2019

Snapshot of Trade Secret Developments

Elizabeth A. Rowe
University of Florida Levin College of Law, rowe@law.ufl.edu

SNAPSHOT OF TRADE SECRET DEVELOPMENTS

ELIZABETH A. ROWE*

TABLE OF CONTENTS

INTRODUCTION 47
I. CIVIL CASE REVIEW 50
A. What Is Generally Known & Readily Ascertainable? 52
B. Failure to State a Claim? 53
C. Identification & Pleading with Specificity 55
D. Reasonable Efforts 58
E. Independent Economic Value 59
F. Preliminary Injunctions 61
G. Misappropriation 62
H. Non-Competes and Other Agreements 66
I. Protective Orders and Requests to Seal 67
J. Damages 72
K. Permanent Injunctive Relief 76
L. DTSA Whistleblower Provision 78
II. CRIMINAL UPDATE 81
A. Convictions 83
1. Former DuPont Employee Pleads Guilty 83
2. Jury Convicts Electrical Engineer for Theft from Defense Contractor 83
3. Sinovel Convicted and Fined for Theft from AMSC 84
4. Former Chemours Employee Pleads Guilty 84

* Irving Cypen Professor of Law, Distinguished Teaching Scholar, University Term Professor, and Director, Program in Intellectual Property Law, University of Florida Levin College of Law. I express my appreciation to Victoria Cundiff and to participants at the 2018 American Intellectual Property Lawyers Association Annual Meeting for insights, comments, or conversations about the ideas expressed in earlier versions of this work. Thank you to Alexandra Beguiristain, Anisha Dutt, and Alexandra Graves for research assistance and to the University of Florida Levin College of Law for its research support.

5. Scientist Convicted for Theft of Engineered Rice 85
6. Developer Pleads Guilty and Sentenced to Five Years in Prison 85
7. Former Executive Convicted for Trade Secret Theft from Medical Company 86
8. Chicago Trader Convicted for Theft of His Employer's Trading Code 86
9. Engineer Pleads Guilty to Selling Secrets to Russian Spy 87
B. Indictments 87
1. Six Former and Current Fitbit Employees Indicted 87
2. Former Apple Employee Indicted 88
3. Man Arrested for Attempting to Steal Trade Secrets from Medrobotics Corp. 89
4. Man Indicted for Stealing Trade Secrets to Benefit Rival Firm in China 89
5. Russian Officers Charged for Hacking Yahoo Email Accounts 90
6. Chinese Hackers Charged for Intrusions Against Moody's, Siemens, and Trimble 90
CONCLUSION 91

INTRODUCTION

Trade secret law protects facts, ideas, inventions and information. A trade secret can be any information of value used in one's business that has been kept secret and provides an economic advantage over competitors.[1] Because companies invest millions of dollars in research, development, and other aspects of their business that provide their competitive edge,[2] they rely on the protections provided under trade secret law as an incentive to invest the resources to create trade secrets, and to share those secrets with employees.[3] Trade secret protection is attractive, relative to other kinds of intellectual property protection, in part because of the broad scope of information that is protectable and the relative ease with which a business can claim such protection.[4] Securing trade secret information is the most critical task for any putative trade secret holder because once a trade secret has been disclosed, even if inadvertently, it ceases to be a trade secret.[5]

Trade secrets are arguably more important now to companies than ever in our history. In fact, since the most recent revisions to our patent laws, many believe that trade secrets might be even more important than patents.[6] Accordingly, the theft of trade secrets or

---

1. *See* UNIF. TRADE SECRETS ACT § 1 (amended 1985), 14 U.L.A. 538 (2005); RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. LAW INST. 1939).

2. *See generally* JERRY COHEN & ALAN S. GUTTERMAN, TRADE SECRETS PROTECTION AND EXPLOITATION 12-13 (Bureau of Nat'l Affairs ed., 1998).

3. *See id.* at 5-13; *see also* PAUL GOLDSTEIN, COPYRIGHT, PATENT, TRADEMARK AND RELATED STATE DOCTRINES 152-53 (2d ed. 1981).

4. *See* Brooks W. Taylor, *You Can't Say That!: Enjoining Publication of Trade Secrets Despite the First Amendment*, 9 COMPUT. L. REV. & TECH. J. 393, 394-95 (2005) (discussing reasons why corporations rely on trade secret protection).

5. *See* Andrew Beckerman-Rodau, *The Choice Between Patent Protection and Trade Secret Protection*: *A Legal and Business Decision*, 84 J. PAT. & TRADEMARK OFF. SOC'Y 371, 376 n.53, 379 (2002). While the risk of loss is one that is inherent in choosing this form of protection, it does not necessarily suggest that a trade secret owner should have instead chosen patent protection. *See id.* at 379-81. One who chooses trade-secret protection over patent protection has not necessarily forgone a "better" form of protection, especially since there is a wide range of information that is eligible for trade-secret protection but not patent protection. *See, e.g.*, *id.*; *see also* JAMES POOLEY, TRADE SECRETS § 3.01[1] [a] at 3-4 (Charles Tait Graves 2007) (1997).

6. *See, e.g.*, David S. Almeling, *Seven Reasons Why Trade Secrets are Increasingly Important*, 27 BERKELEY TECH. L.J. 1091, 1104-06 (2012); Mark A. Lemley, *The Surprising*

trade secret misappropriation from company employees and from outsiders, such as competitors and foreign governments, is on the rise.[7]

The Uniform Trade Secrets Act (UTSA) codifies the basic principles of common law trade secret protection.[8] With Massachusetts's recent adoption (effective October 1, 2018),[9] a total of forty-nine states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have adopted the UTSA (with some variation).[10] The only state that has not yet adopted the UTSA in some form is New York.[11]

After over one hundred years of trade secrecy being the only area of intellectual property (IP) governed by state law, the most significant development to this area of law was the passage of the Defend Trade Secrets Act of 2016 (DTSA).[12] President Obama signed the DTSA, and it went into effect on May 11, 2016.[13] The DTSA is the first federal law in the United States to create a federal civil cause of action for trade secret misappropriation.[14] The DTSA largely mirrors the UTSA, with a nearly identical definition of "trade secret," an identical definition of "misappropriation," and other similarities.[15] Significantly, the DTSA does not preempt or displace state law (except, in some respects), meaning that the

---

Virtues of Treating Trade Secrets as IP Rights, 61 STAN. L. REV. 311, 330 (2008); Tom C.W. Lin, *Executive Trade Secrets*, 87 NOTRE DAME L. REV. 911, 943 (2012).

7. *See, e.g.*, Almeling, *supra* note 6, at 1099-100, 1105, 1110-12.

8. UNIF. TRADE SECRETS ACT § 1 (amended 1985), 14 U.L.A. 538 (2005).

9. Jacob W. Schneider & Taylor Han, *Exploring the Pre-Disocovery Trade Secret Identification Requirement in Massachusetts and Across the Country*, HOLLAND & KNIGHT: TRADE SECRETS BLOG (Nov. 20, 2018), https://www.hklaw.com/TradeSecretsBlog/Exploring-the-Pre-Discovery-Trade-Secret-Identification-Requirement-in-Massachusetts-and-Across-the-Country-11-20-2018/ [https://perma.cc/R7UM-AL9Z].

10. *See Legislative Fact Sheet—Trade Secrets Act*, UNIF. L. COMM'N, http://www.nccusl.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act [https://perma.cc/SFU2-BGHD].

11. *See id.* North Carolina is often counted among the states that have adopted the UTSA because it enacted a statute that is similar. However, because of certain modifications, the Uniform Law Commissioners does not recognize North Carolina as an official adoptee. *See Trade Secrets Law and the UTSA: 50 State and Federal Law Survey*, BECK REED RIDEN (Jan. 24, 2017), https://www.beckreedriden.com/trade-secrets-laws-and-the-utsa-a-50-state-and-federal-law-survey-chart/ [https://perma.cc/UPY5-4Z79].

12. Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376, 380-82, 384-85 (codified as amended at 18 U.S.C. §§ 1832-1836, 1838-1839 (Supp. IV 2016)).

13. *See* §§ 1832-1836, 1838-1839.

14. *See id.*

15. *Id.* § 1839.

United States now has two bodies of civil trade secret law developing in parallel: the DTSA and the UTSA.[16]

The DTSA's enactment means that trade secret owners may now bring a trade secret claim in state or federal court, a choice that was previously available only if they could invoke the diversity jurisdiction of the federal courts or join their state trade secret claim with another federal cause of action.[17] Since the DTSA is largely based upon the UTSA, and is likely to be interpreted in accordance with the UTSA; the existence of two separate trade secret laws is not likely to result in significant divergence of state and federal trade secret principles, for most of the country.

As we enter the second year of the DTSA, this Article presents a snapshot of developments to assess whether there appears to be any significant doctrinal changes afoot in trade secret litigation—including civil and/or criminal—during the past year. Professors David Levine and Christopher Seaman provided some empirical data and quantitative analysis of the case filings during the first year of litigation under the DTSA (from May 2016 to May 2017).[18] This Article complements their excellent work by taking a qualitative look at some of the substantive rulings from the following year. My assessment based on this limited sampling is that there does not appear to be any dramatic changes to the doctrinal development of the law to date.[19] Rather, courts continue to search for fairness as they struggle with problems common to trade secret litigation regarding, for instance, trade secret identification, misappropriation, and damages.[20]

Further contributing to the uniqueness of trade secret law is that, given the evolution of trade secrecy from its state-based, common law origins, it is probably more nuanced and inconsistent than its other federal-law-based IP siblings (patents, trademarks, and

16. *See id.* § 1838.

17. *See id.* § 1836.

18. *See* David S. Levine & Christopher B. Seaman, *The DTSA at One: An Empirical Study of the First Year of Litigation Under the Defend Trade Secrets Act*, 53 WAKE FOREST L. REV. 105, 123-151 (2018).

19. *See infra* Parts I, II; *see generally* SHARON K. SANDEEN & ELIZABETH A. ROWE, TRADE SECRET LAW: INCLUDING THE DEFEND TRADE SECRETS ACT OF 2016 IN A NUTSHELL (West Academic 2d ed., 2018).

20. *See infra* Parts I.C, I.G, I.J.

copyrights).[21] Trade secret law is highly factual.[22] Every state is different, and the trade secrecy law is based upon and supported by the public policy of the relevant states.[23] Nevertheless, the fundamental principles of trade secrecy have become relatively well grounded, so much so that the introduction of a federal law is unlikely to cause tremendous upheaval in its continuing doctrinal development.[24] Of course, it is far too soon to know what will happen in the years ahead, and there are specific provisions from the DTSA that will require judicial interpretation.[25]

This Article proceeds in four parts. Following this introduction, Part I highlights some noteworthy civil cases from select federal and state courts. The cases are organized topically to provide the reader with a quick overview of recent rulings in various categories, from stating a claim for trade secret misappropriation to discovery-related issues, including protective orders, as well as damages and injunctive relief. Furthermore, to the extent some of the cases have interpreted certain provisions of the DTSA, those cases are noted separately. In Part II, the Article includes updates on criminal convictions and indictments over the past year under the Economic Espionage Act. These "headlines" are intended to provide a flavor of the types of cases that are selected for criminal prosecution under federal law. Finally, the Article concludes that there does not appear to be any significant departures in the civil case law to date, and that the criminal cases pursued by federal prosecutors continue to reflect familiar patterns.

I. CIVIL CASE REVIEW

The majority of trade secret cases result from business relationships between the parties.[26] In particular, most trade secret cases

21. *See, e.g.*, Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, 101 VA. L. REV. 317, 322-23 (2015).

22. *See id.* at 363-64.

23. *See id.* at 353.

