WHERE THE TRADE SECRET SITS: HOW THE ECONOMIC ESPIONAGE ACT IS INFLAMING TENSIONS IN THE EMPLOYMENT RELATIONSHIP, AND HOW SMART EMPLOYERS AND EMPLOYEES ARE RESPONDING

ADAM WAKS*

The dawning of the information age, coupled with a greater understanding of the value of intellectual property, has increased the quantity of proprietary information businesses choose to keep as trade secrets. An often-underappreciated cost of trade secrets is the effect they have on the employment relationship – they frequently result in employers and employees involving themselves in convoluted legal and contractual relationships beyond their own expectations or comprehension. Further complicating the matter is the Economic Espionage Act ("EEA"), which increases the stakes of employer-employee conflict by criminalizing the misappropriation of trade secrets. This note provides a primer to help both employers and employees deal with the specific issues trade secrets frequently create in the employment relationship, first by outlining the current status of trade secrecy law, then by examining how the EEA is changing the trade secrecy landscape, and finally by providing a practical summary of best practices.

* Adam Waks is a 2014 J.D. candidate at the New York University School of Law. He received a B.A. in Psychology and in English and Creative Writing from the George Washington University in 2007. He would like to thank Professors Rochelle Dreyfuss and Harry First for their comments and editing during the Innovation Policy Colloquium, for which this note was originally written. He would also like to thank Molly Ryan, Leah Rosenbaum, and the rest of the JIPEL editorial team for their thoughtful assistance.

"We dance round in a ring and suppose,
But the Secret sits in the middle and knows."

Robert Frost, *The Secret Sits*, 1942.

INTRODUCTION

Homaro Cantu's Chicago restaurant, Moto, is a unique destination. Customers entering the space are greeted, not by a floral arrangement or bubbling fountain, but by a Class IV laser set on a pedestal.[1] What draws most patrons to Moto however is not the unusual décor but the inventive food, which includes an edible menu, synthetic "champagne," and dessert flapjacks frozen to -273 degrees Fahrenheit.[2] To foodie diners familiar with molecular gastronomy, such bizarre fare is par for the course. For these customers, the real surprise comes when Moto's signature cotton candy "paper" dessert[3] arrives and they see the following written in edible ink on the confection itself: *Confidential Property of and © H. Cantu. Patent Pending. No further use or disclosure is permitted without prior approval of H. Cantu.*[4]

As remarkable as it is for restaurant customers to see a claim of ownership on their food, it is not surprising that Chef Cantu wants to protect what he considers his intellectual property. The inventive Chef is notoriously secretive, and for good reason: in addition to twelve prospective patents awaiting approval by the Patents and Trademarks Office ("PTO"), Chef Cantu has both invented and perfected a bevy of techniques, materials, machines, and processes that he chooses to keep as trade secrets.[5] Chef Cantu's desire to protect his intellectual property extends to his employees as well: eager chefs seeking apprenticeships receive a full background check and must sign a confidentiality agreement before ever entering his kitchen.[6] This state of affairs creates a vexing problem for those who study under Cantu: when they move on to other restaurants or open one of their own, what knowledge and information are they allowed to take with them, and what, if anything, are they required by law to leave behind?

Trade secrets have always created headaches in the employment relationship. However, as exemplified by Chef Cantu, the dawning of the information age, coupled with a greater understanding of the value of intellectual

---

[1] The laser, normally used for surgery, is used at Moto for food preparation. *See* Jennifer Reingold, *Weird Science*, FAST COMPANY, May 2006, at 40, 42.

[2] *See id.* at 47.

[3] The dessert is a flat sheet resembling a leaf of paper, embossed with an image of a stick of cotton candy, and which tastes like the fairground treat when dissolved on the tongue.

[4] *See* Pete Wells, *New Era of the Recipe Burglar*, FOOD & WINE (Nov. 2006), http://www.foodandwine.com/articles/new-era-of-the-recipe-burglar.

[5] *See* Reingold, *supra* note 1, at 48; Wells, *supra* note 4.

[6] *See* Reingold, *supra* note 1, at 48.

property, has increased the quantity of economically valuable confidential information businesses (high-tech and low-tech alike) choose to classify as trade secrets. As a result, employers and employees frequently find themselves in convoluted legal and contractual relationships beyond their own expectations or comprehension. Further complicating the matter is the Economic Espionage Act ("EEA"), passed by Congress in 1996. It is the first federal statute to criminalize the theft of trade secrets, and it increases the stakes of employer-employee conflict throughout the nation by allowing the use of government resources to criminally prosecute alleged trade secret misappropriation.

This Note is organized into three sections. In Part I, I outline the current status of trade secrecy law at both the state and federal levels. In Part II, I discuss the conflicts created in the employment relationship by trade secrets, and explore how the EEA and its recent amendments are exacerbating these conflicts. In Part III, I provide a summary of best practices aimed at allowing employers to maintain their trade secrets, while allowing employees to preserve their ability to accumulate general knowledge and skill on the job and still retain an optimum level of job mobility.

II
THE CURRENT STATUS OF TRADE SECRECY LAW

A. Civil Law: The Uniform Trade Secrets Act

Trade secrets predate any specific legal regime; they are not statutory creations, but rather secrets kept by one entity to gain advantage over other entities.[7] Over time, laws were developed to provide basic rights to trade secret holders.[8] Modern civil trade secrecy law is primarily governed by state law, which

---

[7] *See* Thomas J. Rechen & Peter L. Costas, *Trade Secrets Law - Principles, Pitfalls and Pronouncements*, 71 CONN. B.J. 360, 362 (1997) (tracing the evolution of trade secrecy laws from the common law to state and then federal statutes).

[8] Because of its common law roots, trade secrecy doctrines developed differently in the different states across the United States. *See id.*; *see also* Unif. Trade Secrets Act, Prefatory Note (with 1985 amendments) ("Notwithstanding the commercial importance of state trade secret law to interstate business, this law has not developed satisfactorily. In the first place, its development is uneven. Although there typically are a substantial number of reported decisions in states that are commercial centers, this is not the case in less populous and more agricultural jurisdictions. Secondly, even in states in which there has been significant litigation, there is undue uncertainty concerning the parameters of trade secret protection, and the appropriate remedies for misappropriation of a trade secret.").

is heavily influenced by the Uniform Trade Secrets Act ("UTSA").[9] With a few notable exceptions,[10] the laws in states that have adopted the UTSA are relatively uniform. While there are differences in the laws of states that have not adopted the UTSA,[11] those differences are largely procedural and do not effect a merits-based determination of a trade secret's existence or its misappropriation.[12]

A trade secret is broadly defined as information which (1) is secret and (2) has value from being unknown to the general public.[13] Information is considered "secret" if the trade secret holder takes reasonable steps to prevent the secret from discovery,[14] and the information has "value" if it can be defined as having worth in general economic terms (although there is some disagreement between states as to how that worth should be calculated).[15] A trade secret is "misappropriated" when

---

[9] In 1979, the Uniform Trade Secrets Act was published in an attempt to codify a national standard for trade secrecy law by offering states a comprehensive package of trade secrecy legislation ready for adoption. *See* Unif. Trade Secrets Act, Prefatory Note (amended 1985). States quickly obliged, and as of March 2013, 46 states have adopted the broad principles of the Act, and legislation to formally adopt the UTSA has been introduced in a 47th state. *See* The Nat'l Conference of Comm'rs on Unif. State Laws, *Legislative Fact Sheet - Trade Secrets Act*, UNIFORM L. COMMISSION (2014), http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act.

[10] *See infra* note 23 on inevitable disclosure and the related discussion.

[11] The laws of states that have not adopted the UTSA are still primarily governed by state common law, even in instances where those states have enacted their own trade secrecy statutes.

[12] Differences include statutes of limitations, the availability of attorneys' fees, and the requirements for preliminary injunctions. One merits based difference is the "continuous use requirement," which exists in some jurisdictions but not others, and which dictates that trade secret holders must continue to use a trade secret in a commercial manner for it to continue to be subject to trade secrecy protection. The UTSA does not include this requirement. *See* Michael H. Bunis & Anita Spieth, *Common Law v. UTSA: The Last States Standing*, LAW360 (Apr. 02, 2012, 12:22 PM ET), *available at* http://www.choate.com/uploads/113/doc/bunis-spieth-law360-common-law-v-utsa-the-last-states-standing.pdf.

