Table of Contents

2

Trade Secret

Trade secret law protects against the theft of valuable business secrets.[1] Why does it do so? Consider the following:

Greek fire was 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. Instead, water somehow caused it to burn hotter – or perhaps spread it around (the accounts are a bit vauge at times). It was used as a weapon either by launching flaming cloth balls doused in it, or later, with a kind of flamethrower device that propelled flaming sprays of the stuff. 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.

Historians credit Greek fire with being responsible, in part, for the longevity of the Byzantine empire. In the 8th century the Byzantines used it to drive off Arab invasions, and they were still using it six centuries later. It was a central element of the Byzantine navy's dominance of the eastern Meditteranean; a flame that can't be extinguished by water is a truly fearsome weapon against wooden ships.

The Byzantines recognized that the military edge that Greek fire 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 it battle didn't know how it was made. A bit of historical folklore holds that each emperor was required to swear three oaths: never to surrender Constantinople, never to abjure the one true Christianity (viz. Eastern Orthodoxy), and never to give up the secret of Greek fire. So closely and effectively did the Byzantines guard it, in fact, that knowledge of how to make Greek 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

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).

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

still don't know today how Greek fire was made.[2]

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**: protecting trade secrets helps resolve Arrow's Information Paradox by making it possible to contract securely for disclosing them.
- **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 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, and the 2016 Defend Trade Secrets Act (DTSA) added a federal civil cause of action and an important seizure remedy.

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."[3]

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 some 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 threshold) can qualify as a trade secret.

2. It still happens. A material codenamed FOGBANK was used in W76 nuclear weapons. FOGBANK's composition was classified. So was its use. And so was the 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.

3. Restatement (Third) of Unfair Competition § 39 (1995).

This is a ***threshold test***: information needs to clear a minimum level of something (value, creativity, fame, etc.) to be protectable. The other is qualitative. Only information with an "economic" value that "can be used in the operation of a business" counts, which suggests that information with non-economic value (e.g. subjective personal importance) does not. This is a ***categorical test***: certain kinds of information are protectable, and certain other kinds are not.

Both tests are interesting, but only one is important. The economic value test 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."[4] When a plaintiff believes that a secret has sufficient value to be worth suing over, the courts almost never second-guess that belief.

The restriction to business information, on the other hand, does real work. 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."[5] The UTSA refers broadly to "information, including a formula, pattern, compilation, program, device, method, technique, or process."[6]

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.* ("*Netcom II*"), in which the Church of Scientology sued Dennis Erlich, a dissident former minister who had posted various of its internal documents on the Internet.[7] 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. But the *spiritual* value of the Church's secrets is not necessarily the same as the *economic* value demanded by trade-secret law.

A bad version of the argument that religious secrets are not trade secrets was that the Church of Scientology was not in business to make money. But religious and non-profit corporations, like their for-profit cousins, can do business, even if the accumulation of profits is not their ultiamte aim. Just as they can own and use real estate for churches and offices, they can own and use information.

A better but still unsuccessful argument against the Church's religious trade secrets was that they were monetized directly by being shared, rather than indirectly in some other commercial or industrial

4. *Id.* § 39 cmt. e.

5. *Id.*
6. Uniform Trade Secrets Act § 1.4 (1985) [hereinafter UTSA].

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

Dennis Erlich holding a press conference

7. Religious Tech. Ctr. v. Netcom On-Line Commc'ns Servs., Inc. ("*Netcom II*"), 923 F. Supp. 1231 (N.D. Cal. 1995).

process. The Church shares its teachings only with members who have been initiated into its higher ranks by underoing a legnthy and expensive "auditing" process. This too is not unique to organized religions. The *Netcom II* opinion persuasively discusses an earlier case, *SmokEnders, Inc. v. Smoke No More, Inc.*, involving a "step-by-step regimented program [to quit smoking] which requires that each [participant] perform each act of the program at a particular time."[8] If this course manual for self-improvement could be a trade secret because the program was shared only with customers who paid for the course, then the secrets of Scientology could also be trade secrets, because they too are techniques for self-improvement shared only with members who are selected for (and pay for) auditing.