24. *See id.*; *see also* Levine & Seaman, *supra* note 18, at 119.

25. *See* Symposium, *Understanding the Defend Trade Secrets Act (DTSA): The Federalization of Trade Secrecy,* 50 LOYOLA L.A. L. REV. 331 (2017).

26. *See* Levine & Seaman, *supra* note 18, at 131-32, 134-35.

arise in the employment context.[27] Employers have the right to protect and preserve trade secrets, confidential, and proprietary information.[28] When an employer discloses trade secrets in confidence to an employee during the course of his or her employment, even without an enforceable restrictive covenant, the employer has a legitimate interest in protecting that information.[29] However, careful consideration must be given to protecting trade secrets in a way that does not unreasonably impinge on employees' and other users' rights.

In addition to the employer-employee cases, many trade secret cases involve actions between competitors.[30] One of the goals of trade secret law is "the maintenance of standards of commercial ethics."[31] Thus, while competition is a valued part of doing business, trade secret laws establish boundaries to ensure that this competition is not done unfairly.[32] It is just as unfair to hire the former employee of a competitor who will disclose the competitor's trade secrets, as it is to break into the competitor's locked safe to steal its secret formula.[33] Accordingly, courts must strike the appropriate balance between anti-competitive conduct and trade secret protection in deciding trade secret cases.

This Part provides an update on some of the civil trade secret cases that were decided in both federal and state courts this past year. Overall, it appears that most of these cases are still being decided under the UTSA, but some do include claims under both the UTSA and the DTSA.[34] Cases that provided specific interpretations of new provisions in the DTSA are noted at the end of the section.

---

27. *See id.* at 134-35.

28. *See, e.g.*, New England Canteen Serv., Inc. v. Ashley, 363 N.E.2d 526, 528 (Mass. 1977); D.C. Wiring, Inc. v. Lamontagne, No. 91-1722, 1993 WL 818562, at *1-2 (Mass. Super. Ct. Dec. 20, 1993); Stevens & Co. v. Stiles, 71 A. 802, 805 (R.I. 1909).

29. *See, e.g.*, *Stevens & Co.*, 71 A. at 805.

30. *See* Levine & Seaman, *supra* note 18, at 122-23, 123 n.91.

31. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481 (1974).

32. *See id.* at 481-82.

33. Elizabeth A. Rowe, *Trade Secret Litigation and Free Speech: Is It Time to Restrain the Plaintiffs?*, 50 B.C. L. REV. 1425, 1429-30 (2009).

34. Only five of the cases reviewed were based on DTSA claims. They are *Xoran Holdings L.L.C. v. Luick*, No. 16-13703, 2017 WL 4039178 (E.D. Mich. Sept. 13, 2017); *CPI Card Group, Inc. v. Dwyer*, 294 F. Supp. 3d 791 (D. Minn. 2018); *Broker Genius, Inc. v. Zalta*, 280 F. Supp. 3d 495 (S.D.N.Y. 2017); *Christian v. Lannett Co.*, No. CV 16-963, 2018 WL 1532849 (E.D. Pa. Mar. 29, 2018); and *Hawkins v. Fishbeck*, 301 F. Supp. 3d 650 (W.D. Va. 2017).

A. What Is Generally Known & Readily Ascertainable?

The definition of a trade secret under the UTSA and the DTSA specifically precludes protection for information that is "generally known" or "readily ascertainable."[35] The phrase "generally known" is not defined by the UTSA or the DTSA, but the commentary to the UTSA and applicable case law recognizes that the concept is not limited to information that is known by the public at large.[36] Information can be generally known and ineligible for trade secret protection "[i]f the principal persons who can obtain economic benefit from information are aware of it."[37] The "readily ascertainable" limitation focuses on how easily a trade secret could be discovered if anyone attempted to do so from a source other than the putative trade secret owner.[38] The focus is on whether the information is "knowable."[39]

HIP, Inc. v. Hormel Foods Corp. from the Eighth Circuit serves as a reminder that information disclosed in a patent application cannot be a trade secret.[40] Such information becomes public knowledge, and as such, it is excluded from coverage under the definition of "confidential" information for the purposes of the nondisclosure agreement at issue in the case.[41]

A plaintiff who claimed that its business strategy of marketing its products through QVC was a trade secret could not sustain its claim.[42] In *Yeiser Research & Dev. L.L.C. v. Teknor Apex Co.,* the court noted that a competitor could easily ascertain this information through public sources.[43] This included a business strategy regard-

35. *See* 18 U.S.C. § 1839 (Supp. IV 2016).

36. *See* UNIF. TRADE SECRETS ACT § 1 cmt. (amended 1985), 14 U.L.A. 538 (2005); *see also Broker Genius, Inc*., 280 F. Supp. at 513-14, 516-17.

37. UNIF. TRADE SECRETS ACT § 1 cmt.

38. *See id.*

39. *Id.* § 2 cmt.

40. 888 F.3d 334, 341 (8th Cir. 2018).

41. *See id.* at 341-42.

42. *See, e.g.*, Yeiser Research & Dev. L.L.C. v. Teknor Apex Co., 281 F. Supp. 3d. 1021, 1046 (S.D. Cal. 2017).

43. 281 F. Supp. 3d at 1046-49.

ing when and where plaintiff sold its products.[44] Accordingly, the plaintiff could not establish the existence of a trade secret.[45]

The Nevada Supreme Court in *MEI-GSR Holdings, L.L.C. v. Peppermill Casinos, Inc.*, was asked to determine whether, under the Nevada Uniform Trade Secrets Act,[46] a defendant is precluded from demonstrating that certain information was readily ascertainable if the defendant acquired the information through improper means.[47] Interpreting the statute, the court held that the determination of whether information was "readily ascertainable by proper means" was "not limited to the defendant's conduct."[48] Furthermore, the court noted:

> Although a defendant's acquisition of information by *proper means* is a relevant consideration in determining whether the information is a trade secret..., we hold that a defendant's acquisition of information by *improper means* does not preclude the defendant from demonstrating that the information is readily ascertainable by other persons.[49]

Thus, whether information is readily ascertainable or generally known is a threshold inquiry in establishing that the type of information at issue qualifies for trade secret protection or is protectable as a trade secret.[50]

B. Failure to State a Claim?

In order to establish a claim for trade secret misappropriation under the UTSA and the DTSA, a plaintiff has the burden of pleading and proving that: (1) plaintiff owns a trade secret; (2) one or more of plaintiff's trade secrets have been or are threatened to be misappropriated by the defendant; and (3) plaintiff is entitled to a remedy.[51] Because the available remedies are broad, the focus of trade

44. *See id.*
45. *See id.*
46. NEV. REV. STAT. ANN. § 600A.030 (West 2017).
47. 416 P.3d 249, 253 (Nev. 2018).
48. *Id.* at 254.
49. *Id.*
50. *See, e.g.*, *id.*
51. *See* Clorox Co. v. S.C. Johnson & Son, Inc., 627 F. Supp. 2d, 954, 968 (E.D. Wisc. 2009)

secret misappropriation cases is usually on the first and second requirements.[52] Generally, the determination whether specific information is a trade secret is a mixed question of law and fact.[53]

Tension Envelope Corporation v. JBM Envelope Company from the Eighth Circuit raises the interesting question of whether information created by a company's customers can be protectable information.[54] The plaintiff in this case alleged that it produced envelopes that complied with technical specifications generated by its customers, not by the plaintiff itself.[55] The Eighth Circuit held that because these customer requirements could have been acquired from the customers themselves, the plaintiff failed to state a claim for misappropriation of trade secrets.[56]

In *Krawiec v. Manly*, the North Carolina Supreme Court considered whether the plaintiff's description of its trade secret was sufficient to allege the existence of a trade secret under the North Carolina Trade Secrets Protection Act.[57] The plaintiff, a dance studio, described its trade secrets as "original ideas and concepts for dance productions, marketing strategies and tactics, as well as student, client and customer lists and their contact information."[58] The plaintiff provided no further details about these "ideas, concepts, strategies, and tactics" in order to put "defendants on notice as to the precise information allegedly misappropriated."[59] Furthermore, the court found that the complaint did not show that the plaintiff's customer lists were trade secret because it failed to allege that the list contained any information that would not be readily accessible to defendants.[60] The plaintiff therefore needed to provide additional information sufficient to put the defendants and the court

(listing the elements of a prima facie case for trade secret misappropriation under California's version of the UTSA).

52. *See infra* Parts I.D, I.G; *see also infra* note 128 and accompanying text.

53. *See, e.g.*, APAC Teleservices, Inc. v. McRae, 985 F. Supp. 852, 864 (N.D. Iowa 1997).

54. 876 F.3d 1112, 1122 (8th Cir. 2017).

55. *See id.* at 1115-16.

56. *See id.* at 1122-23.

57. 811 S.E. 2d 542 (N.C. 2018); *see also* N.C. GEN. STAT. ANN. § 66-153 (West 2017) (outlining an action for misappropriation under the North Carolina Trade Secrets Protection Act).

58. *Krawiec*, 811 S.E. 2d at 549.

59. *See id.*

60. *See id.*

on notice as to *which* "ideas, concepts, strategies, and tactics" were allegedly misappropriated.[61]

C. Identification & Pleading with Specificity

It is not until a trade secret holder is actually in litigation that the validity of its alleged trade secret rights are determined.[62] The first step in establishing the existence of a trade secret is to prove that the information in question was a trade secret before the defendant misappropriated it.[63] This means that the plaintiff must identify the trade secret (precisely each piece of information the plaintiff alleges is a trade secret) and show that it took reasonable efforts to preserve this information.[64] This often can be a challenge for most plaintiffs.[65]

The plaintiff has a duty to identify its trade secrets with specificity.[66] In most states, this requirement is imposed by case law and pleading rules, but in California it is a statutory requirement.[67] Similarly, the Wisconsin UTSA requires for injunctive relief "a description of each alleged trade secret in sufficient detail to inform the party to be enjoined or restrained of the nature of the complaint against that party."[68] One reason for the specificity requirement is to prevent a plaintiff from using trade secret litigation as a means to conduct competitive intelligence through the guise of discovery.[69]

---

61. *Id.*

62. *See* Rowe, *supra* note 33, at 1447.

63. *See id.*; *see also* Robert A. Kearney, *Why The Burden of Proving Causation Should Shift to the Defendant Under the New Federal Trade Secret Act*, 13 HASTINGS BUS. L.J. 1, 3-4 (2016).

> The standard utilized for this inquiry should be akin to the likelihood of success on the merits standard used in preliminary injunction cases. Most trade secret cases, particularly in the context of the problem presented here, will be decided at a preliminary injunction hearing. Thus, use of this standard should present no further difficulty, and may very well fold into the injunction test.

Rowe, *supra* note 33, at 1447 n.124.

64. *See* Rowe, *supra* note 33, at 1447.

65. *See id.*

66. *See* IDX Systems Corp. v. Epic Systems Corp., 285 F.3d 581, 583-84 (7th Cir. 2002).

67. *See* CAL. CIV. PROC. CODE § 2019.210 (West 2005).

68. WISC. STAT. ANN. § 134.90(3)(a) (West 2011).

69. *See* DeRubeis v. Witten Tech., Inc., 244 F.R.D. 676, 680 (N.D. Ga. 2007).

It also serves the due process purpose of letting defendants know the details of the claims against them.