[13] *See* Unif. Trade Secrets Act § 1 (1985); RESTATEMENT (THIRD) OF UNFAIR COMPETITION §39 (1993).

[14] *See* Unif. Trade Secrets Act § 1 (1985); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1993).

[15] *Compare* TEX. PENAL CODE ANN. § 31.05(a)(4) (West 2013) ("'Trade secret' means the whole or any part of any scientific or technical information, design, process, procedure, formula, or improvement that has value and that the owner has taken measures to prevent from becoming available to persons other than those selected by the owner to have access for limited purposes."), *and* H.B. 1225, 2013 Mass. 188th Gen. Ct. (Mass. 2013) (proposing a value requirement), *with* MASS. GEN. LAWS ANN. ch. 93, § 42 (West 2014) (not requiring any value for the existence of a trade secret); *see also* C. Rachal Pugh, *Bernier v. Merrill Air Engineers*, 17 BERKELEY TECH. L.J. 231, 235 (2002) (noting that the UTSA and the First Restatement

an individual or company (1) obtains the trade secret through improper means, (2) obtains the trade secret through proper means but uses or discloses it against the wishes of the owner, or (3) obtains the trade secret from a third party *and* knows or has reason to know that the trade secret was not properly obtained or disclosed by that party.[16]

The remedies available for misappropriation in the civil context include both monetary damages[17] and injunctions.[18] General monetary damages are measured by economic loss and unjust enrichment, and usually take the form of a reasonable royalty for the period of time it would have taken the violator to discover the trade secret independently.[19] In extreme cases, a damages award may be doubled as punishment to the violator.[20] A successful suit can also leave the violator liable for the trade secret holder's attorney's fees.[21] Injunctions can be tailored to fit the needs of any given situation, but the general practice requires barring the violator from utilizing the misappropriated secret for as long as is necessary to eliminate any commercial advantage gained or potentially gained through the misappropriation.[22] An injunction is even available in limited circumstances to prevent an employee possessing trade secrets from joining a competitor.[23]

---

definition of trade secret differ in that the UTSA omits any requirement that the information be "used in one's business," signaling support for a broader definition placing less emphasis on the actual value of the secret).

[16] Unif. Trade Secrets Act § 1(2) (1985) ("(i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (ii) disclosure or use of a trade secret of another without express or implied consent by a person who (A) used improper means to acquire knowledge of the trade secret; or (B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was (I) derived from or through a person who had utilized improper means to acquire it; (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or (C) before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.").

[17] Unif. Trade Secrets Act § 3 (1985).

[18] Unif. Trade Secrets Act § 2 (1985).

[19] Unif. Trade Secrets Act § 3(a) (1985).

[20] *Id.* at § 3(b).

[21] *Id.* at § 4.

[22] *Id.* at § 2 cmt. ("The general principle of Section 2(a) and (b) is that an injunction should last for as long as is necessary, but no longer than is necessary, to eliminate the commercial advantage or 'lead time' with respect to good faith competitors that a person has obtained through misappropriation. Subject to any additional period of restraint necessary to negate lead time, an injunction accordingly should terminate when a former trade secret becomes either

B. Criminal Law: Enter the Economic Espionage Act

The federal government passed the Economic Espionage Act in 1996[24] in an attempt to create a "comprehensive and systematic" approach to address trade secrecy misappropriation through the federal criminal justice system.[25] The EEA's definition of "trade secret" is similar to, and informed by, the definition in the UTSA,[26] requiring that the information be both "secret" and have "value" from being generally unknown.[27] The EEA definition of "misappropriation" includes the three acts prohibited by the UTSA, as well as attempt and conspiracy, for which there is no corresponding civil liability.[28] The EEA also contains a mens rea element not required by the UTSA: there is no criminal misappropriation unless the violator (1) intends to misappropriate the secret and (2) either intends to use it for the economic benefit of someone besides the owner or intends or knows that the use of the misappropriated secret will injure the owner.[29] No criminal liability will attach under the EEA unless the misappropriated property is used or intended

---

generally known to good faith competitors or generally knowable to them because of the lawful availability of products that can be reverse engineered to reveal a trade secret.").

[23] The judicially created doctrine of "inevitable disclosure" holds that where an employee in possession of trade secrets wishes to take a new position with a different company, and where the new position is of such a nature that it is *inevitable* that the employee will disclose the trade secrets in the course and scope of his or her new employment, the court may enjoin the employee from taking the new position. Although a potent tool for employers, the doctrine is inconsistently applied by courts, and has been rejected entirely in some circuits. *See* Barry L. Cohen, *The Current Status of the Inevitable Disclosure Doctrine A Unique Trade Secret Litigation Tool*, 3 LANDSLIDE 40, 41 (2010); *see also* Adam Waks, *Keeping the Cat in the Bag: Inevitable Disclosure Doctrine and Its Inevitable Evolution*, JIPEL BLOG (Feb. 6, 2014, 4:58 PM), http://jipel.law.nyu.edu/2014/02/keeping-the-cat-in-the-bag-inevitable-disclosure-doctrine-and-its-inevitable-evolution/.

[24] Economic Espionage Act of 1996, Pub. L. No. 104–294, 110 Stat 3488.

[25] *See* Presidential Statement on Signing the Economic Espionage Act, 2 Pub. Papers 1814 (Oct. 11, 1996). ("This Act establishes a comprehensive and systemic approach to trade secret theft and economic espionage, facilitating investigations and prosecutions."). While the EEA does not preempt state criminal law, it can provide guidance to trade secret holders and their employees in a globalized world where job opportunities often extend beyond state lines. *See* 18 U.S.C. § 1838 (2012).

[26] H.R. REP. No. 104-788, at 12 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4031 ("The definition of the term 'trade secret' is based largely on the definition of that term in the Uniform Trade Secrets Act.").

[27] 18 U.S.C. § 1839(3) (2012).

[28] *Id.* § 1832(a).

[29] *Id.*

for use in interstate or foreign commerce.[30] Remedies under the EEA for violations by an individual include a fine with no enumerated cap and a prison sentence of up to ten years.[31] Organizations convicted under the EEA can face fines of up to $5 million.[32] Courts have significant discretion when determining the amount of the fine.[33]

A separate provision of the EEA, meant to discourage foreign economic espionage, criminalizes trade secret misappropriation intended to benefit a foreign government, instrumentality, or agent.[34] A violation of this section by an individual carries a maximum fine of $5 million and a prison sentence of up to fifteen years.[35] An organization that violates this provision will be fined the greater of $10 million or "three times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the secret that the organization has thereby avoided."[36]

C. The Impact of the Economic Espionage Act on Trade Secrets Generally

While there are some substantive differences between the EEA and existing civil trade secrecy laws,[37] the main practical difference is that the EEA is a federal

---

[30] *See* Theft of Trade Secret Clarification Act of 2012, Pub. L. No. 112-236, 126 Stat. 1627 (2102). The statute used to require that the trade secret be "included in a product that is produced for or placed in interstate or foreign commerce," but the definition was broadened as a result of a congressional amendment passed in the wake the acquittal of Sergey Aleynikov, a computer programmer accused of stealing information relating to his employer's high frequency trading system. *See* United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012).

[31] 18 U.S.C. § 1832(a) (2012).

[32] *Id.* § 1832(b).

[33] *See* United States v. Howley, 707 F. 3d 575, 582 (6th Cir. 2013) ("Determining the value of a trade secret, we acknowledge, is no easy task. But district courts need not reach an exact figure for the loss a victim suffered or the amount of harm a defendant caused or intended to cause; a "reasonable estimate" will do. U.S.S.G. § 2B1.1, cmt. n. 3(C).").

[34] 18 U.S.C. § 1831 (2012).

[35] Economic Espionage Act 18 U.S.C. § 1831 (2013) amended by the Foreign and Economic Espionage Penalty Enhancement Act (Pub. L. 112-269, January 14, 2013, 126 Stat. 2442) (increasing the available fine for individuals from $500,000).

[36] Economic Espionage Act 18 U.S.C. § 1831(b) (2013) (increasing the available fine for organizations from $10 million).

