?***
2. A Tipsy's employee orders a Flaming Moe, pours it into a thermos, and uses a gas chromatograph to analyze its chemical composition. By so doing, he learns that the secret ingredient is cough syrup. ***What result?***

49. Defend Trade Secrets Act (DTSA), 18 U.S.C. § 1833(a)(1).

"Ace II" lock

Victor Fanberg

3. A Tipsy's employee goes to Moe's Tavern and bribes a bartender to tell her the formula. ***What result?***
4. Same facts as before, except that anyone who tastes the drink can recognize that it's cough syrup. The Tipsy's employee still bribes the bartender to tell them. ***What result?***

Locksmiths Problem

You represent the Chicago Lock Company, whose "Ace" series of locks is used in vending machines, burglar alarms, and other high-security settings. Ace locks use an unusual cylindrical key that requires specialized equipment to cut. Each lock has a serial number printed on it; the company uses a secret formula to translate the configuration of tumblers inside the lock into a serial number. The company's policy is that it will sell replacement keys only to the registered owner of a lock with a given serial number. All Ace locks and keys are stamped "Do Not Duplicate."

For years, locksmiths have known how to analyze Ace locks. After a few minutes poking at the lock with their tools, they can write down the configuration of pins and tumblers inside the lock. They can then go back to their toolkits and grind a replacement key, which will open the lock. If the locksmiths keep the configuration information on file, they can grind replacement keys in the future without needing to go back to the lock and analyze it again. Individual locksmiths have, for years, kept such files for their local customers.

Recently, Morris and Victor Fanberg, two locksmiths, published a book entitled "AA Advanced Locksmith's Tubular Lock Codes." They asked locksmiths around the country to send them lists of Ace lock serial numbers and the corresponding tumbler configurations. Based on that information, they were able to program a computer to reconstruct Chicago's secret formula. The book contains a table that shows how to turn an Ace serial number into a key configuration, which any locksmith with the proper equipment could then use to cut a key opening the lock

Philadelphia Eagles coaching staff giving signals

Jeff Luhnow

with that serial number.

Because the serial numbers on Ace locks are frequently printed on the outside, Chicago is concerned that the publication of this book will undermine the security of Ace locks. It has asked you whether it can and should sue the Fanbergs for damages and to halt publication of the book, and whether it should make any changes to its procedures in the future. What is your advice?

Sports Secrets Problem

In 2007, the New England Patriots football team videotaped the hand signals used by coaches for the New York Jets to send instructions to players on the field. Anyone in the stadium with a clear line of sight is able to see the signals. The National Football League's rules allow for such videotaping, but only from specific areas not including the areas the Patriots taped from (which had better views).

1. You work for the NFL Commissioner's office. Should you recommend that the Patriots or any of their players or employees be subjected to disciplinary action?
2. You work for the New York Jets. Should you sue the Patriots or any of their players or employees for trade secret misappropriation?
3. You are an Assistant United States Attorney. Should you seek an indictment of the Patriots or any of their players or employees for violating the Economic Espionage Act?

In 2011, the Houston Astros baseball team hired Jeff Luhnow as their new general manager. Previously, Luhnow had been an executive with the St. Louis Cardinals. While with the Cardinals, Luhnow and others build an extensive database with detailed statistical information about players and reports on prospective hires. When Luhnow moved to the Astros, several Cardinals employees went with him. Other Cardinals employees suspected that Luhnow might have helped design a similar database for the Astros. They guessed that he and the other ex-Cardinal employees might have used the same passwords for the new Astros system, a guess that turned out to be correct. The Cardinals employees logged into the Astros system using these passwords and examined some of the informa-

tion in it.

1. You work for the Commissioner of Baseball's office. Should you recommend that the Cardinals or any of their employees be subjected to disciplinary action?
2. You work for the Houston Astros. Should you sue the Patriots or any of their employees for trade secret misappropriation?
3. You are an Assistant United States Attorney. Should you seek an indictment of the Cardinals or any of their players or employees for violating the Economic Espionage Act?