The obligation that trade secrets be identified with particularity is not merely a pleading or evidentiary requirement; it is a very practical requirement. Unless the plaintiff can articulate its putative trade secrets in a very concrete way, there is no way to test whether the information meets the requirements for trade secrecy. This is often a challenge for trade secret owners who tend to claim trade secrecy for broad or vague categories of information. By doing so, they may undermine their ability to show that the information is not generally known and has independent economic value.[70]

The Eleventh Circuit in *EarthCam, Inc. v. OxBlue Corp.*, addressed whether conclusory allegations are sufficient to withstand a motion for summary judgment.[71] Even though the court ruled that "whether a particular type of information constitutes a trade secret is a question of fact," conclusory allegations without specific supporting facts are insufficient to resist summary judgment.[72] In this case, the district court had found that the rather general information contained in the defendant's emails at issue contained trade secrets.[73] An affidavit supporting the plaintiff's claim and declaring that certain information "was not publicly available" and that it gave the plaintiff "a competitive advantage" without fleshing out the details was not enough.[74] Another court reviewing confidential information disclosed in emails by a former employee, also found that "generalized assertions" would not be sufficient to meet the plaintiff's burden of proving that it had legitimate trade secrets.[75]

Similarly, in *RE/MAX, LLC v. Quicken Loans Inc.*, the court dismissed the defendant's counterclaim for trade secret misappropriation as conclusory, because it did not provide sufficient facts to support its argument.[76] For instance, the court reasoned that defendant simply states that:

---

70. *See, e.g.*, Blake v. Prof. Coin Grading Serv., 898 F. Supp. 2d 365, 379 (D. Mass. 2012).
71. 703 F. App'x 803, 810 (11th Cir. 2017).
72. *See id.*
73. *See id.* at 810-11.
74. *Id.* at 811.
75. *See* CPI Card Group, Inc. v. Dwyer, 294 F. Supp. 3d 791, 809 (D. Minn. 2018).
76. 295 F. Supp. 3d 1163, 1176 (D. Colo. 2018).

> [u]pon information and belief, [plaintiff] used and shared confidential information it obtained about [defendant's] confidential, proprietary, and trade secret processes and marketing strategies through the negotiation and implementation of the Agreement to develop, launch, and operate Motto Mortgage. While [defendant] alleges various reasons to suspect [plaintiff] was economically motivated to use [defendant's] confidential information for such a purpose, [defendant] does not allege any facts tending to show that it actually did use such information.[77]

Thus, the court pointed out that the defendant did not allege anything about plaintiff's operations that suggested it used defendant's confidential business information.[78] Indeed, the court noted that the only similarities that defendant alleges between its operations and plaintiff's were the "superficial similarity that [plaintiff] is in the same industry and the irrelevant claim that [plaintiff] 'copied [defendant's] slogan,' which is not confidential."[79] Finding that these allegations were insufficient to suggest a plausible inference that the defendant was harmed by the plaintiff's use of its confidential information, the court dismissed the counterclaim.[80]

In *Liberty Mutual Ins. Co. v. Gemma,* however, the defendants were unsuccessful in dismissing the complaint for lack of specificity.[81] Defendants argued that under the Pennsylvania Uniform Trade Secrets Act,[82] the complaint did not describe the alleged trade secrets with sufficient specificity, or explain how the defendants obtained the trade secrets, or used the trade secrets.[83] The court found that the plaintiff alleged that defendants "misappropriated various documents, including customer lists and other customer information."[84] Because misappropriation under the statute requires the "following elements: (1) the existence of a trade secret; (2) communication of the trade secret pursuant to a confidential relationship; (3) use of the trade secret, in violation of that confi-

77. *Id.* at 1173 (internal citations omitted).
78. *See id.*
79. *Id.*
80. *See id.*
81. 301 F. Supp. 3d 523, 541 (W.D. Pa. 2018).
82. 12 PA. STAT. AND CONS. STAT. ANN. § 5301 (West 2004).
83. *See Liberty Mutual Ins. Co.*, 301 F. Supp. at 540.
84. *Id.*

dence; and (4) harm to the plaintiff," the court deemed the complaint to be sufficient.[85]

D. Reasonable Efforts

"In almost every state, the reasonable efforts requirement is embedded in the threshold legal question of trade secret misappropriation analysis: whether the plaintiff owns a legally protectable trade secret."[86] Reasonable efforts require that in order to qualify for trade secret protection, the information must be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[87] The reasonable efforts requirement mandates that a trade secret holder "show more than mere intent to protect something as a trade secret; actual effort to keep the information secret is necessary."[88]

Whether a trade secret owner has utilized appropriate safeguards sufficient to meet the reasonable efforts requirement is a question of fact, based on the particular circumstances.[89] Thus, the decisions necessitate a balancing between using sufficient precautions to protect a company's secret on the one hand, while not imposing overly-burdensome precautions that would impair the functioning of its business on the other hand.[90]

In *CSS, Inc. v. Herrington,* a software provider brought an action against its former employee and competitor, alleging that the defendants misappropriated a number of trade secrets, including its source code.[91] In considering the extent of measures taken to guard the secrecy of the source code, the court found that the source code had been installed on the county's servers for about twenty years,

85. *Id.*

86. Elizabeth A. Rowe, *RATs, TRAPs, and Trade Secrets*, 57 B.C. L. REV. 381, 409 (2006).

87. *See id.* (quoting UNIF. TRADE SECRETS ACT § 1(4)(ii) (amended 1985), 14 U.L.A. 538 (2005)).

88. *Id.*; *see also* Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 901 (Minn. 1983) ("[E]ven under the common law, more than an 'intention' was required—the plaintiff was required to show that it had manifested that intention by making some effort to keep the information secret.").

89. *See* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 176-77 (7th Cir. 1991).

90. *See id.* at 178-80.

91. 306 F. Supp. 3d 857, 864, 877 (S.D.W. Va. 2018).

it was not encrypted, password-protected, or labeled confidential; nor did the plaintiff require any confidentiality agreements when it provided the source code to its clients (the various counties).[92] Accordingly, the court concluded that the source code was not the subject of reasonable efforts to maintain its secrecy and therefore could not be a trade secret.[93]

The Southern District of NewYork in *Broker Genius, Inc. v. Zalta*, (applying the DTSA) similarly found that the plaintiff had not taken reasonable efforts to protect its software.[94] The company regularly disclosed its alleged trade secrets to its customers without requiring them to sign confidentiality agreements.[95] It gave "unfettered access" to the software, as well as extensive training, user manuals, and videos that explained how the software works and its functionalities.[96] In light of these findings, the plaintiff was unable to show that it took reasonable measures to protect the secrecy of the information.[97]

E. Independent Economic Value

The independent economic value requirement of trade secrecy is an often overlooked and misapplied part of the trade secrecy analysis. Technically, the "value" that is required is not any value viewed in the abstract, but a particular kind of value. The plaintiff in a trade secret misappropriation case has the burden of pleading and proving that its putative trade secret: (1) "derives"; (2) "independent"; (3) "economic value, actual or potential"; (4) "from not being generally known or readily ascertainable by" (that is, from being secret); (5) "other persons who can obtain economic value from its disclosure or use."[98]

The specifics of the economic value requirement are often given only brief attention by courts and litigants. Frequently, courts

92. *See id.* at 877-78.
93. *See id.* at 878-79.
94. 280 F. Supp. 3d 495, 517-18 (S.D.N.Y. 2017).
95. *See id.*
96. *See id.* at 520.
97. *See id.* at 521-22.
98. UNIF. TRADE SECRETS ACT § 1(4)(i) (amended 1985), 14 U.L.A. 538 (2005); *see also* 18 U.S.C. § 1839 (Supp. IV 2016).

assume that the alleged trade secrets must have the requisite economic value, otherwise the plaintiff would not have initiated litigation.[99] Plaintiffs sometimes discount or obscure the requirement in order to make it easier for them to prove their prima facie case.

Cy Wakeman, Inc. v. Nicole Price Consulting, L.L.C., addressed independent economic value as it relates to secrecy.[100] Here, the plaintiff alleged that the customer relationships between it and certain clients were confidential.[101] The court, interpreting Nebraska's UTSA, noted, however, that even if those relationships were sufficiently secret, it was unclear how they provided independent economic value to others.[102] According to the court, secrecy alone does not equal economic value.[103] The plaintiff argued that the value created by the secrecy of the plaintiff's client lists is the business those clients generate, and that business would be lost if the plaintiff was unable to maintain their privacy.[104] "But that is just value to [the plaintiff], and is not *independent value.* [Plaintiff] has identified no one else who could obtain an economic advantage from knowing who [plaintiff's] confidential clients are."[105] Thus, the court reasoned that there was no evidence that a competitor with knowledge of the plaintiff's client relationships could reap economic value just from knowing them.[106]

The Ohio Supreme Court in *In re Review of Alternative Energy Rider Contained in Tariffs of Ohio Edison Co.*, in assessing whether protective orders were properly granted, engaged in an analysis of independent economic value.[107] The relevant party in this case, a utility company, had entered into confidentiality agreements with

99. *See, e.g.*, MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 521 (9th Cir. 1993) (holding that plaintiff's customer database had potential economic value because it would allow competitors to direct efforts to potential customers already using the plaintiff's services); Editions Play Bac, S.A. v. Western Pub. Co., No. 92 Civ. 3653 (JSM), 1993 WL 541219, at *7 (S.D.N.Y. Dec. 28, 1993) (holding that the plaintiff's alleged trade secret had economic value because the defendant and another company considered licensing the rights to the secret).

100. 284 F. Supp. 3d 985, 995-96 (D. Neb. 2018).

101. *See id.* at 995.

102. *See id.* at 995-96.

103. *See id.*

104. *See id.* at 996.

105. *Id.*

106. *See id.*

107. 106 N.E.3d 1, 9-10 (Ohio 2018).

its suppliers to prevent the disclosure of certain supplier and pricing information submitted during a competitive bid process.[108] The Public Utilities Commission granted the protective orders, but the Environmental Law and Policy Center and the Office of the Ohio Consumers Council challenged the protective orders and sought disclosure of the records.[109] They argued that the information was not entitled to trade secret protection because, among other things, it did not meet the independent economic value requirement.[110] They further argued that the Public Utilities Commission did not explain how the sealed information, in light of its age and changes in market conditions that have transpired over time, has retained its economic value in today's market.[111] The Commission, on the other hand, asserted that "if [the] trade secret information was public, it could discourage REC suppliers' confidence in the market and impede the function of the REC market."[112] The court concluded that "[w]hile trade secrets may continue to be protected if the information retained some measure of value," the Commission had failed to cite to specific evidence to explain its protective order.[113]

F. Preliminary Injunctions

The basic principles of injunctive relief that were developed at common law continue to be applied under the UTSA and DTSA. Generally, before a court grants a preliminary injunction, the plaintiff must establish: (1) a likelihood of success on the merits; (2) a substantial threat that the plaintiff will suffer irreparable injury if the injunction is denied; (3) that the balance of hardships favors the moving party; and (4) that the injunction will not disserve the public interest.[114]

In *Mercer Health & Benefits L.L.C. v. DiGregorio,* the Southern District of New York granted a preliminary injunction enforcing

108. *See id.* at 8.
109. *See id.* at 7-8.
110. *See id.* at 9-10.
111. *See id.* at 8.
112. *Id.* at 10.
113. *Id.*
114. *See* Hull Mun. Lighting Plant v. Mass. Mun. Wholesale Elec. Co., 506 N.E.2d 140, 141-44 (Mass. 1987); Town of Brookline v. Goldstein, 447 N.E.2d 641, 644 (Mass. 1983).

nonsolicitation agreements and confidentiality agreements signed by the individual defendants relying on affirmative conduct by the defendants.[115] In granting the injunction, the court relied on the following evidence:

> [T]he Individual Defendants met with [defendant's] representatives repeatedly over a period of months while still employed [by plaintiff], and emailed confidential [plaintiff] documents to their personal email accounts during the same period; orchestrated simultaneous resignations from [plaintiff]; sent [plaintiff's] clients targeted announcements of their move to [plaintiff's competitor]; sought and held meetings with several [plaintiff] clients after joining [the competitor]; and persuaded at least one [plaintiff] client ... to move its business to [the defendant].[116]