8. SmokEnders, Inc. v. Smoke No More, Inc., 184 U.S.P.Q. 309 (S.D. Fla. 1974).

Is this a *competitive* advantage? It is true that organized religions claim to answer to a different standard than marketplace success.[9] 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 competition enough for the court in *Netcom II*.

9. 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.")

The real anxiety running through the Scientology litigation – which the court does its level best not to acknowledge – is that the arguments the RTC makes in claiming trade-secret status for its scriptures are in serious tension with the Church's claims to be a *bona fide* religion. For some observers, the way in which the Church monetizes its mysteries – and the vast sums of money involved – is inconsistent with taking their spiritual content seriously. The Church has had extensive battles with the IRS over its tax-exempt status, and there are countries that do not recognize it as a religion.[10] For our purposes, the thing to note is that a version of this anxiety arises whenever IP rights are asserted in a context that is governed by a non-monetary value system.

10. *See* Lawrence Wright, Going Clear (2013) (documenting the Church's controversial history).

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]

11. UTSA, *supra* note 6, § 1(4).

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

"Secrecy" is something of a term of art. Whether something is considered secret as a factual matter depends heavily on what kinds of obser-

vation and disclosure trade secret law will protect against. The "readily ascertainable by proper means" prong explicitly incorporates part of the infringement test. The only way to understand which information is truly "secret" is to become familiar with the cases applying the test.

Consider *United States v. Lange*.[12] 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 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.[13]

Lange was arrested and charged under the federal EEA, which incorporates essentially the UTSA definition of "trade secret."[14]

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

12. United States v. Lange, 312 F.3d 263 (7th Cir. 2002).

RAPCO brake components

13. *Id.* at 265.

14. Economic Espionage Act § 1839 (1996).

did), but they are not free to bribe Lange for the details. (Lange's argument conflates the reverse-engineering defense to an infringement claim with the definition of what is a protectable "secret" at all.)

Matters would be different if recreating an airplane part took two hours and cost $75 instead of two years and $75,000. In this case, the design would be "readily ascertainable," and there would be no trade secret in it in the first place. Lange would still be engaged in an act of disloyalty by misappropriating company resources for his personal benefit, for which he could be liable to RAPCO (and for which it would certainly fire him). But his actions would not also be trade-secret misappropriation or a violation of the EEA.

Lange also raises the issue of who counts as the relevant audience, i.e. "other persons who can obtain economic value from its disclosure or use." Most members of the general public are not in a position to analyze and design aircraft parts. We don't know what to look for, and even if if we did, we wouldn't know how to use a dynamometer, and we certainly don't have 60-ton wheels sitting around. But RAPCO's competitors – other aircraft-part manufacturers – do have the necessary expertise and equipment. The crucial point is that these competitors did not have RAPCO's detailed information on the design of aircraft brakes, and that information would be valuable to them if they did.

In addition to being a subject-matter case, *Netcom II* 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*, and court filings are generally matters of public record. But while the *Netcom II* 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 if not, then 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.

Erlich also argued that because the documents were widely available on the Internet, they could not be considered trade secrets. This argument is a winner, *provided that Erlich himself was not the one responsible for making them widely available*. You can't murder your parents and ask for mercy as an orphan; you can't post trade secrets and then argue that they're no longer secret. But if someone else, not acting in concert with Erlich, posted them, then he is as free as anyone else to repost and share them. They are no longer secret.[15]

15. The OT documents remain widely available, e.g., at https://file.wikileaks.org/file/scientology-ot-levels.pdf.

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 inde-

pendent 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 parties have protectable trade secrets in the information.

