Minnesota Journal of Law, Science & Technology

Volume 19 | Issue 2 Article 3

6-2018

Out of Thin Air: Trade Secrets, Cybersecurity, and the Wrongful Acquisition Tort

Sharon Sandeen
Mitchell Hamline School of Law

Out of Thin Air: Trade Secrets, Cybersecurity, and the Wrongful Acquisition Tort+

Sharon K. Sandeen*

I. INTRODUCTION

On March 19, 1969, two photographers (Rolfe Christopher, a former aerial photographer for the U.S. Navy during World War II, and his son, Gary) flew over a manufacturing plant in Texas that was then under construction and took photographs of the plant.[1] Upon seeing a plane circling its construction site, E.I. du Pont deNemours & Co., Inc. (DuPont) brought a lawsuit for trade secret misappropriation under Texas common law alleging that the actions of the defendants constituted the acquisition of trade secrets by "improper means."[2] At the time, there was no

+ This is a draft chapter. The final version will be available in Research Handbook on Intellectual Property and Digital Technologies as part of the Edward Elgar Research Handbooks in IP series, Tanya Aplin editor, forthcoming 2018, Edward Elgar Publishing Ltd. The material cannot be used for any other purpose without further permission of the publisher, and is for private use only.

* Robins Kaplan LLP Distinguished Professor in Intellectual Property Law and Director of the IP Institute at Mitchell Hamline School of Law. Professor Sandeen is grateful for the work of her Research Assistants, Cara Moulton and Yolanda Wilson, on this project and for the research support of Mitchell Hamline School of Law.

1. E. I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012 (5th Cir. 1970), *cert denied*, 400 U.S. 1024 (1971).

2. *Id.*

recognized trade secret claim for the improper acquisition of trade secrets not followed by a disclosure or use of the trade secrets,[3] nor a well-used claim for the wrongful acquisition of business information not constituting trade secrets (often referred to as confidential and proprietary information). To the contrary, two key facts of *E.I. duPont deNemours & Co. v. Christopher* (hereinafter *Christopher*) were that: (1) the plaintiff owned protectable information in the form of trade secrets; and (2) the defendants either disclosed or threatened to disclose those trade secrets to the unidentified third-party who hired them to take the photographs.[4]

While *Christopher* is famous for holding that the "improper means" used to acquire trade secrets need not constitute "a trespass, other illegal conduct, or breach of a confidential relationship"[5] (at least in Texas) it did not answer three questions that are central to any attempt to use tort law (including trade secret law) to combat the wrongful acquisition of information through cyber-hacking or other means. First, if the information that is acquired is not subsequently disclosed or used, what is the cognizable harm to the information owner?[6] Second, what if the information that was taken does not constitute a protectable "property" interest, for instance, by qualifying for trade secret protection?[7] Relatedly, given the strong public policy in the United States and elsewhere that favors the dissemination of information, particularly information that is a part of the public domain, is it advisable to

---

3. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION, § 40 cmt. b (AM. LAW INST. 1995); ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS, § 1.01 (2017) (citations omitted).

4. *Christopher*, 431 F.2d at 1013–14.

5. *Id.* at 1014; *see also* David S Levine, *Schoolboy's Tricks: Reasonable Cybersecurity and the Panic of Law Creation*, 72 WASH. & LEE L. REV. ONLINE 323, 332 (2015).

6. *See* Intel Corp. v. Hamidi, 71 P.3d 296, 308 (Cal. 2003) (emphasizing the need for provable harm for most torts and finding no harm to support a trespass to chattel claim regarding the misuse of Intel's computer system).

7. *Cf.* Mattel, Inc. v. MGA Ent., Inc., 782 F. Supp. 2d 911, 960–61 (C.D. Cal. 2011) (discussing the inability to prevail on a trade secret misappropriation counter-claim if one cannot prove a protectable property interest through proving something is a trade secret). The under-developed common law tort of "misappropriation" also typically requires an identifiable property interest. *See, e.g.*, Hollywood Screentest of Am., Inc. v. NBC Universal, Inc., 151 Cal. App. 4th 631 (2007).

create a broad wrongful acquisition tort to protect all types of information?