On the other hand, in ruling on a motion for preliminary injunction, the court in *Cerro Fabricated Products L.L.C. v. Solanick* granted an injunction even without such affirmative acts.[117] The court reasoned that even though the defendant, absent evidence that he took any documents with him, was likely to possess a significant amount of confidential information in his memory, he would still be capable of "compartmentalizing and confidential information" to avoid using it with his new employer.[118] Nevertheless, because defendants could not present any evidence of steps taken, or that they intended to take, in order to prevent the disclosure of the plaintiff's trade secrets, there was a sufficient likelihood of disclosure of the trade secret.[119] Accordingly, a preliminary injunction was warranted.[120]

G. Misappropriation

To establish a claim for trade secret misappropriation under the UTSA and the DTSA, a plaintiff has the burden of pleading and proving that: (1) plaintiff owns a trade secret (or otherwise has standing to sue); (2) that one or more of plaintiff's trade secrets have

115. 307 F. Supp. 3d 326, 330-31, 346-48, 350-55 (S.D.N.Y. 2018).
116. *Id.* at 347.
117. 300 F. Supp. 3d 632, 636 (M.D. Pa. 2018).
118. *See id.* at 653.
119. *See id.*
120. *See id.*

been or are threatened to be misappropriated by the defendant; and (3) that plaintiff is entitled to a remedy.[121] Because the available remedies are broad, the focus of trade secret misappropriation cases is usually on the first and second requirements.[122]

An aspect of trade secret law that makes it different from patent, copyright, and trademark law is its knowledge requirement.[123] The definition of misappropriation under all formulations of trade secret law requires that the defendant "knows or has reason to know" of the alleged trade secrets and the wrongful acts of misappropriation.[124] In contrast, patent, copyright, and trademark laws are like strict liability torts in that a defendant may be held liable for patent, copyright, and trademark infringement even if he did not know or have reason to know of the existence of plaintiff's intellectual property rights.[125]

How a plaintiff attempts to prove the requisite knowledge in trade secret cases depends upon the facts of each case, but direct evidence of actual knowledge is not required.[126] Knowledge or reason to know can be inferred from circumstantial evidence.[127] Of course, where a defendant directly engages in the wrongful acts that constitute misappropriation, the requisite knowledge of such acts is relatively easy to prove.[128] The key in such cases is to prove that the

---

121. *See* Clorox Co. v. S.C. Johnson & Son, Inc., 627 F. Supp. 2d, 954, 968 (E.D. Wis. 2009) (listing the elements of a prima facie case for trade secret misappropriation under California's version of the UTSA).

122. *See id.* at 968-69.

123. *See* Deepa Varadarajan, *Trade Secret Fair Use*, 83 FORDHAM L. REV. 1401, 1404 (2014) ("To be liable for trade secret misappropriation, however, one must 'missappropriate' the protected information....This requirement makes trade secret law unique and reflects how its origins differ from those of patent and copyrights laws.").

124. *See* 18 U.S.C. § 1839 (Supp IV. 2012); UNIF. TRADE SECRETS ACT § 1(2)(i) (amended 1985), 14 U.L.A. 538 (2005)); RESTATEMENT (THIRD) OF UNFAIR COMPETITION, § 40 (AM. LAW INST. 1995).

125. *See, e.g.*, Roger D. Blair, *Strict Liability and Its Alternatives in Patent Law*, 17 BERKELY TECH. L.J. 799, 800-01 (2002); N. Coast. Indus. v. Jason Maxwell, Inc., 972 F.2d 1031, 1033 (9th Cir. 1992) ("To establish copyright infringement, the holder of the copyright must prove both valid ownership of the copyright and that there was infringement of that copyright by the alleged infringer.").

126. *See, e.g.*, *Clorox Co.*, 627 F. Supp. 2d at 968-69.

127. *See, e.g.*, *id.*

128. *See, e.g.*, Beard Res., Inc. v. Kates, 8 A.3d 573, 599 (Del. Ch. 2010).

defendant knew or had reason to know that the information he acquired, disclosed, or used was trade secret information.[129]

Circumstantial evidence can be presented and weighed to determine the likelihood that the defendant knew of the misappropriation, and a defendant cannot shield himself by "studious ignorance of pertinent 'warning' facts."[130] A defendant's constructive notice that the information was a trade secret is sufficient.[131]

In *Experian Information Solutions, Inc. v. Nationwide Marketing Services Inc.,* the Ninth Circuit addressed whether the defendant knew or had reason to know that it acquired and used the trade secret that was obtained through improper means.[132] In reviewing the District Court's grant of summary judgment on the issue, the court noted that "improper acquisition and improper use of protected works [were] independent bases" for trade secret misappropriation.[133] As an evidentiary matter, the defendant had "paid less than 1% of the market rate for a one-time license" in order to obtain ownership of the data at issue.[134] The court found that this indicated sufficient knowledge and that the low price paid by the defendant supported plaintiff's contention that the defendant had constructive knowledge that the data in question had been obtained through improper means.[135] This evidence was sufficient to withstand summary judgment.[136]

In *GE Betz, Inc. v. Moffitt-Johnston,* the Fifth Circuit noted that although circumstantial evidence is often relied upon to prove trade secret misappropriation, in this case, a mere inference was not sufficient.[137] Evidence of the defendant downloading company files, lying about working for a competitor, and suspicions of soliciting competitors at industry social events were too speculative to raise an issue of material fact.[138] The plaintiff also argued that it was

129. *See id.*
130. *See* Curtiss-Wright Corp. v. Edel-Brown Tool & Die Co., 407 N.E.2d 319, 324 (Mass. 1980).
131. *See id.*
132. 893 F.3d 1176, 1188-89 (9th Cir. 2018).
133. *See id.* at 1189.
134. *See id.*
135. *See id.*
136. *See id.* 1189-90.
137. 885 F.3d 318, 326 (5th Cir. 2018).
138. *See id.* at 322-24.

reasonable to infer from the defendant's business plan that the defendant used the plaintiff's cost structure to acquire market share.[139] Nevertheless, the court found that "attempting to acquire market share, even in part through lower margins, is a natural goal for a business in its infancy, and it would be unreasonable to infer from this broadly stated objective that [the defendant] planned to use [the plaintiff's] trade secrets."[140]

C.D.S., Inc. v. Zetler is a reminder of the importance of clear contractual terms among business partners relating to ownership of and access to proprietary information.[141] The factual background of this case spans almost a "dozen parties in the fashion technology business and conduct that occurred on at least three continents."[142] In interpreting the terms of a distributorship agreement between the parties, the court found that, among other things, the agreement did not grant the defendants any rights to the source code at issue, and as such, they could be liable for misappropriation.[143] On the other hand, with respect to a customer list that was used by the defendants in their sales efforts, the court found that the distribution agreement did not prohibit such use by the defendants and could not be misappropriation.[144] The court also enforced the "binding forum selection clause in favor of the French courts," that was provided for in the agreement.[145]

How much of an advantage must a trade secret provide to a defendant in order to constitute misappropriation? In *Iconics, Inc. v. Massaro*, the court held that the advantage does not need to be substantial.[146] "If a misappropriator uses a trade secret even to some small benefit, but fails to implement it in a way that maximizes its value, it has still misappropriated the secret."[147] The court concluded that a reasonable jury could find that the defendant's implementation was merely inferior to plaintiff's, but that any advantage,

139. *See id.* at 326.
140. *Id.*
141. 298 F. Supp. 3d 727, 753 (S.D.N.Y. 2018).
142. *Id.* at 734.
143. *See id.* at 759.
144. *See id.* at 761.
145. *Id.*
146. 266 F. Supp. 3d 449, 460 (D. Mass. 2017).
147. *Id.*

whether small or ephemeral, would still be enough to constitute trade secret misappropriation.[148]

In *Elenza, Inc. v. Alcon Labs. Holding Corp.*, the Supreme Court of Delaware evaluated whether it was sufficient that the defendant had "motive and opportunity" to misappropriate a trade secret.[149] In this case, the plaintiff attempted to show that the defendant had the "motive and opportunity" to misappropriate its trade secrets based on the defendant's collaboration with other third parties and that the defendant's designs were "sufficiently similar" to plaintiff's based on the defendant's patent application.[150] The court found, however, that this was insufficient to give rise to an inference of misappropriation.[151] It was not enough to show that they "could have" used the plaintiff's designs. Instead, they needed to point to evidence in the patent application and elsewhere that the defendant actually did.[152]

H. Non-Competes and Other Agreements

When employers wish to restrict employees from working for competitors, they should enter into written restrictive covenants (often labeled "Noncompetition Agreements" or "Noncompete Agreements") that are designed to protect their legitimate business interests.[153] By entering into a noncompetition agreement, the employee usually agrees that for a specified period of time, after the end of his or her employment, he or she will not work for any company that is a competitor of the employer.[154]

Although it is too early after the adoption of the DTSA to have definitive guidance on how federal courts will interpret section 1836(b)(3)(A)(i) of the DTSA, when cases allege violations of both the DTSA and the state UTSA, many district courts seem to be granting injunctions restraining employees and other defendants

148. *See id.*
149. 183 A.3d 717, 725 (Del. 2018).
150. *Id.*
151. *See id.* at 725-26.
152. *Id.* at 726.
153. *See, e.g.*, Hawkins v. Fishbeck, 301 F. Supp. 3d 650, 659-60 (W.D. Va. 2017).
154. *See id.*

from competing with the trade secret owner in much the same way that they would have done under the UTSA.[155]

Applying Virginia law, one district court held a noncompetition agreement unenforceable in *Hawkins v. Fishbeck*.[156] The agreement provided that:

> During the term of this Agreement and for a period of twelve (12) months thereafter, Executive shall not, *in any capacity whatsoever, own, participate in the ownership of, manager* [sic]*, operate, exercise any control over, render services to, derive income from or engage in any of the foregoing for any business*, firm, corporation, limited liability company, partnership, or other entity which operates a business competitive with Employer.[157]

The court found the agreement overbroad for two reasons. First, it went too far in restricting the roles that the employee could perform for a competitor by prohibiting work "in any capacity whatsoever."[158] Second, the agreement contained no geographical limitation period, and could restrict the employee from working in an area where he never performed any functions for the former employer.[159]

I. Protective Orders and Requests to Seal

Because defendants in trade secret cases have the right to discover the identification and details of the plaintiff's putative trade

---

155. *See, e.g.*, T&S Brass & Bronze Works, Inc. v. Slanina, No. 6:16-03687-MGL, 2017 WL 1734362, at *13, *17 (D.S.C. May 4, 2017) (preliminary injunction granted despite an objection that it would prevent the defendant from entering into an employment relationship); First W. Capital Mgmt. Co. v. Malamed, No. 16-cv-1961-WJM-MJW, 2016 WL 8358549, at *6, *13 (D. Colo. Sept. 30, 2016) (preliminary injunction granted in a case where the moving party appears to have carefully limited the requested injunction to avoid any problems under the DTSA, but where the injunction nonetheless prohibited the defendant from providing any services to plaintiff's existing and prospective clients); Panera, L.L.C. v. Nettles, No. 4:16-cv-1181-JAR, 2016 WL 4124114, at *2, *6 (E.D. Mo. Aug. 3, 2016) (temporary restraining order issued to enforce a confidentiality and noncompete agreement and to protect plaintiff's trade secrets).

156. *See Hawkins*, 301 F. Supp. 3d at 660-61.

157. *Id.* at 660 (emphasis added).