[37] For example, the EEA expressly defines several technologies not mentioned in the UTSA as trade secrets, ostensibly for the purpose of updating the definition to keep pace with fast changing technologies. The EEA also defines "value" more broadly than the UTSA to include any information that has value from not being known by the public, whether or not the trade secret owner is actually capable of capturing any of that value. *See* Gerald J. Mossinghoff et. al.,

criminal statute. As a result, violators of the EEA are subject to criminal penalties, and prosecutions are financed with public funds. Criminal prosecutions also implicate constitutional protections for defendants not implicated in civil trials, including the Fifth Amendment protection against self-incrimination, the Sixth Amendment guarantee to a speedy/prompt/timely trial, and the higher burden placed on prosecutors of proof beyond a reasonable doubt.

III
TRADE SECRECY LAW IN THE EMPLOYMENT CONTEXT

An economically efficient trade secrecy regime should allow employers to feel secure in their possession of trade secrets[38] and allow employees to gain general knowledge and skills in the workplace[39] while retaining an appropriate level of job mobility.[40] Such a regime requires that participants be able to distinguish between unprotected information that employees can take with them to subsequent jobs and protected information that they cannot. Current trade secrecy laws do a poor job of making this distinction and, as a result, create tension in the employment relationship.

A. Trade Secrecy and the Employment Relationship: Policy

To date, much of the commentary on trade secrecy in the employment context has focused on striking a balance between an employer's interest in protecting proprietary information and an employee's interest in gaining and using knowledge and skill to earn a living.[41] In reality, these interests are

---

The Economic Espionage Act: A New Federal Regime of Trade Secret Protection, 79 J. PAT. & TRADEMARK OFF. SOC'Y 191, 197 (1997).

[38] *See* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 178 (7th Cir. 1991) (describing the dual purpose of trade secrecy law as protecting personal property and regulating interpersonal relationships, and noting that each rationale serves a different purpose: the first encourages inventive activity, and the second prevents the undeserved redistribution of wealth).

[39] *See e.g.* Peter C. Quittmeyer, *Trade Secrets and Confidential Information Under Georgia Law*, 19 GA. L. REV. 623, 656 (1985) ("The distinction between trade secrets and general trade information reflects the principle that an individual should not be precluded from practicing his chosen trade or profession merely because he has become more skillful, sophisticated, and proficient as a result of prior experience and business associations.").

[40] High levels of job mobility are beneficial to both employees and employers: employees want to work for employers who need them most and will compensate them accordingly, and employers want to hire the most skilled employees. *See, e.g.,* Charles Tait Graves, *Trade Secrets as Property: Theory and Consequences*, 15 J. INTELL. PROP. L. 39, 43–44 (2007).

[41] *See generally* Melvin F. Jager, Trade Secrets Law § 8.01[3] (rev. 1992); *see also* ROGER MILGRIM, MILGRIM ON TRADE SECRETS § 5.02 (rev. 1990).

complementary: employers and employees both benefit from a regime that seeks to maximize the protection of these interests.[42] Although there are strong public policy rationales for favoring a trade secrecy regime that recognizes the relative importance of these complementary interests, this Note focuses on the practical implications for each party in the employment relationship.[43]

Employees benefit from laws protecting trade secrets because if employers do not feel secure in their possession of a trade secret, they will superficially limit the employee's access to that information. Employers will do this by hiring fewer employees, by unduly limiting which existing employees may work with the secret, or by installing economically inefficient safeguards in the workplace,[44] all of which result in negative outcomes for employees.[45] Meanwhile, employers benefit when their employees gain knowledge and skill on the job, as the fruits of an experienced employee generally accrue to the employer. Employers also benefit from a high level of employee mobility: if an employee suspects that experience or knowledge gained on the job is a trade secret, and thus not marketable, the employee has less of an incentive to acquire the experience or knowledge in the first place. Furthermore, employers do not want to limit themselves to the employees they already have; they also want to be able to hire new, highly skilled, highly knowledgeable employees away from their competitors.[46] In a world where trade secrecy laws unduly restrict employee's mobility, employers will be left with

---

[42] *See* Graves, *supra* note 40*; see also* Miles J. Feldman, *Toward A Clearer Standard of Protectable Information: Trade Secrets and the Employment Relationship*, 9 HIGH TECH. L.J. 151, 157 (1994).

[43] As a society, we have an interest in maximizing the productivity and satisfaction of our citizenry – having citizens trapped in jobs they cannot leave is a perversion of that interest. Moreover, many of those citizens were educated and trained using public funds, at public schools and universities. In order to get the best return on our educational investment, we need to ensure that each citizen can maximize the use of his or her skills. Additionally, we as a society benefit from the free exchange of information; we want to balance, within reason, the ability of an individual or group of individuals to work with and improve on the knowledge of others, while at the same time understanding that people want to benefit from their creations, and will likely demand some protection in order to invest in the creative process in the first place.

[44] *See* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*,* 925 F.2d 174, 180 (7th Cir. 1991) ("If trade secrets are protected only if their owners take extravagant, productivity-impairing measures to maintain their secrecy, the incentive to invest resources in discovering more efficient methods of production will be reduced, and with it the amount of invention.").

[45] Fewer employees hired means fewer job prospects for potential employees, and fewer employees allowed to work with the secret or increased safegaurds means fewer employees are able to gain valuable knowledge and skill while on the job.

[46] *See* Quittmeyer, *supra* note 39.

a disillusioned workforce with little incentive to expand their knowledge and experience, while also lacking the ability to hire new, quality employees.

B. Trade Secrets or "Know-How" v. General Knowledge and Skill

Whether a particular piece of information is a protectable trade secret owned by an employer, or general knowledge and skill an employee may take between jobs, is the crux of the issue creating tension in the employment relationship regarding trade secrets. Unfortunately, it is impossible to draft a set of rules *ex ante* to describe the millions of potential scenarios involving the classification of a particular piece of information as protectable or not.[47] This issue is significant—if too much information is protected as trade secrets employees lose job mobility, but if too little information is protected employers lose some of the economic value of their information when their employees leave for a new company. As described above, either scenario will have adverse impacts on both employees and employers.

Historically, courts have attempted to distinguish unprotectable "general knowledge and skill" from protectable trade secrets or "know-how,"[48] on the basis that the former stem from an employee's "education, ability, and experience,"[49] while the latter "derive their economic value from not being public information or general knowledge within an industry"[50] or are "informational and experiential expertise related to [the] practical application of specifics."[51] Courts often rely on lists of factors, such as those enumerated in past versions of the Restatement of Torts, for additional guidance.[52] While this approach provides some direction,

---

[47] *See* RESTATEMENT (FIRST) OF TORTS § 757, cmt. b (1939). ("The law of trade secrets looks to be stretched in further directions with the development of new forms of technology."); s*ee also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39, cmt. d (1995) ("It is not possible to state precise criteria for determining the existence of a trade secret. The status . . . [is] ascertained through a comparative evaluation of all the relevant factors, including the value, secrecy, and definiteness of the information as well as the nature of the defendant's conduct.").

[48] The concept of "know-how" is so important that it is expressly included in the definition of a trade secret in the UTSA commentary. *See* Unif. Trade Secrets Act § 1, cmt. 5 (1985) ("The words 'method, technique' are intended to include the concept of 'know-how.'").

[49] 2 TRADE SECRETS LAW § 8:6.

[50] ¶ 4.01 Nature of the Asset (Trade Secrets), 1998 WL 1038678, 3.

[51] *Id.* at 1 (quoting 1 R. MILGRIM, MILGRIM ON TRADE SECRETS § 1.09[3] (Matthew Bender, 1995)).

[52] *See e.g.* Richard F. Dole, Jr., *The Uniform Trade Secrets Act-Trends and Prospects*, 33 HAMLINE L. REV. 409, 420-21 (2010) ("A number of courts have found that the six factors identified by the Restatement (First) of Torts as pertinent to the existence of a trade secret remain

balancing multiple lists of factors and wading through complex judicial prose is a heady task for those formally trained in legal analysis, let alone the average American, and there remain many circumstances in which an employee or employer will be unsure *ex ante* whether a piece of information is general knowledge or skill or a protected trade secret. This confusion results in a system of after-the-fact litigation, even in cases where neither party is aggressively flouting cultural or legal norms.