Since the advent of the personal computer and the internet, and the concomitant increase in the risk of computer hacking, policymakers have struggled with how to address the acquisition of information by means that are deemed (or seem) improper. In the United States, for instance, the federal law known as the Computer Fraud and Abuse Act (CFAA) was adopted in 1986 to address,[8] among other things, the wrongful access to and wrongful acquisition of information from a "protected computer."[9] In 1996, the European Union (EU) adopted a Database Directive that gives "the maker of a database" a *sui generis* right to protect databases in which they made "a substantial investment."[10] More recently, the United States enacted the Defend Trade Secrets Act of 2016 (DTSA),[11] and the EU adopted a Trade Secret Directive for the stated purpose of combatting the misappropriation of trade secret information.[12] In designing these laws, policymakers skirted the questions posed above by statutorily: (1) defining the interests to be protected;[13] (2) identifying cognizable harm to include, at least, threatened disclosure or use;[14] and (3) specifying a private right of action and remedies.[15] But none of these laws answer the questions left unresolved by *Christopher* with respect to the common law development (or lack thereof) of a wrongful acquisition tort which, at best, seems to have come "out of thin air" based upon the unique facts of *Christopher*.

The analysis undertaken in this chapter was prompted by two puzzles. First, since U.S. trade secret law was developed

---

8. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (2012)).

9. 18 U.S.C. § 1030(e)(2) (2012).

10. Directive 96/9, of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, 1996 O.J. (L 77) 20, 25 (EC) [hereinafter Database Directive].

11. Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, § 1890, 130 Stat. 376 (codified at 18 U.S.C. §§ 1832–1833, 1835–1836, 1838–1839).

12. Directive 2016/943, of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, 2016 O.J. (L 157) 1 (EU) [hereinafter Trade Secret Directive].

13. *See, e.g.*, Database Directive, *supra* note 10, arts. 2, 3, 7.

14. *See, e.g.*, 18 U.S.C. § 1030(c)(4) (2012).

15. *See, e.g.*, 18 U.S.C. § 1836 (2012); Database Directive, *supra* note 10, art. 12.

based upon the breach of confidence law of England,[16] and the law of England does not recognize an acquisition by improper means theory of recovery except in rare and nascent circumstances,[17] how and why did such a theory develop in the United States? Second, to the extent the acquisition by improper means prong of U.S. trade secret law (unlike its counterpart in England) is disconnected from a duty of confidence and should be thought of as a separate tort,[18] what are its elements, including the definition of cognizable harm? These questions are important not only for an understanding of trade secret law in the United States,[19] but also for the implementation of the EU Trade Secret Directive which borrows from U.S. law to include the "acquisition by improper means" prong of U.S trade secret law.[20] They also relate to the debate concerning the harms caused by data breaches and whether the mere taking or misuse of personal information, like credit information, is a cognizable "injury-in-fact" under U.S. law.[21]

This chapter proceeds in three parts. First, based upon historical research, it examines how the "acquisition by improper means" prong of U.S. trade secret law developed and how it became disconnected from the requirement of a subsequent disclosure or use of the trade secrets.[22] This analysis begins in Section II with an overview of the laws of the United States that protect information. In Section III, the history of the "acquisition by improper means" prong of trade secret misappropriation is discussed, showing that it is undertheorized, particularly when the alleged wrongful

16. *See* BRIAN T. YEH, CONG. RES. SERV., PROTECTION OF TRADE SECRETS: OVERVIEW OF CURRENT LAW AND LEGISLATION 5 (2016) (discussing the historical development of trade secret law).

17. Some recent English cases have provided relief in wrongful acquisition situations involving rights of privacy by finding that a duty of confidence arose from the wrongful acquisition. *See, e.g.*, Tchenguiz v. Imerman, [2010] ECWA Civ 908. This, however, is different from finding a stand-alone wrongful acquisition claim not based upon a breach of confidence which, only in the last few years, has begun to emerge in England. *See* Google v. Vidal Hall, [2015] EWCA Civ 311.

18. *See* MILGRIM, *supra* note 3, § 1.01 (discussing the prongs for liability for disclosure or use of another's trade secret).

19. 18 U.S.C. §§ 1832–1833, 1835–1836, 1838–1839.