3 Collaborations

Finally, actual secrecy helps resolve questions of allocating ownership within collaborations. Two or more people working together can jointly own a trade secret.[16] 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."[17] This default can be broadened or narrowed by contract. The 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 busness, 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. 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 reason-

16. "Three may keep a secret, if two of them are dead." Benjamin Franklin, *Poor Richard's Almanack*, July 1735

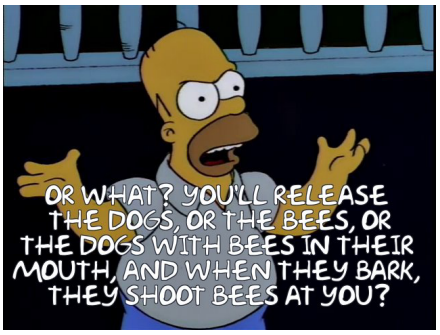
17. Restatement (Third) of Unfair Competition, *supra* note 3, § 42 cmt. e.

> able period of time or to inventions or discoveries resulting solely from the general skill and experience of the former employee.[18]

18. *Id.* § 42 cmt. g.

C Procedures: Reasonable Efforts

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. 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."[19] 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.



Reasonable efforts? (*The Simpsons* episode 1F16, "Burns' Heir")

> 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. 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.[20]

19. UTSA, *supra* note 6, § 1(4)(i)(i).

20. United States v. Lange, 312 F.3d 263, 266 (7th Cir. 2002).

It is always possible to imagine even stronger efforts. (Indeed, almost by definition, 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.[21]

21. *Id.*

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

that they are costly? Why isn't the test simply efforts sufficient to maintain actual secrecy? A useful list of theories why comes from Judge Richard Posner's opinion in an otherwise-unremarkable trade secret case, *Rockwell Graphic Systems, Inc. v. DEV Industries, Inc.*[22] To summarize:

1. They 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. They are evidence of actual secrecy. The fact that papers are kept under lock and key helps show that they are not widely available.
3. They are evidence of misappropriation. (This one takes a little more thought to see.) If documents are not normally shared with subcontrators, it is less likely that a rival obtained them innocently from a subcontractor on a job site.
4. They provide fair notice to potential defendants. If papers are stamped "CONFIDENTIAL," employees who deal with them know they are dealing with information the company considers proprietary.
5. The requirement provides an incentive for owners to 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.

Which of these strike you as persuasive?

22. Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174 (7th Cir. 1991).

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".[23]

23. UTSA, *supra* note 6, § 1; Restatement (Third) of Unfair Competition, *supra* note 3, § 40.

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."[24] 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."[25] 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.

24. UTSA, *supra* note 6, § 1(1).

25. Restatement (Third) of Unfair Competition, *supra* note 3, § 43.

a Espionage

The classic case on espionage is *E.I. du Pont de Nemours & Co. v. Christopher*[26] The DuPont chemical company was building a methanol plant in Beaumont, Texas, when employees noticed a small aircraft circling over the plant. Within hours, their investigation revealed that Rolfe and Gary Christopher were in the plane, taking aerial photographs. DuPont surmised that they had been hired by a competitor, and that their photographs would enable that competitor to infer DuPont's secret process for making methanol.[27] When the Christophers refused to identify their client, DuPont sued for trade secret misappropriation, and won.

What makes *Christopher* a fun case is that nothing the Christophers did was otherwise criminal or totrious. So far as the record shows, the Christophers' plane was complying with all Federal Aviation Administration regulations, and trespass law does not prohibit overflights. There is no general law against taking photographs from a place where you have a right to be. So if these were "improper means," it is trade secret law itself that considers them so.

One strand of the court's reasoning is economic. "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." This point resonates with the innovation theory of trade secrecy; it emphasizes that trade-secret law prevents competitors from taking unfair shortcuts by free-riding on each others' efforts.

The hard question in *Christopher* is which surveillance techniques are allowed. To answer this question is also to answer the question of which efforts to maintain secrecy are sufficient, which is the flip side of the same coin. DuPont could have prevented the overflight surveillance by putting a temporary shed over the construction side, at enormous expense. Why not require that precaution too? Alternatively, why require DuPont to put up fences? Shouldn't trade-secret law protect it against photographers at ground level, too? The court's reasoning is typical of trade-secret cases:

> 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 manufac- ture. 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.[28]

This sounds like a forseeability or cost-benefit analysis, but the court's

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

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

27. "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).