An example of information that can be difficult to classify is "negative information," a form of legally protected know-how that "has commercial value from a negative viewpoint."[53] Put simply, negative information is the knowledge that some technique, process, formula etc. *does not* work. The UTSA expressly protects negative information as a trade secret, but gives no express justification for doing so.[54] On the one hand, the thought that an employee cannot take and utilize negative information seems strange; we, as a society, want inventors to find solutions to problems, and the knowledge that something does not work is precisely the sort of information we think of as a starting point that can lead to scientific and cultural breakthroughs.[55] On the other hand, it makes perfect sense that an employer would want to keep and protect this information if it is not generally known in the industry.[56] Regardless of whether a given piece of

---

relevant under the Uniform Act. The factors are: (1) the extent to which the information is known outside of his business; (2) the extent to which it is known by employees and others involved in his business; (3) the extent of measures taken by him to guard the secrecy of the information; (4) the value of the information to him and to his competitors; (5) the amount of effort or money expended by him in developing the information; [and] (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.").

[53] Unif. Trade Secrets Act § 1 (1985).

[54] *See* Charles Tait Graves, *The Law of Negative Knowledge: A Critique*, 15 TEX. INTELL. PROP. L.J. 387, 391 (2007)

[55] *See id.* ("The perceived mistakes and errors of one's predecessors, or of one's own making, can be a springboard to new ideas. Indeed, it is commonplace that creative individuals sometimes use detailed knowledge about previous approaches to problems in order to reject them."). Moreover, it can be almost impossible for an employee not to take this sort of information with them from job to job; how is an architect, hired to design an office building, supposed to ignore any failures he experienced in the past when designing similar office buildings?

[56] For example, a contractor hired to build a complicated piece of software might spend six months exploring multiple avenues that lead to dead ends before finally completing the project. If another company subsequently hires that same contractor to produce a similar product, he or she would produce it in significantly less time as a result of not having to repeat those previous mistakes. Since the contractor's previous employer paid for this knowledge, they have an interest in ensuring that their competitors do not benefit from it down the road.

information is protected or not, unless the employer and the employee agree on its classification up front, there may be legal ramifications down the road if that information turns out to be valuable.

C. How the EEA Increases Conflict in the Employment Relationship

As of September 2012, only 124 cases have been filed under either Section 1831 or 1832 of the EEA, with the vast majority brought under Section 1832.[57] However, the dearth of prosecutions under the act to date should not be taken as proof that the EEA is not currently affecting employment relationships. To begin with, Congress recently amended the Act,[58] and President Obama has stated that he intends to step up prosecutions under the Act as amended.[59] The broad bipartisan support for these amendments, coupled with the President's statement, has already led the Department of Justice ("DOJ") to place an increased emphasis on prosecuting trade secrecy misappropriation under the EEA.[60] Furthermore, regardless of the number of prosecutions the DOJ brings, the Act is still likely to have a chilling effect on job mobility and innovation as employees must consider the "worst-case scenario" when making decisions about how to treat potentially actionable information. The lack of clarity about what information is protected, combined with the potential for massive fines and jail time for misappropriation, likely deters employee action to an extent above and beyond what is suggested by the number of prosecutions actually filed.

---

[57] A Report on Prosecutions Under the Economic Espionage Act, Peter Toren, Esq., (Trade Secret Law Summit AIPLA Annual Meeting, Washington, D.C. October 23, 2012). Most prosecutions were brought against former employees, and the sentences for those convicted range from probation to over five years in prison. *See id.* at 5, 11.

[58] *See* The Foreign and Economic Espionage Penalty Enhancement Act (Pub. L. 112-269, January 14, 2013, 126 Stat. 2442); *see also* Theft of Trade Secret Clarification Act of 2012 Pub. L. No. 112-236, 126 Stat. 1627 (2012).

[59] *See* EXECUTIVE OFFICE OF THE PRESIDENT, ADMINISTRATIONS STRATEGY ON MITIGTING THE THEFT OF U.S. TRADE SECRETS 7 (2013), *available at* http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf (last visited March 31, 2013).

[60] *Colloquium on Innovation Policy Class Discussion with Andrea Sharrin, Deputy Chief, Computer Crime and Intellectual Property Section of the United States Dep't. of Justice* (April 2, 2013) (citing a 39% increase in prosecutions in 2012 compared to 2011 and a desire on the part of the DOJ to work with companies to bring additional prosecutions on their behalf).

1. Issues for Employers

The EEA benefits employers in two ways: (1) employers do not need to use private money to prosecute alleged violators and (2) criminal penalties provide a strong deterrent to potential violators. However, these benefits are not easily realized. For one, while the federal government will use public money to prosecute alleged EEA violators, trade secret holders must first convince the DOJ to take their case.[61] In the past, this has required trade secret holders to invest considerable time and money, up to and including actually preparing the case for the DOJ.[62] Moreover, the increased deterrent created by the EEA cuts both ways for employers: while the threat of criminal sanctions may prevent an employer's employees from leaving to join a competitor and taking trade secrets with them, that employer may not be able to hire competitors' employees, since those employees too fear the risk of changing jobs. Even worse, employers now have to worry about exposing themselves to the threat of criminal sanctions for misappropriating trade secrets when hiring employees from a competitor.

The EEA also has the potential to hurt employers in other ways. First, the federal government will receive the money from any fines assessed for a criminal conviction of trade secret misappropriation, meaning there will be fewer assets available to compensate the intellectual property holder for economic damages caused by the misappropriation.[63] In fact, it is feasible that an intellectual property holder might spend significant time and money working up a case for the DOJ, only to find that there is no money left to compensate the intellectual property holder when the criminal case is over, leaving the intellectual property holder worse off than he or she was before initiating the prosecution. Second, a criminal

---

[61] To date, the DOJ has been notoriously picky regarding EEA prosecutions. *See* Toren, *supra* note 57(noting that only 124 cases have been initiated under the EEA since it was passed in 1996).

[62] With limited federal dollars to spend on prosecutions, the DOJ has in the past been more likely to take cases that were already worked up by private entities. While the DOJ claims to be interested in working with trade secret holders to prosecute alleged misappropriations, it is likely that they will continue to choose which cases to pursue based on a reasonable cost-benefit analysis. Andrea Sharrin, Deputy Chief, Computer Crime and Intellectual Property Section of the United States Dep't. of Justice, Colloquium on Innovation Policy Class Discussion (April 2, 2013).

[63] While it is possible for a trade secret holder to both initiate a private suit and refer a criminal case to the DOJ, the DOJ is less likely to prosecute a case that is pending in civil court. *Id.* (citing as reasons the inability to control the actions of a private party engaged in a parallel suit coupled with a lessened need to initiate a criminal prosecution where a civil suit is already ongoing).

trial means that the intellectual property holder may be forced to disclose private financial information he or she would prefer to keep secret,[64] and possibly even be required to disclose the trade secret itself.[65]

2. Issues for Employees

For employees, the EEA is uniformly negative. The creation of serious federal criminal penalties results in over-deterrence, as employees who genuinely believe they possess unprotected information may still choose not to utilize it, fearing that if the information is later found to be protected, they will face jail time, large monetary fines, and the stigma associated with a criminal conviction. As a result, fewer employees will move between companies to new positions where they would be more economically useful, and fewer employees will leave to start businesses that compete with those of their current employers. Furthermore, employees generally now have less of an incentive to gain experience on the job, knowing that their employer might appropriate any knowledge or skill the employee gains simply by classifying it as a trade secret.

IV
BEST PRACTICES

As companies increase the amount of valuable, protectable information they create, and as the EEA provides for the federal prosecution of, and criminal penalties for, trade secret misappropriation, employers and employees are placed in an uncomfortable position regarding the classification and use of trade secrets. While this state of affairs is clearly adding to the inherent tension trade secrets

---

[64] For example, when determining fines in a criminal case, courts will often require intellectual property holders to disclose their research and development budgets so the court can place a "cost" on the misappropriation.