20. Trade Secret Directive, *supra* note 12.

21. *See, e.g.*, Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016).

22. *See* MILGRIM, *supra* note 3 (discussing the development of trade secret law in the United States).

acquisition is not connected to a duty of confidence or a subsequent disclosure or use of trade secrets.[23] Third, in Section IV, the pros and cons of recognizing a separate wrongful acquisition tort are discussed, including observations concerning the inability of trade secret law to address all incidents of cyber-hacking and how a standalone wrongful acquisition tort might be designed.[24]

II. SUMMARY OF INFORMATION LAW

With the increase in accusations and incidents of "leaking," "hacking," and "spying," including cyber-hacking,[25] the law governing the protection of information has taken on greater importance, requiring an understanding of the types of information that can be protected and the nature of cognizable harms related to information.[26] This is particularly true with respect to "non-confidential" and "public" information because the policy in the United States (and many other countries)[27] is that information is *not* protected except in limited circumstances, and once information is made public it is free for anyone to use.[28] As has been repeatedly stated by the U.S. Supreme Court, all ideas and information in general circulation are dedicated to the common good unless protected by applicable (but limited) intellectual property rights.[29] As Justice O'Connor explained with respect to U.S. patent law: "From their inception, the federal patent laws have embodied a careful balance between

---

23. *See id.* § 15.01 (discussing how the great preponderance of cases involve a breach of duty of confidence).

24. Defend Trade Secrets Act of 2016, §§ 4–5 (discussing how companies are increasing measures to combat hacking and how the current state of trade secret law is ineffective).

25. *Id.* § 3 (discussing the increased risk of trade secret misappropriation).

26. *See generally* Defend Trade Secrets Act of 2016 (discussing the need for strengthening trade secret law).

27. *See* Universal Declaration of Human Rights, art. 19 (declaring that freedom of information includes the right "to receive and impart information"); Charter of Fundamental Rights of the European Union, art. 11.1 (stating that the right to freedom of expression includes the right "to receive and impart information without interference by public authorities").

28. *See* MILGRIM, *supra* note 3, § 15.01 (discussing how matters of public knowledge are not protectable).

29. *See e.g.*, Golan v. Holder, 565 U.S. 302, 328–32 (2012); Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 146 (1989); Kewanee Oil Co. v. Bicron Corp. 416 U.S. 470, 481 (1974); *see also* RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

the need to promote innovation and the recognition that imitation and refinement through imitation are both necessary to invention itself and the very lifeblood of a competitive economy."[30] This same sentiment explains the limited scope of all laws that protect information and why trade secret protection in the United States is designed so as not to interfere with the disclosure purpose of patent law.[31] Thus, the desire to protect information and databases, even against acts of wrongful acquisition, must always be balanced against the essential role that information plays in creating knowledge and the conditions for innovation and competition.[32]

Based upon existing law in the United States and elsewhere, there are currently five (perhaps six) limited means to protect information, each providing varying degrees of protection. First, certain types of information may be protected by patent and copyright laws, but only for a limited time and with respect to certain types of uses or wrongs.[33] Second, if information qualifies as "personal information," it may be protected by applicable privacy and data protection laws.[34] Third, if information meets the legal definition of a trade secret then it might be protected against "misappropriation,"[35] but trade secret protection ends when the information becomes generally known or readily ascertainable.[36] Fourth, an information owner might protect its confidential information pursuant to contract law, but usually contract law cannot be

30. *Bonito Boats*, 489 U.S. at 146.

31. *Id.*

32. *See generally* Defend Trade Secrets Act of 2016, §§ 2–5 (discussing how companies desire to protect information and databases, and discussing the trade-off between patent protection and trade secret protection).

33. 17 U.S.C. §§ 106, 501 (2012); 35 U.S.C. § 271 (2012).

34. *E.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (2012); Freedom of Information Act, 5 U.S.C. § 552a(a)(5) (2012) (stating that a "system of records" includes any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying signature that is assigned to the individual); Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681b(a) (2012) (stating that any consumer reporting agency may furnish a consumer report only under a set of specific limitations).