158. *See id.*

159. *See id.*

secrets,[160] there is an obvious risk that whatever trade secrets exist will be revealed during the course of the litigation. As a practical matter, when presenting its case at trial, a plaintiff will have to explain what its trade secrets are as part of its prima facie case.[161] To facilitate the discovery process, most courts will issue protective orders that are designed to protect plaintiff's information during the pendency of litigation.[162] Indeed, both the UTSA and the DTSA require courts to do so.[163] Section 5 of the UTSA states:

> "[A] court shall preserve the secrecy of an alleged trade secret by reasonable means, which may include granting protective orders in connection with discovery proceedings, holding in-camera hearings, sealing the records of the action, and ordering any person involved in the litigation not to disclose an alleged trade secret without prior court approval."[164]

Generally, it is easier to protect trade secrets during the pleading and discovery phases of litigation than it is during trial.[165] This is because of the strong public policy favoring open and publicly accessible judicial proceedings.[166]

Accordingly, courts will sometimes restrict public access to court proceedings in order to protect trade secrets, once the appropriate showings have been made regarding trade secrecy status and the lack of other reasonable alternatives to protect the information.[167] Courts will also consider whether the parties to the litigation would suffer competitive harm if their information were to be made pub-

---

160. *See* Brian D. Range, *Identification of Trade Secret Claims in Litigation: Solutions for a Ubiquitous Dispute*, 5 NW. J. TECH. & INTELL. PROP. 68, 69, 71, 73 (2006).

161. *See* Rowe, *supra* note 33, at 1447.

162. *See, e.g.*, Apple, Inc. v. Samsung Elecs. Co., 727 F.3d 1214, 1223-24, 1229 (Fed. Cir. 2013).

163. *See* 18 U.S.C. § 1835 (Supp. IV 2016); UNIF. TRADE SECRETS ACT § 5 (amended 1985), 14 U.L.A. 538 (2005).

164. UNIF. TRADE SECRETS ACT § 5.

165. *See, e.g.*, Citizens First Nat'l Bank of Princeton v. Cincinnati Ins., 178 F.3d 943, 944-45 (7th Cir. 1999).

166. *See id.* at 945 ("[T]he public at large pays for the courts and therefore has an interest in what goes on at all stages of a judicial proceeding. That interest does not always trump the property and privacy interests of the litigants, but it can be overridden only if the latter interests predominate in the particular case." (citations omitted)).

167. *See* Publicker Indus., Inc. v. Cohen, 733 F.2d 1059, 1071 (3d. Cir. 1984).

lic.[168] If so, the court could order that certain information be sealed from the public and third parties.[169]

Nevro Corp. v. Boston Scientific Corp. serves as a reminder that federal litigation is a public process, and that attorneys who file frivolous sealing requests could be sanctioned.[170] The Northern District of California made it clear that potential embarrassment to a company is not sufficient grounds for sealing documents that should otherwise be available to the public.[171] After denying a request to seal documents, the court warned both parties that frivolous requests would result in sanctions.[172] The defendants again filed another frivolous request, and the court issued an order to show cause why the lawyers should not be sanctioned.[173] The Ninth Circuit's decision in *Kamakana v. City and County of Honolulu*, which held that there must be "compelling reasons" to seal documents, guided the court.[174] The *Nevro* court noted that:

> At the hearing on the order to show cause, there was discussion of the fact that attorneys—particularly attorneys for corporate clients—are under great pressure to file motions to seal information that their clients would prefer to keep secret, even if there is no legitimate basis to keep the information secret. This is no doubt a significant issue for corporate lawyers, but the answer is not to file frivolous sealing requests. The answer is to firmly explain to their clients that litigation is a public process, and that the public has the right to know what the litigation is about, subject only to very limited exceptions.[175]

The court concluded that there was no justification for the sealing request, and the request was objectively frivolous in violation of Rule 11 of the Federal Rules of Civil Procedure.[176]

---

168. *See id.* at 1071-72.

169. *See, e.g.*, Apple, Inc. v. Samsung Elecs. Co., 727 F.3d 1214, 1224-25 (Fed. Cir. 2013) (sealing product-specific financial information from public disclosure).

170. 312 F. Supp. 3d 804, 804-05 (N.D. Cal. 2018).

171. *See id.* at 805.

172. *See id.* at 804-05.

173. *See id.* at 805.

174. 447 F.3d 1172, 1178-79 (9th Cir. 2006).

175. *Nevro Corp.*, 312 F. Supp. 3d at 805.

176. *See id.*

Lyft, Inc. v. City of Seattle, addressed the Washington state Public Records Act and whether it was appropriate to grant an injunction preventing disclosure of records regarding car rides provided in each zip code within the city.[177] Following an evidentiary hearing, the King County Superior Court had found that these records, were trade secrets pursuant to the UTSA.[178] The issue before the Washington Supreme Court was whether records containing trade secrets are "categorically excluded from public disclosure under the [Public Records Act]."[179] Lyft had agreed to "submit quarterly standardized reports to the City that included the total number of rides, the percentage of rides completed in each zip code, pick-up and drop-off zip codes, the percentage of rides requested but unfulfilled, collision data, and the number of requested rides for accessible vehicles."[180] In response to Lyft's concerns regarding the confidentiality of some of the information, the Seattle City Council enacted an ordinance that provided that if a public records request were made for documents that had been designated as confidential, the City would inform the owner of the records request prior to disclosure.[181]

Accordingly, when a resident of Texas submitted a public records request to the City, Lyft sought an injunction to prevent disclosure of the requested reports.[182] The court reasoned that no provision of the Public Records Act exempted trade secrets from disclosure, and therefore any exemption would need to be pursuant to another statute (in this case, the UTSA).[183] Yet, according to the court, the "UTSA contains no specific exemption of trade secrets from public disclosure laws."[184] The court began its UTSA analysis by determining whether the data at issue qualified for trade secret protection under the UTSA.[185] It concluded that the zip code reports constituted "a compilation of information consistent with the UTSA."[186] However, the court reasoned that the UTSA authorized an injunc-

177. 418 P.3d 102, 104 (Wash. 2018).
178. *See id.* at 106.
179. *Id.* at 110; *see generally* WASH. REV. CODE § 42.56 (2018).
180. *Lyft, Inc.*, 418 P.3d at 105.
181. SEATTLE, WASH., MUNICIPAL CODE § 6.310.540(D) (2014).
182. *Lyft, Inc.*, 418 P.3d at 106.
183. *See id.* at 106-07.
184. *Id.* at 108.
185. *See id.* at 108-09.
186. *Id.* at 109.

tion only when there had been an actual or threatened misappropriation of trade secrets.[187] Therefore, "the City owed no legal duty to maintain the confidentiality of the public records," and did not have authority to promise confidentiality in any manner that was inconsistent with the Public Records Act.[188] The case was therefore remanded back to the trial court for a fact-based determination of whether injunctive relief was warranted under the "more stringent in junction standards" of the Public Records Act, rather than the "lesser UTSA standard" involving misappropriation between private parties.[189]

The Alabama Supreme Court in *Ex parte Industrial Warehouse Services., Inc.*, reviewed whether a party was entitled to a protective order in response to a discovery request.[190] A trucking company that was sued as a result of injuries that occurred in an auto accident involving a truck driven by one of its employees was seeking a protective order.[191] As part of the personal injury litigation, the estates of the parties who died from injuries incurred as a result of the accident sent discovery requests to the trucking company.[192] In response, the trucking company sought a protective order to prohibit dissemination "of its bills of lading and its operations and safety manuals."[193] The circuit court denied the motion for protective order, finding that the company failed to establish good cause under Rule 26(c) of the Alabama Rules of Civil Procedure.[194] The company argued, however, that the information sought contained confidential and trade secret information.[195] The Alabama Supreme Court found that the safety manuals were not trade secrets because the company was required by federal law to report some of the information from these sources to the Federal Motor Carrier Safety Administration.[196] Furthermore, the information in the operations and safety manuals contained information based on regulations that were applicable to

187. *See id.* at 110.
188. *Id.* at 111.
189. *Id.* at 114.
190. Nos. 1170013 & 1170087, 2018 WL 1126576, at *1 (Ala. Mar. 2, 2018).
191. *See id.* at *1-2.
192. *See id.*
193. *Id.*
194. *Id.* at *2.
195. *See id.*
196. *See id.* at *4-5.

the entire trucking industry, and were readily ascertainable from public sources.[197] As to the information contained in the bills of lading, the court ruled that that information satisfied the definition of a trade secret.[198]

J. Damages

The UTSA provides that "actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss" can all be included as a measure for trade secret damages.[199] Accordingly, a trade secret plaintiff may recover both actual losses and the "unjust benefit" caused by the defendant.[200] While compensatory damages can be combined with injunctive relief, the UTSA cautions that "injunctive relief ordinarily will preclude a monetary award for a period in which the injunction is effective."[201]

When there is evidence that the defendant used or disclosed the trade secret, thus causing actual harm, an award of compensatory damages is justified.[202] The measure of damages in these circumstances is "likely to be the actual and potential value of the trade secrets" to the plaintiff's without the disclosure.[203] A number of different measures are available to establish compensatory damages. These include lost profits, erosion of market share, out-of-pocket expenses, and advantage to the defendant.[204]

*Title Source Inc. v. HouseCanary Inc.,*from a Texas state court, was one of the largest jury verdicts of 2018, with a total of over $706 million in compensatory and punitive damages.[205] This case de-

197. *See id.* at *5.
198. *See id.*
199. UNIF. TRADE SECRETS ACT § 3(a) (amended 1985), 14 U.L.A. 538 (2005).
200. *Id.* § 3 cmt.
201. *Id.*
202. *See id.*
203. SANDEEN & ROWE, *supra* note 19, at 258-59.
204. *See, e.g.*, Univ. Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518, 536 (5th Cir. 1974); Synergeering Group, L.L.C. v. Jonatzke (*In re* Jonatzke), 478 B.R. 846, 861 (Bankr. E.D. Mich. 2012).
205. Eric J. Fues & Maximilienne Giannelli, *Title Source Inc. v. HouseCanary Inc.*, FINNEGAN (May 29, 2018), https://www.finnegan.com/en/insights/title-source-inc.-v.-housecanary-inc.html [https://perma.cc/FQ4J-AUG4].

serves attention not only because of the high damages award, but because the damages went to the defendant on its counterclaim against the plaintiff.[206] The plaintiff, Title Source, filed suit against HouseCanary, "alleging nonperformance under the license agreement and breach of the [nondisclosure agreement]."[207] HouseCanary then counterclaimed for misappropriation of trade secrets, breach of contract, and fraud.[208] The defendant's tremendous success on its counterclaim against the plaintiff serves as a note of caution to plaintiffs to be careful what they start, especially when filing actions potentially involving trade secrets.[209]

On a motion for summary judgment, the court in *Repat, Inc. v. IndieWhip, L.L.C.*, entered summary judgment in favor of the defendants because the plaintiff was unable to show proof of damages.[210] The plaintiff argued that there was evidence of threatened use by virtue of the fact that the defendant had an incentive to exploit what it was able to learn from the plaintiff's trade secrets.[211] The court noted that while this argument might have been persuasive at the beginning of the litigation, two years had passed and plaintiff's business continued to thrive.[212] "If [plaintiff] can find no material evidence (direct or indirect) today that [defendant] has made use of its proprietary marketing secrets in the interval, the court is hard pressed to understand the nature of the 'imminent and irreparable harm' that it is being asked to enjoin."[213] Therefore, plaintiff could not "show any dispute of material fact over actual damages, present or future, [and] failed to carry its burden of proof" on the trade secrets claim.[214]

The issue of disgorgement and whether it could be decided by a jury arose in two cases. First, the Ninth Circuit briefly addressed disgorgement in *GSI Technology, Inc. v. United Memories, Inc.*, noting that profit disgorgement was an equitable remedy to be de-