[65] Judges can issue protective orders to prevent the disclosure of trade secrets. *See e.g.* FED. R. CIV. P. 26(c)(1)(G). In fact the EEA contains a clause specifically instructing judges to do just that. Orders to Preserve Confidentiality, 18 U.S.C. § 1835 (1996). However, the fact remains that in a criminal trial the focus is on the defendant; intellectual property holders face the possibility that their rights will not be at the forefront, and that they will not be respected to the degree they might be were the intellectual property holders an actual party to the litigation. *See* Federal Open Market Committee v. Merrill, 443 U.S. 340, 362 n. 24 (1979); s*ee also* Coca-Cola Bottling Co. of Shreveport, Inc. v. Coca-Cola Co., 107 F.R.D. 288, 292 (D. Del. 1985) ("It is well established that trade secrets are not absolutely privileged from discovery in litigation."); Centurion Industries, Inc. v. Warren Steurer & Associates*,* 665 F.2d 323, 325 (10th Cir. 1981). *But see* Susan V. Metcalfe, *Protecting Trade Secrets: Is the Remedy Worse Than the Wrong?,* 104 DICK. L. REV. 503, 504 (2000).

generate in the employer/employee relationship, the question remains: what actions can employers and employees take to exploit new incentives produced by this regime, while minimizing their exposure to new risks?

A. For Employers

1. Protecting Your Trade Secrets

i. Make Sure Your Intellectual Property Satisfies The Trade Secrecy Requirements

For information to qualify as a trade secret, the information must be secret and derive value from being generally unknown.[66] Value is something information usually does or does not have, and, while "value" is defined differently in different statutes,[67] there are few practical things you as an information holder can do to ensure your information has value.[68] More important, from the standpoint of practical action, you must ensure that your information remains secret. The secrecy condition has three requirements: you must (1) identify the information as a trade secret, (2) notify others that you consider the information a trade secret, and (3) take precautions against reasonably foreseeable intrusions.[69]

The first requirement simply implies that you, as a possessor of information, should determine whether that information is a trade secret, as opposed to general knowledge or skill.[70] This requirement can be satisfied with some generality, but it

---

[66] *See supra* Section II.A Unif. Trade Secrets Act discussion; *see also supra* Section II.B EEA discussion.

[67] *See* Unif. Trade Secrets Act § 1 (1985), *and* RESTATEMENT (THIRD) OF UNFAIR COMPETITION §39 (1993); *See also* TEX. PENAL CODE ANN. § 31.05(a)(4) (West 2013) *and* MASS. GEN. LAWS ANN. ch. 93, § 42 (West 2014).

[68] Generally speaking, it is unlikely that any piece of intellectual property will not meet the legal definition of "value" if you as a trade secret holder believe it is valuable. As previously noted, some states require that a trade secret be used in the trade secret holder's business in order to have "value." *See* Bunis & Spieth, *supra* note 12. Generally speaking, if your secret has so little value to your business that you are not currently using it, it is likely not worth your time to find a way to use just to retain the right to protect it from misappropriation.

[69] *See supra* Section II.A Unif. Trade Secrets Act discussion; *see also supra* Section II.B EEA discussion.

[70] In most cases this is not a hard question to answer: a machine you designed with unpatented components or an unpatented mixture you invented is clearly a trade secret. Furthermore, no one expects a property owner to spend all of his or her time categorizing every component in an invention for intellectual property purposes. On the other hand, a property owner who simply declares that everything in his or her factory is a trade secret is likely to face a higher level of scrutiny if a lawsuit for misappropriation becomes neccessary at a later date.

is important: taking time *ex ante* to determine what information you consider proprietary places you in a better position to satisfy the next two requirements of the test, and to prevail in court if litigation becomes necessary.

There is a large body of literature concerning what it takes to satisfy the second and third requirements of notification and protection against intrusion.[71] Generally speaking, no one expects a trade secret owner to hold daily meetings to apprise employees of what information is or is not protected, but employers are expected to make some effort to notify employees where trade secrets exist. Potential actions include updating employee and contractor contracts, agreements, and handbooks to include information on trade secrecy, marking trade secrets in the workplace as "confidential," and posting notices reminding workers that they are working with trade secrets.[72] Regarding efforts to protect the information from intrusion, examples of steps an intellectual property owner can take include installing computer security (such as firewalls and passwords) and physical restrictions (such as locked doors and locked file cabinets) where trade secrets are stored.[73]

ii. When Hiring a New Employee

a. Contract and Employee Hiring Materials

Contracts are the single most important factor affecting the outcome of trade secrecy litigation and are the primary means by which employers and employees negotiate the boundaries between "know-how" and "general knowledge and skill" ex-ante.[74] Through contracts, you can tell your employees exactly what you expect of them, including what information they need to keep secret. While employees have a common law duty not to reveal an employer's trade secrets,[75] it is in both

---

[71] *See e.g.* Laurence H. Reece, III, *Developing a Program for the Protection of Trade Secrets*, MASS. CONTINUING LEGAL EDUCATION, April 1998; *see also* Diane Siegel Danoff, *New U.S. Laws Criminalize Theft of Trade Secrets, Including Quantitative Trading and Investment Models*, DECHERT LLP (February 2013), http://sites.edechert.com/10/926/february-2013/2013-02-06---ip---new-u.s.-laws-criminalize-theft-of-trade-secrets--including-quantitative-trading-and-investment-models.asp.

[72] *See id.*

[73] *See id.*

[74] *See* Alois Valerian Gross, *What is "Trade Secret" So As to Render Actionalable Under State Law Its Use or Disclosure by Former Employee,* 59 A.L.R. 4TH 641 (1988).

[75] *See* L.S. Tellier, *Implied Obligation of Employee Not to Use Trade Secrets or Confidential Information for His Own Benefit or That of Third Persons After Leaving the Employment,* 165 A.L.R. 1453 (1946); *see also* Unif. Trade Secrets Act, § 2 (ii)(B) (1985).

parties' interest to have an express, written contractual agreement addressing trade secrecy.[76]

Contracts can contain either general trade secrecy provisions or a separate non-compete agreement ("NCA") or non-disclosure agreement ("NDA").[77] You should have your employees sign your trade secrecy agreement when you first hire them, ensuring that the secrecy provisions are considered part of your overall business arrangement, and thus obtained in return for valuable consideration.[78] If you require additional contractual protection at a later date, you may need to give the employee additional consideration in return.[79] If you do not have a formal employment contract with some of your workforce, you should require all such individuals working with or around protectable information to sign an NDA.

When contracting for trade secrecy protections and limits to employee mobility, specificity is key. If a contract is too broad, an employee may refuse to sign it, or may demand compensation beyond what you are willing to pay. In the worst-case scenario for an employer, an employee may agree to the terms of a contract, only to have a court find the contract unenforceable or modify it.[80] All employees should receive and sign an employee handbook, updated regularly, to remind them about your trade secrets and their duty to safeguard them.

---

[76] Regardless of the common law duty, employees may use as a defense to infringement the claim that they were not put on notice that the information was protected. A good way to put an employee on notice is to make them sign a contract specifically stating that they are working with trade secrets, and listing (with some generality) the trade secrets involved.

[77] NDAs limit an employee's ability to disclose certain information from their job for a certain period of time. NCAs require that the employee not do certain work within a defined set of parameters (usually a time-frame or geographical location, although geographic limitations are not as useful in the modern age).

[78] *See* RESTATEMENT (SECOND) OF CONTRACTS § 71 (1981). Any agreement between parties must be made in return for consideration (meaning essentially that each party gets something out of the deal). At the start of a business relationship, the law will view any trade secrecy restrictions placed on the employee as being exchanged in consideration for the job.

[79] *See* Maura Irene Strassberg, *An Ethical Rabbit Hole: Model Rule 4.4, Intentional Interference with Former Employee Non-Disclosure Agreements and the Threat of Disqualification, Part II*, 90 NEB. L. REV. 141, 145–46 (2011).

[80] *See* Michael J. Garrison & John T. Wendt, *The Evolving Law of Employee Noncompete Agreements: Recent Trends and an Alternative Policy Approach*, 45 AM. BUS. L.J. 107, 130 (2008) ("Although some states continue to reject partial enforcement of any kind or limit the courts' power to rewrite the terms of a restrictive covenant based on common law contract principles, there has been a clear shift from the blue pencil doctrine to reformation.").