35. For information on the definition of a "trade secret," see 18 U.S.C. § 1839(3) (2012) which states a "trade secret" has three parts: (1) information; (2) reasonable measures taken to protect the information; and (3) which derives independent economic value from not being publicly known. *See also* MILGRIM, *supra* note 3, § 4.02.

36. *See* 18 U.S.C. § 1839(3)(B); *see also* Coco v. A.N. Clark (Eng'rs) Ltd., [1968] F.S.R. 415 (U.K.) (detailing English breach of confidence claim elements).

used to protect non-confidential information or to designate information as protectable trade secrets, and it usually does not apply to third-parties to the contract.[37] Fifth, some statutes provide *sui generis* forms of protection for specified types of information, for instance, laws that protect information that is submitted to the government, databases, and so-called "data exclusivity" laws.[38] The possible sixth claim for relief, although limited and suffering from various preemption and preclusion problems, relates to common law misappropriation and unfair competition causes of action that are recognized in some states.[39]

The limited types and scope of protection for information mean that not all information is protected by law and, in fact, not all "secret" or "confidential" information is protected. This is particularly true with respect to information that can be gleaned from public sources, whether the information is widely-distributed or not. Although the language that is used under various areas of law, and in different countries, varies, generally, information that is "generally known," "readily ascertainable," and "in the public domain" is not protected.[40] Thus, the unprotected status of some information means that someone can "wrongfully acquire" information from another without violating a recognized interest in the information.[41] This might happen, for instance, when the information taken does not qualify as "confidential information"[42] in breach of confidence

---

37. *See* Sharon K. Sandeen, *A Contract by Any Other Name Is Still a Contract: Examining the Effectiveness of Trade Secret Clauses to Protect Databases*, 45 IDEA 119, 146–150 (2005) (discussing some of the limitations of protecting trade secrets with contracts in the context of databases).

38. *E.g.*, 18 U.S.C. § 1905 (stating that any government agent or employee is subject to fines or imprisonment if, during the course of their employment, it discloses information that "concerns or relates to the trade secret, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data. . ." or any amount of income or expenditure); 41 U.S.C. § 2102 (2012) (stating that an employee of a private sector organization cannot knowingly disclose contractor bids or proposal information while working for the federal government).

39. *See, e.g.*, Sioux Biochem., Inc. v. Cargill, Inc., 410 F. Supp. 2d 785, 804 (N.D. Iowa 2005) (discussing Iowa's common law claim for misappropriation and the preemption and preclusion issues attendant thereto).

40. Kewanee Oil Co. v. Bicron Corp. 416 U.S. 470, 476 (1974); Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 150 (1989).

41. *Bonito Boats*, 489 U.S. at 150.

42. *See* 19 C.F.R. 201.6(a)(1) (2017) ("[Confidential information] is information which concerns or relates to the trade secrets, processes, operations, style of works, or apparatus, or to the production, sales, shipments,

jurisdictions, or as "trade secrets"[43] in jurisdictions which apply the Uniform Trade Secrets Act (UTSA) definition, or as "property" where common law misappropriation claims are recognized.[44] It can also happen where the alleged bad actor is not subject to a contractual or implied duty of confidentiality[45] or where the holder of the information does not own the information, for instance, businesses which collect and compile pre-existing information from public databases and individuals that, technically, is owned by others or no one.[46]

III. THE ELUSIVE WRONGFUL ACQUISITION TORT

Currently, when wrongfully acquired information meets the definition of a trade secret, then wrongful acquisition is a subset of the "acquisition by improper means" form of trade secret misappropriation as defined in the UTSA, the DTSA, and the EU Trade Secret Directive, and can be redressed by bringing a claim for relief under those laws.[47] Similarly, when the information meets the definition of "confidential information" in breach of confidence jurisdictions, a breach of confidence claim may lie. However, if the wrongfully acquired information does not meet

---

purchases, transfers, identification of customers, inventories, or amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or other organization, or other information of commercial value, the disclosure of which is likely to have the effect of either impairing the Commission's ability to obtain such information as is necessary to perform its statutory functions, or causing substantial harm to the competitive position of the person, firm, partnership, corporation, or other organization from which the information was obtained, unless the Commission is required by law to disclose such information.").