28. *Christopher*, 431 F.2d at 1016.

explanation of why it strikes the balance where it does takes a decidedly non-economic turn:

> 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 wheel- ing industrial competition must not force us into accepting the law of the jungle as the standard of morality expected in our commercial relations. . . .
>
> 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.[29]

29. *Id.* at 1016—17.

This too is typical of trade-secret cases. Courts' views of proper commercial morality drive their interpretations of what constitue "impromper means."

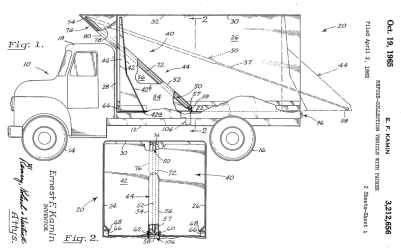
Cases of accident or mistake are often usefully thought of as espionage-adjacent. It is the difference between stealing deal documents from an airplane seatmate's briefacse, and shoulder-surfing as they read through the documents.

b Breach of Confidence

Turn now to the other prong of improper means, breach of confidence. *Kamin v. Kuhnau* is reasonably representative.[30] 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 1955, he struck a deal with Richard Kuhnau to use Kuhnau's machine shop to experiment with truck designs and build prototypes.

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

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.



One of Kamin's garbage-truck designs

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 v. Prudential-Bache Securities, Inc.*, contract law would suffice. But, like so many other business partners, they neglected the IP terms in their contracts. And 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.[31] 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.[32] "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*:

> 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.[33]

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 v. Wilder* 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

31. Restatement of Emp't Law § 8.01 (2015).

32. Restatement of Emp't Law § 1.01.

33. *Kamin*, 374 P.2d at 152—53.

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 through use or disclosure that it is made actionable. There is 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 posssession, 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.[34]

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

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 screts, 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 complete 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 a recipient makes a "material change of position" before learning of the mistake, they are free of their trade-secret obligations.[35] 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,"[36] which sounds in reasonable efforts, rather than intent.

35. UTSA, *supra* note 6, § 1(2)(C).

36. Restatement (Third) of Unfair Competition, *supra* note 3, § 40(b)(4).

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. Here is a typical holding from a court dismissing a trade-secret claim on the basis of no substantial similarity:

> 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 secret is discernible, DuPont's products implicate almost none of its elements.[37]

37. Big Vision Private, Ltd. v. E.I. Dupont De Nemours & Co., 1 F. Supp. 3d 224 (S.D.N.Y.).

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*.[38] 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.

38. Grynberg v. BP, PLC, No. 06 Civ. 6494 (RJH) (S.D.N.Y Mar. 30, 2011).

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 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 pro-

> posed consortium. That it did so is unsurprising and does not evince the kind of suspicious similarity present in [previous cases].

This is the opposite of *Big Vision Private, Ltd. v. E.I. Dupont De Nemours & Co.* 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.[39] An email from a mysterious hacker is likely to put MatrixCorp on notice that the information was obtained by nefarious means.

39. UTSA, *supra* note 6, § 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."[40]

40. Restatement (Third) of Unfair Competition, *supra* note 3, § 43.

1 Independent Rediscovery

Independent discovery needs little further discusison; it is nearly indistinguishable from ordinary research and development. In this con-

text, "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."[41] 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.

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. 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."[42]

41. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974).

42. Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 14 (1989).

3 Freedom of Expression

Free-speech concerns also weigh on trade-secret cases. *Netcom II* is a case in point; Scientology was using trade-secret law to silence its critics. But *Netcom II* is also typical of how courts handle such cases: mostly by finding ways internal to trade-secret law to avoid imposing liability on defendants making expressive use. Ehrlich won because the documents might already have been public when he posted them, and Scientology couldn't prove that they weren't.