Additionally, all contracts, handbooks, and NDAs should specify what information you consider proprietary.[81]

When hiring someone specifically to develop or improve intellectual property you intend to keep as a trade secret, you should include contractual provisions expressly assigning any and all information developed in the course and scope of the employment (if the individual is an employee) or project (if the individual is a contractor) to you. Where negative information is a concern, you should announce your intention to retain this information up front to avoid confusion later.[82] You may also wish to ask the employee/contractor to assign to you any intellectual property he or she is bringing into the relationship that relates to the work-product being developed.[83]

In limited circumstances, you may also want to have your employees sign an NCA. While NCAs do not generally influence trade secrecy litigation,[84] NCAs can be useful as a blunt instrument to protect intellectual property whose usefulness is of limited duration. Several states, including California, will not enforce NCAs on general policy grounds.[85] In states that do enforce NCAs, courts will require that the NCA comply with the "rule of reason," meaning that any restraints placed on the employee are (1) no greater than necessary to protect the employer, (2) not unduly oppressive to the employee, and (3) reasonable in light of sound public policy. If the judge finds, on balance, that the NCA does more to limit employee

---

[81] There is some disagreement regarding the benefits of specificity in an employment contract, handbook and/or NDA. On the one hand, telling employees exactly what information they can and cannot take with them following their employment can help prevent misunderstandings, and will decrease after-the-fact litigation in scenarios where employees misappropriate your intellectual property because they honestly did not know that it was your protected intellectual property. On the other hand, it can be problematic to draw employees' attention to specific information you consider valuable, and may result in more after-the-fact litigation involving employees who purposefully misappropriate your most valuable trade secrets. You need to decide for yourself which of these situations is more relevent to you and your business.

[82] *See id.* regarding specificity.

[83] Assignment will only cover information that is traded for consideration and that is not general knowledge and skill. *See e.g.* 2 TRADE SECRETS L. § 8:6.

[84] NCAs generally do not influence trade secrecy litigation: an employee agreeing not to work in a certain field for a certain time will not necessarily be on notice that any trade secrets exist, just that the employee is not allowed to do certain work for contractual reasons.

[85] *See* a full list of such states at Carmen Nobel, *Non-competes Push Talent Away*, HBS WORKING KNOWLEDGE (July 11, 2011), http://hbswk.hbs.edu/item/6759.html (last visited March 30, 2013).

mobility than is necessary, the judge can either find the NCA unenforceable altogether or limit its terms to the extent the judge deems sufficient to protect the employer.[86] Specificity is helpful for a "rule of reason" analysis: the more specific the agreement limiting an employee's right to work, the more likely a court will find that it satisfies the rule of reason.[87]

b. Have Certain Employees Conduct a Brain Dump[88]

Employees who leave their jobs to start ventures that compete with their former employers will often claim that they had the idea for their venture before beginning employment, and that any information they learned on the job was general knowledge and skill, not protected intellectual property.[89] This tactic is a common defense to allegations of trade secret misappropriation, and if successful, allows these employees to retain the intellectual property for themselves. The best way to prevent this defense is to ask all employees to conduct a "brain dump" prior to beginning the employment relationship, wherein they lay out all relevant intellectual property they own.[90] Employees should retain a copy of the brain dump and should give you a copy for your records.

Brain dumps benefit both employees and employers. A brain dump will put the employee at ease regarding ownership of the items the employee records, facilitate the transition into the employment relationship, and give you clear notice regarding what the employee believes he or she is bringing into the relationship. The brain dump will also provide you with specific knowledge regarding the

---

[86] *See e.g.*, Picker Intl, Inc. v. Parten, 935 F.2d 257 (11th Cir. 1991) (giving examples of "rule of reason" cases and their outcomes); *see also* Pugh, *supra* note 15, at 246.

[87] Examples of good limitations include lists of the specific protectable interests (a trade secret is generally a reasonable protectable interest), the type of protectable interest, the length of time before competition can resume, the geographical area where competition is disallowed, and the specific type of competition that is disallowed (e.g. a court is more likely to find enforceable an NCA that prohibits building a specific type of high frequency trading system than one which prohibits building high frequency trading systems in general). As previously stated, the value of a geographical limitation will greatly depend on the type of information at issue, as such limitations no longer serve a purpose in many types of businesses.

[88] Telephone Interview with Charles Valauskas, Senior Partner, Valauskas Corder LLC (March 20, 2013) (using "brain dump" as a term of art, meaning the transfer of all of the employee's knowledge on a given subject from one person to another or to a document).

[89] *Id.*

[90] At this point, it is imperative to let the employee know that you do not want them to divulge any trade secrets from their previous employer. In order to protect yourself from liability under the EEA, you should give the employee the disclaimer discussed in Section IV.A.2 below.

boundaries of the employee's claims to any intellectual property developed for you. A further benefit is that brain dumps are notoriously under-inclusive, and you may actually capture some otherwise protectable intellectual property the employee brings into the relationship.[91]

Some employees may push back against writing this information down and handing it to their employer – they may worry that you will appropriate this information and use it yourself. You can try to answer the employee's concerns by letting the employee know that the purpose of the exercise is specifically to make sure the employee gets to keep his or her prior intellectual property. You can also emphasize that it is up to the employee to phrase the brain dump, so the employee can control the conversation by writing down just enough to keep his or her intellectual property without actually giving away potential business ideas. In some cases this will not assuage the employee, who will refuse to hand any brain dump over to you.

iii. Terminating an Employee/When An Employee Chooses to Leave

a. Exit Interview

The exit interview gives you an opportunity to remind your employee of his or her contractual obligations regarding your intellectual property.[92] Where no contract exists, the exit interview provides you with a chance to tell the employee about his or her common law duties not to reveal your trade secrets.[93] The exit interview also enables you to control the conversation regarding potential future conflicts by telling the employee exactly what information you consider proprietary.[94]

Equally important, the exit interview allows you to learn where your soon-to-be ex-employee is going. This information can help you determine how much attention you should pay to the employee's future activities to ensure no trade secrets are misappropriated. Knowing your employee's plans will also help you

[91] *See* the limits on capturing value brought into the relationship by the employee, *supra* note 83.

[92] To the extent that they exist, you should remind the employee of any NDAs, NCAs, or contractual agreements entered into with you or your organization.

[93] *See* Tellier, *supra* note 75.

[94] *See supra* text accompanying note 81.

determine whether this is one of the rare instances in which you should seek a preliminary injunction to prevent your employee from taking the new position.[95]

Additionally, knowing where the employee is going enables you to contact the employee's new employer with any concerns you may have. Any conversation with, or letter to, the new employer should include the statement that your ex-employee possesses trade secrets, and should be as specific as possible without placing your trade secrets in danger of disclosure.[96] When deciding whether or not to contact the new employer, it is important to remember that conversations between competitors can raise the specter of anti-trust issues: any conversation you have with your employees' future employer should steer well clear of any topics which might even suggest the appearance of impropriety regarding competition for employees.[97]

Finally, the exit interview gives you the ability to maintain your relationship with your ex-employee, or at the very least, end the relationship on a professional, civil note. This simple touch can, in some cases, make an employee think twice before walking away with information he or she suspects might be a trade secret. While only successful in this capacity on the margins, the cost of an exit interview is an hour of time, as opposed to the massive monetary, emotional, and reputational costs of litigation. There is no reason not to try it, and every reason to hope it works.

b. Do Not Delete the Employee's Records

When an employee leaves, it is not always immediately clear whether he or she has misappropriated a trade secret. Upon receiving notice of the employee's upcoming departure, you should prepare an inventory of sensitive information the

---

[95] *See supra* text accompanying note 23.

[96] This will help fulfill the "on notice" requirement in the EEA regarding the new employer. Specifically mentioning the EEA is not a requirement, but it is a good idea.

[97] In a theoretical world, employers would not engage in this sort of anti-competative behavior because any agreement that limits the ability of competitors to poach talent from each other limits the competitor's ability to hire talented employees. Unfortunately, these sorts of arrangements do happen in the real world. *See, e.g.*, US v. Adobe Systems, Inc., No. 10-CV-01629, settlement announced (D.D.C. Sept. 24, 2010) (several high technology companies, including Adobe, Apple, Intel, and Google, agreed not to actively contact each other's employees with job opportunities). Whether or not such conversations between employers make sense from a public policy standpoint, they certainly make sense from the standpoint of an individual employer looking to protect his or her intellectual property, so long as the employer takes care to make sure that no anti-competitive discussions take place.

employee worked with, placing you on notice of what potential misappropriation, if any, you should be concerned about. You should also plan to retain the employee's records in case they are needed later for litigation. If the employee's physical workstation is required for another employee, you should have your IT department make a copy of the employee's hard drive and store it in order to maintain these records.

iv. If You Need to Sue

a. Civil, Criminal, or Both?