206. *See id.*
207. *Id.*
208. *See id.*
209. *See, e.g.*, Elizabeth A. Rowe, *Unpacking Trade Secret Damages,* 55 HOUS. L. REV. 155, 195-96 (2017) (providing empirical data on the size of trade secret damage awards).
210. 281 F. Supp. 3d 221, 223-24 (D. Mass. 2017).
211. *See id.* at 231.
212. *See id.* at 231-32.
213. *Id.* at 232.
214. *Id.*

cided by the trial court and not by the jury.[215] Second, in *Texas Advanced Optoelectronic Solutions, Inc. v. Renesas Electronics America, Inc.*, the Federal Circuit engaged in some historical analysis to determine whether disgorgement of profits was available at law in 1791 for trade secret misappropriation; the Federal Circuit concluded that it was not.[216] The jury in this case awarded disgorgement profits to the plaintiff based on what the plaintiff's expert had proposed.[217] The evidence supporting this claim for monetary relief did not limit the covered sales to a "head-start period."[218] The court found that the absence of any limitation to a "head-start" could have had significant consequences.[219] If the disgorgement claim could not have been brought in the law courts in 1791, then no right to a jury trial would attach to that claim, and the plaintiff would not have the constitutional right for a jury to decide the disgorgement question.[220]

The court in *In re Mandel* concluded that compensatory damages in a trade secret case could be established with a flexible approach, and a plaintiff should be given latitude to prove damages once misappropriation has been shown.[221] That being said, however, the plaintiffs were required to produce enough credible evidence to show "the extent of the damages as a matter of just and reasonable inference, even if the result be only approximate."[222] The dissent cautioned, however, that "[o]ur flexible and creative standard is not a license for pie-in-the-sky damages; rather, damages must be grounded both in theory and fact."[223]

The New York Court of Appeals in *E.J. Brooks Co. v. Cambridge Security Seals*, held that a plaintiff cannot recover compensatory damages measured by the cost a defendant avoided due to its unlawful activity.[224] Reviewing a question from the United States Court of Appeals for the Second Circuit, as to whether "under New York law, a plaintiff asserting claims of misappropriation of a trade

215. 721 F. App'x 591, 594 (9th Cir. 2017).
216. 888 F.3d 1322, 1338 (Fed. Cir. 2018).
217. *See id.* at 1336.
218. *See id.*
219. *See id.* at 1336-37.
220. *See id.* at 1337.
221. 720 F. App'x 186, 190-91 (5th Cir. 2018).
222. *Id.* at 191 (internal quotations omitted).
223. *Id.* at 199.
224. No. 26, 2018 WL 2048724, at *1 (N.Y. May 3, 2018).

secret, unfair competition, and unjust enrichment can recover damages that are measured by the costs the defendant avoided due to its unlawful activity," the court answered the question in the negative.[225] In the underlying case, "the jury returned a verdict finding [the defendant] liable for trade secret misappropriation, unfair competition and unjust enrichment," and assessing $1.3 million in compensatory damages on each claim (totaling $3.9 million).[226] The defendant moved for judgment as a matter of law, arguing that "avoided costs was an improper measure of damages."[227] The trial court denied the motion, holding that avoided costs could either measure the defendant's gains or the plaintiff's losses.[228] The Court of Appeals of New York agreed with the defendant "that damages in trade secret actions must be measured by the losses incurred by the plaintiff," and that they may not be based on the infringers avoided development costs.[229] Damages tied to the defendant's gains rather than the plaintiff's losses were not a permissible measure of damages.[230] Recognizing that loss was broadly defined in trade secret cases, the court noted, however, that it was "neither automatically nor presumptively the case that costs avoided by the *defendant* will be an adequate approximation of the *plaintiff's* investment losses, any more than it can be presumed that the defendant's sales would approximate those of the plaintiff."[231] The court further noted that the plaintiff's actual costs were a better measure than the defendant's, as the plaintiff's actual development costs had been incurred and were a known quantity, while the defendants avoided costs were merely hypothetical.[232]

In *Eagle Oil & Gas Co. v. Shale Exploration, L.L.C.*, the Texas Court of Appeals addressed whether the economic loss rule barred recovery for misappropriation of trade secrets.[233] A jury found the defendant liable for trade secret misappropriation, and awarded the

225. *Id.*
226. *Id.* at *2.
227. *See id.*
228. *See id.*
229. *Id.* at *6.
230. *See id.*
231. *Id.*
232. *See id.*
233. No. 01-15-00888-CV, 2018 WL 1870081, at *1 (Tex. App. Apr. 19, 2018).

plaintiff "$14,300,000 in lost profits and $4,500,000 in exemplary damages".[234] The defendant argued that the economic loss rule barred the plaintiff's misappropriation claim because it was based on a confidentiality agreement and was thus recognizable only as a contract claim.[235] In this case, the plaintiff sought to recover lost profits under both breach of a confidentiality agreement and misappropriation of trade secrets.[236] The court noted that "the breach of a confidential relationship may be a breach of contract and result in contractual liability, but a breach of confidence also gives rise to an independent claim for misappropriation of trade secrets, regardless of contractual liability."[237] Accordingly, the court held that "if the evidence is sufficient to show the elements of the tort of misappropriation of trade secrets" independent from a contractual obligation, the economic loss rule does not bar the misappropriation claim.[238]

K. Permanent Injunctive Relief

In the absence of provable monetary damages (and often in addition thereto), the principal remedy for trade secret misappropriation is likely to be permanent injunctive relief.[239] According to the DTSA, such relief may be granted to enjoin actual or threatened trade secret misappropriation "on such terms as the court deems reasonable," including with respect to the length of the injunction.[240]

The USTA limits the length of permanent injunctive relief in trade secret cases to the period of time during which the subject trade secrets remain secret.[241] Presumably, the same limitation will apply under the DTSA, but it remains to be seen whether, and to what extent, federal courts rely upon state rules and decisions on this issue, and what federal courts will determine to be *reasonable*.

---

234. *Id.*
235. *See id.* at *5.
236. *See id.* at *17.
237. *Id.* at *5.
238. *Id.* at *6.
239. *See* Rowe, *supra* note 209, at 195.
240. 18 U.S.C. § 1836(b)(3)(A)(i) (Supp. IV 2016); *see also* UNIF. TRADE SECRETS ACT § 2(a) (amended 1985), 14 U.L.A. 538 (2005).
241. *See* UNIF. TRADE SECRETS ACT § 2(a).

Once a plaintiff in a trade secret case proves misappropriation, particularly in a UTSA jurisdiction or in a DTSA case, the plaintiff may argue that they are "automatically" entitled to injunctive relief because such relief is a statutorily prescribed remedy.[242] Whether this argument will work depends upon the law of the applicable state and how the federal courts interpret and apply the DTSA.[243] There is nothing in the language of the UTSA or DTSA that specifically requires courts to apply "principles of equity," as was the case with patent law in the *eBay* case.[244] However, consistent with the common law origins of trade secret law, the grant of permanent injunctive relief is ordinarily subject to principles of equity.[245] Applicable law and the facts of each case will dictate the equitable factors on which courts focus when deciding whether to grant permanent injunctive relief.[246]

The Federal Circuit in *CardiAQ Valve Technologies, Inc. v. Neovasc Inc.*, upheld the denial of a permanent injunction because the requested injunction would have been duplicative of the monetary relief received by the plaintiff.[247] The district court below also had considered the uncertainty in the market, the impact the injunction would have had on the defendant, and "the public's interest in having access to a potentially life-saving technology."[248]

In *TMRJ Holdings, Inc. v. Inhance Technologies., L.L.C.*, a court of appeals in Texas reviewed whether a trial court erred in awarding both damages and permanent injunctive relief.[249] The defendant against whom the injunction was entered argued that the two remedies were duplicative, and that awarding both violated the one-satisfaction rule.[250] The jury awarded "$4 million in reasonable royalty-damages and $10,500 in lost profits" to the plaintiff.[251] The

242. *See, e.g.*, E.I. DuPont de Nemours & Co. v. Kolon Indus., No. 3:09cv58, 2012 WL 4490547, at *5, *12 (E.D. Va. Aug. 30, 2012).

243. *See id.*

244. *See* eBay, Inc. v. MercExchange, L.L.C., 547 U.S. 388, 391-94 (2006).

245. *See, e.g.*, *E.I. DuPont de Nemours & Co.*, 2012 WL 4490547, at *4-5, *7, *12, *16, *22-23.

246. *See id.*

247. 708 F. App'x 654, 667-69 (Fed. Cir. 2017).

248. *Id.* at 667.

249. 540 S.W.3d 202, 204-05 (Tex. App. 2018).

250. *See id.* at 205.

251. *Id.* at 204.

trial court entered judgment on those damages and also granted a permanent injunction.[252] In reviewing whether the reasonable royalty damages overlapped with the permanent injunction that prohibited future use of the trade secrets, the court reasoned that the reasonable royalty damages did not make the plaintiff whole.[253] That is because the reasonable royalty damages awarded by the jury were not based on actual future use of the trade secret, but were meant to compensate purely for the misappropriation of the technology.[254] The present value of the technology was "based in part on potential for future use, regardless of whether that use came to fruition."[255] In addition, the court found that the evidence at trial showed that the plaintiff never intended the trade secrets to be commercially available; thus, they were never intended to be licensed or otherwise used by a third-party.[256] Accordingly, a reasonable royalty would not fully compensate for misappropriation of a trade secret that the owner seeks to preserve for its exclusive use and would not sell.[257] The court further found that although the royalty determination conceivably included future revenue that licensing the trade secrets might have produced, "the trial court reasonably could have concluded that this measure of actual damages did not fully compensate [the plaintiff] absent an injunction because [the plaintiff] never intended that the trade secrets be available in the marketplace."[258]

L. DTSA Whistleblower Provision

The newest defense to a trade secret misappropriation claim is provided by a provision of the DTSA which applies to *all* potential criminal and civil trade secret liability, state or federal.[259] This defense is known as the "whistleblower immunity" or "whistleblower

252. *See id.* at 204-05.
253. *See id.* at 210.
254. *See id.*
255. *Id.*
256. *See id.*
257. *See id.*
258. *Id.* at 211.
259. 18 U.S.C. § 1833(b) (Supp. IV 2016).

defense," and it specifies that certain *disclosures* of trade secrets cannot serve as the basis of a trade secret claim.[260]

There are three parts to the DTSA's whistleblower provision. Subsections (b)(1)(A) and (b)(1)(B) set forth the applicable immunity, stating that it applies in two situations.[261] First, when a "disclosure" of trade secrets is made "in confidence" to specified government officials, and "solely for the purpose of reporting or investigating a suspected violation of law."[262] Second, when the disclosure "is made in a complaint or other document filed" in a legal proceeding, and is filed "under seal," presumably in accordance with the rules of the applicable court.[263]

Subsection (b)(2) concerns the use of trade secrets in retaliation lawsuits, allowing trade secrets to be disclosed by the plaintiff to his or her attorney, provided that the trade secrets are kept confidential and, if filed with the court, are filed under seal.[264]

Subsection (b)(3) does not immunize disclosures, but may affect the availability of remedies in a trade secret misappropriation case because it requires employers to give a specified notice to their employees.[265] If they fail to do so, "the employer may not be awarded exemplary damages or attorney fees under subparagraph (C) or (D) of section 1836(b)(3) in an action against an employee to whom notice was not provided."[266] Significantly, "employee" is defined broadly for purposes of the whistleblower immunity to include "any individual performing work as a contractor or consultant for an employer."[267]

The first year of the DTSA had few reported decisions involving the whistleblower immunity, but one case where it arose sparked concerns about how the provision is being interpreted and applied.[268] In *Unum Group. v. Loftus*, the court considered a Motion to Dismiss based upon the whistleblower immunity and refused to

---

260. *See id.*; *see also* Peter S. Menell, *Misconstruing Whistleblower Immunity Under the Defend Trade Secrets Act*, 1 NEV. L.J.F. 92, 93-94 (2017).