Similarly, in *DVD Copy Control Ass'n, Inc. v. Bunner*, Andrew Bunner posted the code for a program, DeCSS, that would let users decrypt DVDs and copy rip them to their computers.[43] The association that controlled the copy-protection on DVDs sued him for trade-secret misappropriation. He argued that an injunction against position DeCSS would violate his First Amendment rights, but the California Supreme Court disagreed: although the UTSA restricted speech, it did so in a content-neutral fashion for an important government purpose. On remand, however, the appellate court dissolved the injunction for essen-

43. DVD Copy Control Ass'n, Inc. v. Bunner, 75 P.3d 1 (Cal. 2003).

tially the same reason as in *Netcom II*.[44] 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.

44. DVD Copy Control Ass'n Inc. v. Bunner, 10 Cal. Rptr. 3d 185 (Cal. Ct. App. 2004).

H Near Misses

This section isn't about trade secret law. Instead, it covers near misses to trade secret law: other laws protecting secrets (or in some cases, requiring them to be disclosed). Consider whether it is appropriate to describe each of these bodies of law as a kind of "intellectual property." Why or why not?

1 Property Law

There is a symbiotic relationship between trade-secret law and underlying property law that is worth exploring. Suppose that instead of flying over the Beaumont refinery, the Christophers had climbed over a perimeter fence, picked the lock on a construction trailer, and left with a stack of engineering diagrams. This would have been trade-secret misappropriation, but it would also have been trespass, burglary, and theft. The Christophers could have been prosecuted, and DuPont could have sued them, even if trade-secret law did not exist.

Most obviously, trade-secret law depends on property law to identify zones of exclusive access that are protected from prying eyes. The physical boundary around the Beaumont plant corresponds to a legal boundary that others, including competitors, are legally bound to respect. Trade-secret law can simply point to existing legal boundaries when identifying intrusions on these zones as improper means. It does not always draw precisely the same boundaries; *Christopher* is a hard case precisely because the Christophers found a way to observe the construction that was not also a violation of DuPont's property rights. But most of the time, property law provides the natural starting point. This includes real property protected by trespass law, like the Beaumont facility; personal property protected by theft law, like briefcases of corporate documents; and personal property protected by computer-misuse law, like corporate networks. Some of trade secret's other boundaries, like the reverse-engineering defense, also have roots in property law.

Property law also creates a line of virtual fenceposts around trade-secret law, much as it allows owners to erect physical fenceposts around their property. Breaking and entering is still criminal even if the burglar is caught before reaching the shop floor where the secret prototypes are stored. The prosecution does not need to prove that the burglar was there in search of trade secrets; the entry itself is prohibited. This simplifies the legal system's job, and it also simplifies competitors' jobs: rather than worrying about exactly which room in an office building contains the confidential marketing plans, they know that they shouldn't enter the building at all without permission.

A little less obviously, trade helps provide a normative justification for property law. One might ask what harm a few fence jumpers really do, provided they are careful not to damage any of the construction equipment. Why should such harmless trespasses be prohibited? One important answer is that property law protects against more than physical damage; the interest in exclusivity is also a way of securing confidentiality. Owners can do what they want with their property, and they are entitled to do it in a way that shields them from observation. Buidlings have walls; briefcases have locks; servers have passwords.

Given this baseline of property rights, what does trade-secret law add? First, as noted, it catches a few oddball fact patterns where there is no violation of underlying property law, like overflights. Second, it unifies property- and contract-based ways of misappropriating secrets. Third, it provides conceptual clarity about what is being protected: the confidentiality of information as such, rather than a more abstract interest in exclusive ownership. And finally, it provides a remedial menu better tailored to the harm of misappropriation, including injunctions on the use of information, damages for the value improperly obtained, and remedies against downstream recipients who are aware that the information was improperly taken.

Looking at property law from a secrecy perspective sheds a new light on an interesting and difficult cluster of cases that have to do with who is granted permission to use property, and on what conditions. Ordinarily, consent of the owner is a complete defense to property torts and crimes, and voluntarily revealed information cannot be the subject of a trade-secret claim. DuPont cannot sue its own employees for being on the site of the Beaumont plant, or for observing its trade secrets while they are there. So what if the Christophers *have themselves hired* by DuPont to assist with constuction, and pass along what they learn to a competitor? The trade-secret answer is that this is a breach of confidence leading to liability. But is it also trespass? On these facts, the question is unimportant; the trade-secret cause of action gives DuPont everything it needs.