If you determine that your trade secrets have been misappropriated, you will likely want to seek a legal remedy. Which legal remedy is right for you will depend on many case-specific factors, including but not limited to the extent of your damages, what assets the violator has, the expected cost of civil litigation, whether you plan to seek a preliminary injunction, and whether the additional weight of criminal sanctions on the violator might harm your prospects of receiving damages. Before you can make an informed decision regarding a legal remedy however, you must first conduct a preliminary investigation to obtain all the relevant details about the misappropriation. This information will benefit you regardless of your eventual decision.[98] Following the investigation, you can weigh your options and decide whether to initiate a private civil lawsuit, refer the issue to the DOJ for criminal prosecution, or pursue a dual suite strategy.[99]

b. Be "White of Heart and Empty of Head"[100]

At every stage in a trade secrecy case, from the initial discussions between a trade secret holder and an accused violator, to the time a verdict is handed down by a judge or jury, facts trump law.[101] This means that you should not do anything that gives even the *appearance* of impropriety. Instead, you should contract up front to

---

[98] *See supra* discussion at III.C.1. The DOJ is less likely to take a case that has not been worked up for them already.

[99] You can also try and have your state government prosecute your ex-employee under state criminal law, where it exists. This option however is outside the scope of this Note.

[100] Telephone Interview with Charles Valauskas, Senior Partner, Valauskas Corder LLC (March 20, 2013) (using the phrase as a term of art, meaning the individual in question should behave in a way that avoids even the appearance of impropriety while actively avoiding information that could subject the individual to liability).

[101] *Id*. (stating a general principle of law as practiced in the real world that the circumstances surrounding a case, and how those circumstances reflect on the parties involved, will often determine the outcome of the litigation, regardless of the legal principles implicated).

protect your trade secrets, be clear with employees about what information you consider protected, and remind outgoing employees of their continuing contractual obligations and what you consider protected information. Above all, you should be reasonable regarding what information you claim is protected – inevitable disclosure doctrine aside,[102] judges tend to have little patience for employer's attempts to wrest legal protection from employees they failed to bargain with up front or to prevent employees from seeking meaningful employment elsewhere.[103]

2. Protecting Yourself From Liability For Misappropriating Others' Trade Secrets

Employers must be as careful to protect themselves from violating the trade secrets of their competitors as they are when protecting their own trade secrets. The civil liability for trade secret misappropriation can be large,[104] and the criminal liability can be even larger.[105] The key to protecting yourself from civil liability under the UTSA is defeating the "knowledge" requirement in the statute,[106] while in the criminal context, avoiding liability under the EEA is most easily accomplished by defeating the statute's "intent" requirement.[107] Fortunately, there are several simple steps employers can take to essentially guarantee this freedom from liability.

i. Employment Contract and Acknowledgement Forms

The employee contract and/or employee handbook should state that you take trade secrecy seriously, that it is your employees' responsibility to police their own actions regarding their previous employer's trade secrets, and that employees should report any concerns they have to you. You should require new employees to sign a statement acknowledging your policy and agreeing to its terms. The handbook should also give an overview of state trade secrecy laws and the EEA, and you should require new employees to sign a statement that the laws have been explained to them, that they understand them, and that they acknowledge their responsibility to use all possible efforts to avoid misappropriating a previous employer's trade secrets.

---

[102] *See supra* text accompanying note 23.

[103] *See* Strassberg, *supra* note 79.

[104] *See* Unif. Trade Secrets Act § 3 (1985).

[105] *See* Economic Espionage Act of 1996, Pub. L. No. 104–294, October 11, 1996, 110 Stat 3488 and related discussion, *supra* Section II.B.

[106] *See* Unif. Trade Secrets Act § 2 (1985) ("'Misappropriation' means: (i) acquisition of a trade secret of another by a person *who knows or has reason to know* that the trade secret was acquired by improper means") (emphasis added).

[107] *See* 18 U.S.C. 1832(a) (2012) and related discussion, *supra* Section II.B.

ii. Entrance Interview With the New Employee

An entrance interview will let you discern what, if any, potential trade secrets your new employee possesses from previous employment. Whether or not you are aware of any red flags, during the entrance interview you should repeat the admonishment contained in your employment contract and acknowledgement forms: it is the employee's responsibility to police his or her actions with respect to his or her former employer's trade secrets, that you take trade secrecy seriously, and that the employee should immediately bring any concerns he or she has to your attention. If there are any red flags, you should take the additional steps discussed below.

iii. Contact the Employee's Previous Employer[108]

Contacting your new employee's previous employer has two benefits. First, it allows you to form a relationship with the previous employer before any issues arise. Second, it gives you the opportunity to go on the record about your company policy regarding trade secrecy and the EEA. You should specifically mention the EEA in your conversation, and, depending on your level of concern, even suggest that they instruct their former employee, if they have not already done so, what information that was within that employee's purview they regard as a protected trade secret.

iv. Construct "Ethical Walls"[109]

Where a specific concern exists that an employee possesses actionable proprietary information from a previous employer relevant to his or her new position with your company, you may wish to construct an "ethical wall" around the employee to prevent disclosure. Effective restraints include hiring the employee into a position where trade secret disclosure is unlikely, telling your other employees not to discuss troubling topics with the new employee, and, if

[108] *See supra* text accompanying note 97.

[109] "A process for avoiding conflicts of interest by limiting disclosure of information to certain attorneys or individuals within a firm or corporation, thereby building a metaphorical wall between the holders of information and colleagues who represent interests or hold opinions which conflict. Also known as a Chinese wall." Ethical Wall – Legal Definition, YOUR DICTIONARY, http://law.yourdictionary.com/ethical-wall (last visited March 31, 2013).

necessary, completely separating the new employee from employees engaged in the area of concern.[110]

B. For Employees

While a system that enhances employee mobility benefits employees and employers equally, individual employees have a stronger incentive to retain mobility.[111] To succeed in this endeavor, employees must be aware of the issues trade secrecy laws present so they can take action to gain marketable skills, retain job mobility, and protect themselves from the threat of future litigation. Negotiating this complex landscape is not easy, and there is significant variability regarding a given employee's ability to bargain with his or her employer. Regardless, there are several actions most employees can take to help effectuate a positive outcome in their employment relationships regarding the use and retention of information.

1. When Hired At A New Company

i. Conduct Your Own Brain Dump[112]

The absolute worst-case scenario for you as an employee is to have your employer lay claim to knowledge, skill, or intellectual property that you rightfully owned before beginning employment.[113] If you are starting a job where you will be working with trade secrets, in an area where you believe you already possess intellectual property, it is imperative that you create a record of that property before beginning employment. [114] The most efficient way to do this is to write down all of the aforementioned information, and send a copy, certified mail, to a professional such as your attorney or accountant.[115] This way, if you ever face

---

[110] Telephone Interview with Charles Valauskas, Senior Partner, Valauskas Corder LLC (March 20, 2013).

[111] *See supra* Section III.A. Employees have the strongest incentive in a given relationship because, economically speaking, the most efficient outcome for an individual employer is a system in which everyone else's employees have maximum job mobility, but that employer's employees do not.

[112] *See supra* note 88.

[113] *See* TRADE SECRETS LAW § 8:6, *supra* note 83.

[114] The information you write down can include general knowledge and skill in addition to any protectable ideas. It is better to be over-inclusive then under-inclusive when conducting a brain dump.

[115] Telephone Interview with Charles Valauskas, Senior Partner, Valauskas Corder LLC (March 20, 2013).

trade secrecy litigation, you will have a record of what property was rightfully yours prior to employment, backed up by a quality witness.[116]

ii. Encourage Specificity in Your Contract

If your employer asks you to assign your rights regarding trade secrets, or demands that you sign an NDA or NCA, you should request that your employer specify what information you are being asked to renounce your claim to. Specificity in the contract provides you, as an employee, with two important benefits. First, it is important to know your employer's expectations. Your employer's expectations are especially important if you are going to be working directly with information that you believe may create negative information.[117] You should stress that this is for your employer's benefit as much as your own – you want to be sure you do not accidentally misappropriate information your employer believes to be a trade secret because you thought it was general knowledge or skill.