261. *See* 18 U.S.C. § 1833(b)(1)(A)-(B).

262. *Id.* § 1833(b)(1)(A)(i)-(ii).

263. *Id.* § 1833(b)(1)(B).

264. *Id.* § 1833(b)(2)(A).

265. *Id.* § 1833(b)(3)(A)-(D).

266. *Id.* § 1833(b)(3)(C).

267. *Id.* § 1833 (b)(4).

268. *See* Menell, *supra* note 260, at 94-97.

grant it, ruling that application of the immunity required findings of fact that could not be determined on a Motion to Dismiss.[269] This sparked concern by the author of the DTSA provision that the immunity is being treated like an affirmative defense that a defendant must plead and prove, rather than as an immunity that can be raised in a Motion to Dismiss.[270]

The whistleblower provision was subsequently applied in *Christian v. Lannett Co.*[271] The Eastern District of Pennsylvania dismissed the defendant's federal counterclaims for trade secret misappropriation against the plaintiff.[272] A former employee sued the defendant pharmaceutical company for discrimination, and the company counterclaimed, alleging that the former employee had transferred 22,000 pages of company documents to her attorney and had retained company trade secrets after her employment was terminated.[273] However, the court found that those documents fell within the immunized disclosure parameters defined by the DTSA:

> Plaintiff's alleged disclosure was made to Plaintiff's counsel pursuant to a discovery Order of this Court, within the context of a lawsuit regarding violations of Title VII, the ADA, and the FMLA. Therefore, said disclosure to counsel cannot be used to allege a continuing misappropriation of the documents acquired before the DTSA enactment date.[274]

The DTSA requires employers to provide notice of its whistleblower immunity provisions.[275] Failure to do so prevents recovery of attorney's fees or exemplary damages.[276] In *Xoran Holdings L.L.C. v. Luick*, the Eastern District of Pennsylvania, again interpreting the DTSA, applied the whistleblower immunity provision to bar the plaintiff from recovering attorney's fees or exemplary damages on

269. 220 F. Supp. 3d 143, 146 (D. Mass. 2016).

270. *See* Peter S. Menell, *Misconstruing Whistleblower Immunity Under the Defend Trade Secrets Act*, THE CLS. BLUE SKY BLOG (Jan. 3, 2017), http://clsbluesky.law.columbia.edu/2017/01/03/misconstruing-whistleblower-immunity-under-the-defend-trade-secrets-act [https://perma.cc/3S3P-GR7L].

271. No. CV-16-963, 2018 WL 1532849 (E.D. Pa. Mar. 29, 2018).

272. *See id.* at *1.

273. *See id.* at *1-2.

274. *Id.* at *4.

275. *See* 18 U.S.C. § 1833(b)(3)(A) (Supp. IV 2016).

276. *Id.* § 1833(b)(3)(C).

its DTSA claim because it had not provided notice of the whistleblower immunity provision in its employment agreement or anywhere else.[277]

II. CRIMINAL UPDATE

The Economic Espionage Act (EEA) is the federal statute criminalizing trade secret misappropriation and espionage.[278] The EEA gives federal authorities, including the US Department of Justice and local federal prosecutors, "the power to investigate and prosecute individuals or companies who engage in criminal trade secret misappropriation."[279] Considering "the indictments that have been brought under the EEA, the vast majority of prosecutions involve employees, former employees, and other company 'insiders.'"[280] However, acts of corporate espionage by outsiders are also covered by the EEA.[281]

The EEA contains two main sections that address specifically theft of trade secrets to benefit a foreign government (section 1831), and more generally, all other theft of trade secrets (section 1832).[282] Section 1832 is the more widely utilized section, and it prohibits intentionally or knowingly "convert[ing] a trade secret that is related to a product or service used in or intended for use in interstate or foreign commerce."[283] It is worth noting that a defendant can be prosecuted under the EEA even if no trade secrets were actually stolen.[284] That is because both section 1831 and 1832 "make an attempt to steal trade secrets and a conspiracy to steal trade secrets a crime."[285]

The EEA also has extraterritorial reach and can be applied even where conduct does not occur on U.S. soil.[286] Section 1837 extends

277. No. 16-13703, 2017 WL 4039178, at *7 (E.D. Mich. Sept. 13, 2017).

278. Foreign and Economic Espionage Penalty Enhancement Act of 2012, Pub. L. No. 112-269, 126 Stat. 2442 (codified as amended at 18 U.S.C. § 1831 (2012)).

279. Rowe, *supra* note 86, at 387; *see also* 18 U.S.C. § 1831.

280. Rowe, *supra* note 86, at 387.

281. *Id.*

282. *See* 18 U.S.C. §§ 1831, 1832.

283. *Id.* § 1832(a).

284. *See* Rowe, *supra* note 86, at 388.

285. *Id.*; *see also* 18 U.S.C. §§ 1831(a)(4)-(5), 1832 (a)(4)-(5).

286. *See* 18 U.S.C. § 1837; *see also* Rowe, *supra* note 86, at 394.

jurisdiction if (a) the defendant is a U.S. citizen or corporation, or (b) any "act in furtherance of the offense was committed in the United States."[287] In practice, this provision has not been widely used by prosecutors due to the accompanying challenges of enforcement and service in foreign countries.[288]

The penalties under the EEA include both fines and prison sentences.[289] Violations under section 1831 may result in fines of up to $5 million for individuals, and up to $10 million or three times the value of the trade secrets for organizations.[290] The maximum term of imprisonment is fifteen years.[291] The DTSA increased the financial penalties for organizations from a maximum of $5 million to the greater of $5 million or three times the value of the trade secrets.[292] For individuals, the prison term is ten years.[293]

Overall, the number of prosecutions under the EEA have been relatively low since its enactment in 1996.[294] The past year has produced a steady pace of activity relating to federal criminal trade secret offenses.[295] Headlines from a number of convictions and indictments from the past year are highlighted below.[296] It is worth observing that these cases of espionage often involve well-known companies, high-level employees,[297] and competitors seeking to acquire technology.[298]

287. 18 U.S.C. § 1837.

288. *See* Rowe, *supra* note 86, at 394.

289. *See* 18 U.S.C. § 1831(a)-(b).

290. *Id.*

291. *Id.* § 1831(a).

292. *See* 18 U.S.C. § 1832(b) (Supp. IV 2016).

293. *Id.* § 1831(a) (2012).

294. THE NATIONAL BUREAU OF ASIAN RESEARCH, THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY, THE IP COMMISSION REPORT 43 (May 2013), http://www.ipcommission.org/report/IP_Commission_Report_ 052213.pdf [https://perma.cc/QG42-YUMX].

295. *See infra* Parts II.A, II.B.

296. *See infra* Parts II.A, II.B.

297. In an upcoming article I will explore this phenomenon of scientists, engineers, and executives as criminals under the EEA.

298. *See infra* Part II.A, II.B.

A. Convictions

1. Former DuPont Employee Pleads Guilty

Josh Harry Isler admitted that while employed with DuPont, he accepted employment with a competitor of DuPont in the ethanol fuel enzyme business.[299] While still employed with DuPont, and after accepting his new employment, Isler downloaded proprietary information and trade secrets belonging to DuPont, and many of the files related to DuPont's customers, who were also potential customers of his new employer.[300]

2. Jury Convicts Electrical Engineer for Theft from Defense Contractor

On July 9, 2018, a jury in Hartford, Connecticut found Jared Dylan Sparks, an electrical engineer who worked for a defense contractor (LBI, Inc.), guilty of trade secret theft.[301] LBI "designed and built unmanned underwater vehicles" for the Navy.[302] Sparks left LBI to work for Charles River Analytics.[303] Before leaving, Sparks uploaded thousands of LBL files to his Dropbox account, which included accounting and engineering files, as well as photos related to designs and renderings used to make the unmanned underwater vehicles.[304]

---

299. *See* Press Release, U.S. Dep't of Justice, Former DuPont Employee Pleads Guilty to Stealing Trade Secrets and Lying to the FBI (July 11, 2018), https://www.justice.gov/usao-ndia/pr/former-dupont-employee-pleads-guilty-stealing-trade-secrets-and-lying-fbi [http://perma.cc/ 3JZ9-YF9Y].

300. *See id.*

301. *See* Press Release, U.S. Dep't of Justice, Electrical Engineer Found Guilty for Intending to Convert Trade Secrets from Defense Contractor (July 10, 2018), https://www.justice.gov/opa/pr/electrical-engineer-found-guilty-intending-convert-trade-secrets-defense-contractor [http://perma.cc/JWD4-336X].

302. *Id.*

303. *See id.*

304. *See id.*

3. Sinovel Convicted and Fined for Theft from AMSC

A jury in Madison, Wisconsin convicted Sinovel Wind Group of conspiracy to commit trade secret theft from AMSC.[305] "Sinovel stole proprietary wind turbine technology from AMSC" to produce its own turbines.[306] The "[c]ourt found that AMSC's losses from the theft exceeded $550 million."[307] Sinovel received the statutory maximum fine of $1.5 million and one year probation.[308] The company was also ordered to pay restitution of about $57 million.[309]

4. Former Chemours Employee Pleads Guilty

On June 8, 2018, Jerry Jindong Xu, a Canadian citizen, pled guilty to conspiracy to steal trade secrets related to sodium cyanide from The Chemours Company.[310] Chemours was formed in 2015 from DuPont's chemicals business, and the company "performs the research and development for sodium cyanide products."[311] Xu previously worked for DuPont in China.[312] He admitted to, among other things, misleading his colleagues in order to accumulate pricing information, using personal email accounts to transfer confidential information, using an "encrypted Chinese-based messaging service to communicate with his co-conspirators," and receiving information from a "Chinese investor who indicated that it is common practice in China to steal technology from others."[313]

305. *See* Press Release, U.S. Dep't of Justice, Court Imposes Maximum Fine on Sinovel Wind Group for Theft of Trade Secrets (July 6, 2018), https://www.justice.gov/opa/pr/court-imposes-maximum-fine-sinovel-wind-group-theft-trade-secrets [http://perma.cc/V68C-RK5R].

306. *Id.*

307. *Id.*

308. *See id.*

309. *See id.*

310. *See* Press Release, U.S. Dep't of Justice, Former Chemours Employee Pleads Guilty to Theft of Trade Secrets Conspiracy in Bid to Lure Chinese Investors into Sodium Cyanide Market (June 12, 2018), https://www.justice.gov/usao-de/pr/former-chemours-employee-pleads-guilty-theft-trade-secrets-conspiracy-bid-lure-chinese [http://perma.cc/2MNT-ZC2S].

311. *Id.*

312. *See id.*

313. *Id.*

5. Scientist Convicted for Theft of Engineered Rice

Weiqiang Zhang was convicted in February 2017 for acquiring, without authorization, genetically programmed rice seeds which are used in the therapeutic and medical fields.[314] These seeds have various applications in health research, and Ventria, the defendant's former employer, spent millions of dollars finding cost-effective methods to extract proteins from the rice seeds.[315] Zhang provided the seeds to representatives of a Chinese crop institute when they visited him at his home in Manhattan, Kansas.[316] He was sentenced to 121 months in prison.[317]

6. Developer Pleads Guilty and Sentenced to Five Years in Prison

Xu Jiaqiang pled guilty to stealing proprietary source code from his former employer to benefit the National Health and Family Planning Commission of the People's Republic of China.[318] The defendant worked as a developer for the company and had access to the underlying source code.[319] At various times, the defendant communicated with two undercover officers who posed as a financial investor and a project manager, respectively.[320] He also uploaded proprietary source code to a server set up by the FBI.[321] He was sentenced to five years in prison.[322]

---

314. *See* Press Release, U.S. Dep't of Justice, Chinese Scientist Sentenced to Prison in Theft of Engineered Rice (Apr. 4, 2018), https://www.justice.gov/opa/pr/chinese-scientist-sentenced-prison-theft-engineered-rice [http://perma.cc/6RLS-JFJZ].