On other facts, where trade secrecy is unavailable, the question matters more. There is a danger that property laws will be used to conceal information that should not actually remain secret. Consider *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, in which two reporters for ABC *PrimeTime Live* went undercover as employees at Food Lion supermarkets, where they videotaped allegedly unsafe food-handling practices.[45] "The broadcast included, for example, videotape that appeared to show Food Lion employees repackaging and redating fish that had passed the expiration date, grinding expired beef with fresh beef, and applying barbeque sauce to chicken past its expiration date in order to mask the smell and sell it as fresh in the gourmet food section." Food Lion sued ABC and the reporters for trespass.

There was no question that the reporters entered on Food Lion property, or that they had Food Lion's consent to do so. But consent procured by fraud is sometimes invalid, so the court had to decide whether the re-

45. Food Lion, Inc. v. Capital Cities/ABC, Inc., 194 F.3d 505 (4th Cir. 1999).

Hidden-camera footage from ABC's investigation of Food Lion

porters' failure to disclose that they were also working for ABC, or their disloyalty in airing Food Lion's dirty laundry, was so serious that it effectively negated Food Lion's consent. The Fourth Circuit (applying state law) split the difference. On the one hand, it reasoned that their entry after failing to disclose their employment with ABC in their job applications "was not invasive in the sense of infringing the kind of interest of the plaintiffs that the law of trespass protects; it was not an interference with the ownership or possession of land." On the other, it held that "the breach of duty of loyalty—triggered by the filming in non-public areas, which was adverse to Food Lion" was sufficient to trigger trespass liabiity. If there is a planet on which this distinction makes sense, it is not the planet Earth. But this inconsistency is characteristic of the false-pretenses trespass caselaw. Compare *Desnick v. American Broad. Cos.* (no trespass for ABC *PrimeTime Live* reporters to pose as patients of an ophthalmic surgeon performing allegedly unnecessary operations) with *Shiffman v. Empire Blue Cross & Blue Shield, 256 A.D.2d 131* (trespass for CBS reporters to "gain[] entry to plaintiff's private medical office by having a reporter pose as a potential patient using a false identity and bogus insurance card.")

Hidden-camera footage from ABC's investigation of Desnick Eye Care Centers

Trade secrecy provides a useful perspective on these cases because it allows us to step back from the details of trespass and consent, and to ask whether the acquisition and disclosure of information is wrongful. That is what Food Lion was truly upset about, and why it was initially able to obtain a $5.5 million punitive-damage jury verdict (later reduced). Trespass was just a convenient doctrinal peg. From this point of view, there are serious problems with Food Lion's case, and good reasons why it could not also win a trade-secret claim. The expressive interest in revealing dangerous food-handling practices, or unnecessary surgery, is a powerful one. This is where the real action is, and it is not possible to reach a coherent answer to these cases within property law without taking the relative strength of these expressive interests into account. Similar issues arise with "ag-gag" laws that prohibit entry into or videotaping inside of slaughterhouses, and with hidden-camera interviews designed to catch abortion advocates making allegedly embarassing admissions. Few of these cases involve trade secrets as such, but they helpfully point out trade secret law's pragmatism.

2 Computer-Misuse Law

These are cases in which property law should perhaps stay its hand in light of trade secret's *reluctance* to impose liability. There are also cases in which other bodies of law should perhaps stay their hands in light of trade secret's *willingness* to impose liability.