Second, to the extent that you do have any leverage when it comes to negotiating your contract, you increase that leverage by requesting specifics – it is easier to demand a higher salary when you are asked to give up all future rights to x, y, and z than it is when you are, for example, asked to sign a simple, standard NDA form. Tell your employer that the work you will do for them is worth more than their initial offer, since you are not simply agreeing to do work in exchange for a salary, but also being asked to give up rights to a higher salary in the future. This tactic will have varying degrees of success based on your negotiating leverage as a potential employee, but it is worth the chance to get either a higher salary or be allowed to keep rights you otherwise would have to give up.

iii. Be Prepared to Walk Away

Job prospects can be few and far between, even for highly educated employees. However, it is imperative that you remember what is at stake when a potential employer demands that you give up intellectual property rights in return for employment. When you agree to forego those rights, you decrease your future employment mobility, impair your ability to gain knowledge and skill while on the job, and face the prospect of civil and criminal liability in the future if you do not

[116] Attorneys and accountants you utilize in a professional capacity are good people to send this information to; they have a professional responsibility to be truthful regarding their interactions with you, which makes them particularly believable and reliable witnesses. Telephone Interview with Charles Valauskas, Senior Partner, Valauskas Corder LLC (March 20, 2013).

[117] *See supra* Section III.B and notes 53–56.

live up to your end of the bargain. If an employer demands that you give up rights above and beyond what the employer is willing to compensate you for, you must be prepared to turn down the job.

2. When Terminated And/Or Resigning

ii. Keep The Moral High Ground

When your relationship with your employer ends, voluntarily or not, it is vital that you maintain a "white heart and an empty head."[118] This means you should comply with all agreements executed between you and your now former employer and not take any company data or property with you.[119] In addition, you should refrain from conveying any memorized data to your next employer. This will require you to determine where your previous employer's trade secrets stop and where your general knowledge and skills begin. You may wish to be conservative in this regard until you have an opportunity to talk to your previous employer about what information he or she considers proprietary. If you are leaving voluntarily, you should be open and honest with your ex-employer about your new employment and what it entails.

ii. Request an Exit Interview

Few employees ever think of requesting an exit interview if their employer does not plan on conducting one, but there are several ways an exit interview can be beneficial. For example, while an exit interview does give your employer the opportunity to define what he or she considers protected intellectual property, it can also apprise you of your employer's expectations regarding that property, provide you an opportunity to protest if you think your employer is being unreasonable, and give you some idea of how aggressively your employer may pursue alleged trade secret misappropriation.[120] Second, and more important, the

---

[118] Telephone Interview with Charles Valauskas, Senior Partner, Valauskas Corder LLC (March 20, 2013).

[119] Telephone Interview with Professor Daniel DeWolf, Adjunct Professor of Law at the New York University School of Law, and Member, Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. (June 25, 2013) (noting that in many cases it is not the act itself, but the cover up of an act, that leads to legal action).

[120] On the other hand, most employees should already have some idea of what their employer considers intellectual property, and should have a feel for the company culture and how aggressively the employer might pursue perceived trade secret misappropriation. Moreover, employees have very little leverage at this stage in the process, so it is unlikely that they will change the employer's mind regarding the classification of information the employer considers

exit interview enables you to maintain your relationship with your ex-employer. It will surprise many employees to hear, but employers can feel genuinely hurt when a trusted employee decides to leave. Taking a few minutes to make sure you leave on good terms is well worth the investment.

3. When Leaving to Start Your Own Company

Employees leaving to start their own company or join an emerging company face a more difficult situation than those moving to an established company. The clout of an established company will deter litigation over intellectual property, because established companies are more likely to have the resources to defend against such litigation, as well as intellectual property of their own they can use as a shield.[121] Furthermore, the chance that an ex-employer will detect a small or inadvertent misappropriation by an ex-employee working for a large, well-financed organization is relatively small.

Individuals starting or joining an emerging company will not have the benefit of money or an organization to stand behind them, and the cost of litigation against startups is much lower than against established companies.[122] Potential misappropriation is also more easily detected, especially where the startup's business model revolves around the information at issue. Finally, startup investors are easily scared away by the threat of litigation, making the new company extremely vulnerable.[123] For all of these reasons, employees looking to leave an existing employer and start a new company must be extremely careful regarding the potential disclosure of that employer's trade secrets.

---

protected. Telephone Interview with Professor Daniel DeWolf, Adjunct Professor of Law at the New York University School of Law, and Member, Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. (June 25, 2013).

[121] *See e.g.* § 21:8. *Intellectual property strategy: Defensive protection, mutually assured destruction (MAD)*, 2 INTERNET LAW AND PRACTICE § 21:8 (noting that intellectual property can be equally valuable as a shield as it can as a sword, by functioning as a defense against lawsuits from companies worried about potential cross-suits).

[122] Since startups have fewer resources and often possess no intellectual property with which to threaten a cross-suit.

[123] While actual or threatened litigation will scare away potential investors, the mere possibility of future lawsuits is unlikely to have a dramatic effect. For early stage investors especially, such a possibility is simply one of many potential outcomes of an already high risk venture, and will likely not effect their decision regarding investment. Telephone Interview with Professor Daniel DeWolf, Adjunct Professor of Law at the New York University School of Law, and Member, Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. (June 25, 2013).

i. Request an Exit Interview

If you are planning to leave your current position to start a new company, it is essential that you request, and obtain, an exit interview. In the exit interview, you should be clear that you are leaving to start or join a new company. If your employer intends to assert ownership claims to any information required for your business, you want to know that as soon as possible. This is your opportunity to try to settle any potential issues without litigation – take full advantage of this meeting.

In certain circumstances, you may wish to disclose your basic business model to your employer in the exit interview for the purpose of determining if your employer believes that your business plan infringes on their intellectual property. For example, if your business plan does touch on your employer's intellectual property, then you are likely leaving because you have perceived an opening in the market that your employer is not currently exploiting. If it is not possible for you to discuss your business model without surrendering this knowledge to your employer, and you believe your employer might wish to expand into the market and compete with you if they become aware of the market opportunity, you will likely not wish to discuss it. On the other hand, if you can discuss your business plan generally without betraying your core competitive advantage, or if you do not believe your employer intends to expand into that market and compete with you, then it can be helpful to get your employer's tacit "approval" before you even walk out the door.

ii. Construct Ethical Walls

If you are concerned that you are in danger of disclosing information you know to be your ex-employer's trade secret, you should place a wall between yourself, as an entrepreneur building and running a new company, and any position within the new company that works with the information in question.[124] Even where you do not think you are in danger of disclosure, when hiring someone to do

[124] This strategy is not universally embraced. Professor DeWolf disagrees with the assertion that it makes sense to hire an otherwise unnecessary individual and put up an ethical wall when dealing with potential trade secrets, reasoning that an ex-employer who believes an ex-employee's new company is infringing on a trade secret is likely to litigate regardless of any ethical walls the ex-employee claims to have put in place. Meanwhile, hiring an additional employee in the early stages of a company means giving up valuable equity. Telephone Interview with Professor Daniel DeWolf, Adjunct Professor of Law at the New York University School of Law, and Member, Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. (June 25, 2013).

work you performed for your previous employer, it makes sense to put up an ethical wall to protect yourself from even the appearance of impropriety.

CONCLUSION

As the modern world continues to shift to an information-based economy, more companies of all stripes are relying on intellectual property laws to protect their valuable information assets. To the extent that companies rely on trade secrecy to protect these assets, they create tension in the employment relationship. The EEA increases this tension by making public money available to prosecute trade secret misappropriation and establishing criminal liability for those convicted. Fortunately, there remain ways for employers and employees to protect themselves and continue innovating in a global marketplace. Just look at Homaro Cantu: he is working to protect his intellectual property in the kitchen while also training the next generation of molecular gastronomists, several of whom have already gone on to start successful operations of their own.[125] Trade secrecy may be increasing, but as long as employers and employees alike are knowledgeable about the issues trade secrets create, there is no reason why it should arrest innovation.

[125] *See, e.g.*, D'Andre Cater, the creative force behind pop-up restaurant Feast & Imbibe (http://chicago.eater.com/archives/2013/01/08/feast-on-new-popups-from-former-moto-chef.php) and Mike Ryan, the mixologist at Sable Kitchen and Bar (http://www.starchefs.com/cook/chefs/bio/mike-ryan-0). Both studied under Homaro Cantu (Chef Carter as an intern and then as a sous chef, and Mike Ryan as a sous-chef and then as a mixologist). Both continue to utilize molecular gastronomy in their current positions.