315. *See id.*

316. *See id.*

317. *See id.*

318. *See* Press Release, U.S. Dep't of Justice, Chinese National Sentenced for Economic Espionage and Theft of a Trade Secret from U.S. Company (Jan. 18, 2018), https://www. justice.gov/opa/pr/chinese-national-sentenced-economic-espionage-and-theft-trade-secret-us-company [http://perma.cc/8G57-LDAT].

319. *See id.*

320. *See id.*

321. *See id.*

322. *See id.*

7. Former Executive Convicted for Trade Secret Theft from Medical Company

Christopher Barry, former Vice President of Research and Development for Lutonix, Inc., pled guilty to theft of trade secrets for the benefit of his new employer, a startup medical device company.[323] The defendant had been "responsible for all research and development, quality assurance, and manufacturing" for his former employer.[324] He stole trade secret files in order to use the proprietary information in connection with his new employment and to transfer those files to his new employer.[325] He was sentenced to twelve months and one day in prison, three years supervised release, and is required to pay $533,842 in restitution.[326]

8. Chicago Trader Convicted for Theft of His Employer's Trading Code

David Newman pled guilty to theft of trade secrets for downloading and stealing "all of the proprietary computer code and trading software belonging to his employer," WH Trading LLC.[327] He apparently downloaded over 400,000 files to multiple USB thumb drives and then resigned from the company to establish his own trading firm.[328] He intended to use the stolen trade secrets to compete with his former employer.[329] Proprietary codes are used for "pricing futures and options contracts, executing trades on various exchanges, analyzing the risk of trades, and interpreting exchange

323. *See* Press Release, U.S. Dep't of Justice, Former Lutonix Executive Sentenced to a Year and a Day in Prison for Stealing Trade Secrets (Aug. 17, 2017), https://www.justice.gov/usao-mn/pr/former-lutonix-executive-sentenced-year-and-day-prison-stealing-trade-secrets [http://perma.cc/G3X4-RTBF].

324. *Id.*

325. *See id.*

326. *Id.*

327. Press Release, U.S. Dep't of Justice, Chicago Trader Sentenced to a Year in Federal Prison for Stealing Proprietary Trading Secrets from His Employer (June 5, 2017), https://www.justice.gov/usao-ndil/pr/chicago-trader-sentenced-year-federal-prison-stealing-proprietary-trading-secrets-his [https://perma.cc/GVY3-BMKM].

328. *See id.*

329. *See id.*

market data."[330] He was sentenced to one year and one day in prison and fined $100,000.[331]

9. Engineer Pleads Guilty to Selling Secrets to Russian Spy

Gregory Allen Justice pled guilty to "selling sensitive satellite information to a person he believed to be an agent of a Russian intelligence service."[332] Justice was an engineer who worked for a defense contractor on military and commercial satellite programs.[333] After stealing the proprietary trade secrets from his employer, Justice provided them to an undercover FBI agent who he believed was a Russian agent.[334] He received thousands of dollars in cash payments in exchange for the proprietary trade secrets.[335]

B. Indictments

1. Six Former and Current Fitbit Employees Indicted

On June 14, 2018, six former and current Fitbit employees were indicted in the Northern District of California for alleged federal trade secret offenses.[336] The individuals are accused of either stealing market research regarding fitness tracker opportunities from Jawbone, or stealing internal studies—including a comparison study of consumer behavior in which consumers wore both Jawbone and Fitbit devices.[337] The employees were charged with felony "posses-

330. *Id.*

331. *See id.*

332. Press Release, U.S. Dep't of Justice, Defense Contractor Employee Pleads Guilty to Selling Satellite Secrets to Undercover Agent Posing as Russian Spy (May 22, 2017), https://www.justice.gov/opa/pr/defense-contractor-employee-pleads-guilty-selling-satellite-secrets-undercover-agent-posing-0 [https://perma.cc/AQ5J-BXTT].

333. *See id.*

334. *See id.*

335. *See id.*

336. *See* Press Release, U.S. Dep't of Justice, Six Former and Current Fitbit Employees Indicted for Possessing Multiple Trade Secrets Stolen from Jawbone (June 14, 2018), https://www.justice.gov/usao-ndca/pr/six-former-and-current-fitbit-employees-indicted-possessing-multiple-trade-secrets [https://perma.cc/AE2R-BC48].

337. *See id.*

sion of stolen trade secrets, in violation of 18 U.S.C. § 1832(a)(3)," for which the maximum sentence is 10 years in prison.[338]

This indictment is particularly interesting because in 2015, Jawbone sued Fitbit, including these same individuals, "for 'systematically plundering' trade secrets, including over 300,000 confidential files."[339] After a nine-day trial, the International Trade Commission (ITC) ruled in favor of Fitbit and the individuals.[340] The administrative law judge determined on the merits that "no Jawbone trade secrets were misappropriated or used in any Fitbit product."[341] Nevertheless, U.S. federal prosecutors decided to move forward with a criminal prosecution.[342] The indictment states that the defendants "received and possessed one or more of the trade secrets for the economic benefit of someone other than Jawbone ... [and] each defendant was aware following his or her departure from Jawbone that the trade secrets were stolen and that they were being possessed without authorization."[343] This criminal case is worth following to see how it unfolds in light of the findings in the ITC proceeding.

2. Former Apple Employee Indicted

On July 12, 2018, a grand jury in San Jose indicted Xiaolang Zhang for allegedly taking "a confidential 25-page document containing detailed schematic drawings of a circuit board designed to be used ... in an autonomous vehicle."[344] Zhang told Apple that he was resigning from his job to return to China to be closer to his mother, but they subsequently learned that he was going to work for

338. *Id.*

339. Shannon Liao, *Feds Charged Six Current and Former Fitbit Employees for Stealing Trade Secrets From Jawbone*, THE VERGE (June 15, 2018), https://www.theverge.com/circuitbreaker/2018/6/15/17467820/fitbit-employees-charged-stolen-jawbone-trade-secrets-jawbone [https://perma.cc/SPB2-YTNY].

340. *See id.*

341. *Id.*

342. *See* U.S. Dep't of Justice, Six Former and Current Fitbit Employees Indicted for Possessing Multiple Trade Secrets Stolen from Jawbone, *supra* note 336.

343. *See id.*

344. Press Release, U.S. Dep't of Justice, Former Apple Employee Indicted on Theft of Trade Secrets (July 16, 2018), https://www.justice.gov/usao-ndca/pr/former-apple-employee-indicted-theft-trade-secrets [https://perma.cc/T6PS-QTFW].

a Chinese company "focused on electric automobiles and autonomous vehicle technology."[345] After the company discovered that Zhang had allegedly downloaded information from project databases containing trade secrets, Federal agents intercepted and arrested him at the San Jose International Airport.[346]

3. Man Arrested for Attempting to Steal Trade Secrets from Medrobotics Corp.

Dong Liu, a dual citizen of China and Canada, was arrested and charged with attempting to steal trade secrets from Medrobotics Corporation, headquartered in Raynham, Massachusetts.[347] Medrobotics manufactures a robot-assisted device used by surgeons to access "hard-to-reach places in the human body for minimally invasive surgery."[348] He was arrested after being caught by the CEO of Medrobotics sitting in a conference room at the company with three open laptop computers.[349] He was not authorized to be on the premises and he gave conflicting explanations for why he had entered the building.[350]

4. Man Indicted for Stealing Trade Secrets to Benefit Rival Firm in China

Robert O'Rourke had worked for a Woodstock-based manufacturer of cast-iron products since 1984.[351] In 2015, O'Rourke allegedly began discussions with a Chinese company to take a similar position as vice president with the Chinese company.[352] According to the

345. *Id.*

346. *See id.*

347. *See* Press Release, U.S. Dep't of Justice, Dual Canadian/Chinese Citizen Arrested for Attempting to Steal Trade Secrets and Computer Information (Aug. 31, 2017), https://www.justice.gov/usao-ma/pr/dual-canadianchinese-citizen-arrested-attempting-steal-trade-secrets-and-computer [https://perma.cc/9386-6ENA].

348. *Id.*

349. *See id.*

350. *See id.*

351. Press Release, U.S. Dep't of Justice, Businessman Indicted for Allegedly Stealing Employer's Trade Secrets While Planning for New Job with Rival Firm in China (July 20, 2017), https://www.justice.gov/usao-ndil/pr/businessman-indicted-allegedly-stealing-employer-s-trade-secrets-while-planning-new-job [https://perma.cc/WM44-7RVF].

352. *See id.*

indictment, O'Rourke allegedly took the proprietary information from the Woodstock company and intended to catch a flight from Chicago to China.[353] He was arrested at the O'Hare International Airport by federal authorities.[354]

5. Russian Officers Charged for Hacking Yahoo Email Accounts

Four defendants, including two offices of the Russian Federal Security Service (FSB), were indicted by a grand jury in the Northern District of California in March 2017.[355] They allegedly used "unauthorized access to Yahoo's systems to steal information from about at least 500 million Yahoo accounts" and then used the stolen information to access other accounts at Google and other webmail providers.[356] Among the accounts accessed were those of Russian journalists, as well as U.S. and Russian government officials.[357] Private-sector employees of financial, transportation, and other companies were also targeted.[358]

6. Chinese Hackers Charged for Intrusions Against Moody's, Siemens, and Trimble

Three Chinese nationals were indicted for computer hacking and theft of trade secrets in November 2017.[359] They allegedly conspired to hack into private corporate servers to steal confidential business information.[360] They did so by exploiting employees' computers and conducting "spearphish" email campaigns to deploy "malicious code"

353. *See id.*

354. *See id.*

355. *See* Press Release, U.S. Dep't of Justice, U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts (March 15, 2017), https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions [https://perma.cc/F2TZ-DGPK].

356. *Id.*

357. *See id.*

358. *See id.*

359. *See* Press Release, U.S. Dep't of Justice, U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage (Nov. 27, 2017), https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations [https://perma.cc/WSH5-5SG7].

360. *See id.*

into the companies' computer networks.[361] The victim companies were Moody's Analytics, Siemens AG, and Trimble, Inc.[362] The hackers worked for the China-based Internet security firm Guangzhou Bo Yu Information Technology Company Limited.[363]

CONCLUSION

We are in the second year following enactment of the federal DTSA, which governs trade secret misappropriation concurrently with the state-based UTSA.[364] This Article highlighted some noteworthy cases from select federal and state courts during the past year, arranged topically to follow the life cycle of a trade secret case from filing to damages.[365] It is evident that the majority of the cases are still being decided under the UTSA, and that there does not appear to be any significant doctrinal departures in the case law so far.[366] This Article also provided headline updates from the past year on criminal convictions and indictments under the Economic Espionage Act.[367] These cases continue to reflect cloak-and-dagger patterns that involve well-known companies, high-level employees (often foreign citizens), and competitors seeking to acquire technology.[368]

361. *Id.*
362. *Id.*
363. *Id.*
364. *See supra* note 17 and accompanying text.
365. *See supra* Part I.
366. *See supra* Part I.
367. *See supra* Part II.
368. *See supra* Part II.