Consider *United States v. Nosal* and *United States v. Nosal*. David Nosal was a former employee of Korn Ferry, an executive-recruiting firm, who left to start his own executive-recruiting firm, and you can probably see where this is going already. He persuaded several colleagues still at Korn Ferry to download large quantities of data from

David Nosal

Korn Ferry's internal database of names and contact information. Nosal and the colleagues were indicted for violating subsection (a)(4) of the federal Computer Fraud and Abuse Act, which makes it a crime to "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtain anything of value."[46]

46. Computer Fraud & Abuse § (a)(/4).

The prosecution initially proceeded on the theory that Nosal aided and abetted his colleagues in violating subsection (a)(4), i.e., that they had exceeded authorized access by using the information downloaded from Korn Ferry computers for purposes prohibited by Korn Ferry. The Ninth Circuit dismissed these counts of the indictment, reasoning that punishing "individuals who access a computer with authorization but then misuse information they obtain by means of such access" would "make criminals of large groups of people who would have little reason to suspect they are committing a federal crime" such as employees who use work compputers for "gchatting with friends, playing games, shopping or watching sports highlights" in violation of their employer's computer-use policies. Undetterred, the government reindicted Nosal on a different theory – effectively, that he accessed Korn Ferry computers through the account of his former executive assistant, who was still at Korn Ferry. This time, the Ninth Circuit upheld the conviction, reasoning that his account had been permanently revoked when he left Korn Ferry, so he personally was categorically not authorized to access Korn Ferry computers at all.

It is possible to defend either opinion based on the text of the CFAA. It is even possible to defend both, although the line between having your friend access a computer for you using their account and accessing it yourself through their account with their permission is an exceedingly fine one. It makes civil and criminal liability turn on which one of two co-conspirators was at the keyboard.

But perhaps a better question to ask is why this is a job for the CFAA at all, when trade-secret law stands at the ready. Nosal was also convicted for violating the EEA, which is squarely on point under either theory of his conduct. Nosal committed open-and-shut misappropriation through breach of confidence. Taking the CFAA out of the picture still leaves his acts appropriately subject to civil and criminal sanction, while cancelling the parade of horribles about employees playing online poker on their lunch breaks. The difference is that Nosal took valuable Korn Ferry secrets, which slacking employees do not.

To be clear, there are appropriate roles for computer-misuse law to play in protecting secrets. Among other things, it helps to define the property boundaries that trade-secret law protects through its espionage prong. If Nosal had been an outsider who hacked into Korn Ferry's computers using a password cracker and downloaded confidential files, this would have been an unambiguous CFAA violation *and also* trade-secret misappropriation. Having trade-secret law available to protect the confidentiality of valuable information reduces the pres-

sure to turn an anti-hacking law like the CFAA into a general-purpose information-protection law.

Problems

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.

Moe Syzslak preparing a Flaming Moe

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 start 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?***
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?***

Christopher Redux Problem

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?

Whistleblower Problem

Your client works as a data scientist for a large insurance firm. She has written a widely-circulated internal report on racial and gender biases in an machine-learning algorithm the firm uses to flag claims for review, and is deeply dissatisfied with what she sees as the firm's lack of concern about her findings. Some of her colleagues to whom she circulated the report share her frustration, but the head of claims adjusting made a final decision to continue using the algorithm. She believes that there would be public outrage if the facts were more widely known, and is prepared to suffer some personal consequences, but would prefer not to if she doesn't have to. Counsel her on her options.

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 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 Commisioner'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 information in it.

1. You work for the Commisioner 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?

Exploits Problem

Exploit brokers are in the business of helping people defeat computer security. Governments want to thumb through the hard drives of terrorists, criminals, and dissidents. Identity thieves want passwords and bank account numbers. Extortionists want to delete data and hold it for ransom. Corporate spies want access to competitors' computers. All of them are willing to pay handsomely for the technical tools that enable them to do so. These tools are typically built around "exploits": short pieces of software that take advantage of bugs in commonly-used software like Windows, Adobe Flash, and iOS. As soon as as software companies learn about these bugs, they race to issue updates to fix them; once that happens, any exploits based on those bugs stop working. Thus, secrecy is essential to the exploit business in two ways: many of the uses are illegal, and exploits become worthless soon after they become public knowledge.

Can exploit brokers – who buy exploits from the computer security experts who discover them and then resell those exploits to various clients – rely on trade secret law? Should they be able to? Do the materials in this chapter and the previous one shed any light on how you would expect the exploit business to work, and how it ought to be regulated?