43. *See* 18 U.S.C. § 1839(3) (2012) (stating a "trade secret" has three parts: (1) information; (2) reasonable measures taken to protect the information; and (3) which derives independent economic value from not being publicly known).

44. *See* SunPower Corp. v. SolarCity Corp., No. 12-CV-00694-LHK, 2012 WL 6160472, at *2 (N.D. Cal. Dec. 11, 2012) (dismissing plaintiff's common law misappropriation claim for failure to allege a sufficient property interest).

45. UNIF. TRADE SECRETS ACT WITH 1985 AMENDMENTS § 7 (UNIF. LAW COMM'N 1985) (stating the act does not apply to duties voluntarily assumed through an express or an implied-in-fact contract and the Act does not apply to duties imposed by law that are not dependent upon the existence of significant secret information).

46. *See generally Bonito Boats*, 489 U.S. at 154.

47. Sharon K. Sandeen, *The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act*, 33 HAMLINE L. REV. 493, 501 (2010).

the definition of a trade secret or confidential information, then some other claim for relief must exist.

The principal hypothesis underlying this article is that no tort of "wrongful acquisition"[48] developed in the United States either separately or as part of trade secret law. Instead, language of bad acts amounting to wrongful acquisition often appears in trade secret cases that otherwise involve breach of confidence claims.[49] In this regard, most trade secret cases are imbued with the rhetoric of "theft" and "espionage" even if acts of wrongful acquisition did not occur. Thus, one must carefully examine the factual allegations of cases to distinguish between those involving the breach of confidence type of trade secret misappropriation (including claims of inducement of breach of a duty of confidence) and those involving wrongful acquisition claims as defined herein.[50] A corollary hypothesis is that, even if a separate tort of wrongful acquisition developed at common law, a theory of harm for wrongful acquisition not accompanied by the subsequent disclosure or use of the wrongfully acquired information is non-existent.

To test these hypotheses, relevant reported cases and secondary sources were examined that establish that few reported cases of the wrongful acquisition of trade secrets or other information exist in the United States. The first set of reported cases examined was for the period of 1837 (the date of the first trade secret case in the United States)[51] to 1938 (the year before the *Restatement (First) of Torts* provisions on trade secret law were published).[52] Using the online database, Westlaw, the author identified a pool of over 1200 cases and carefully reviewed the first 150, ranked by relevance. Next, using the initial 1200 cases, additional search queries were conducted for the terms "theft," "bribery," "misrepresentation,"

---

48. To differentiate a wrongful acquisition tort from a trade secret or breach of confidence claim, the term "wrongful acquisition" is used herein to refer to bad acts that either: (1) do not involve breaches of the duty of confidence in the first or second degree; or (2) lead to the acquisition of unprotected information held by another. Breach of confidence in the "second degree" refers to acts by third-parties to the original misappropriation, where the first-party was subject to a duty of confidentiality.

49. Sandeen, *supra* note 47, at 499.

50. *See* UNIF. TRADE SECRETS ACT WITH 1985 AMENDMENTS § 7 (UNIF. LAW COMM'N 1985).

51. Vickery v. Welch, 36 Mass. 523 (1837).

52. RESTATEMENT (FIRST) OF TORTS, §§ 757–59 (1939).

"inducement of breach," "espionage," and "fraud," in an attempt to find examples of wrongful acquisition cases.[53] Additionally, because the language of "discovery by improper means" is contained in the *Restatement (First) of Torts*, section 757, the archives of the American Law Institute (ALI) related to the drafting of the provisions on trade secrecy, as well as early treatises and casebooks on tort law, were examined to identify additional cases involving allegations of wrongful acquisition and to determine if early tort scholars recognized the existence of a wrongful acquisition claim that was separate from the common law breach of confidence claim. This included a review of the *Restatement's* provisions on trade secret law and the Reporter's Explanatory Notes to those provisions.[54]

It is clear from the early development of trade secret law in the United States that it was originally conceived of as an act of unfair competition resulting from a breach of confidence and that this conception of wrongdoing was borrowed from England.[55] Justice Holmes famously said as much in *E. I. duPont deNemours Powder Co. v. Masland*.[56] However, at that time, the cognizable harm was the "disclosure or use of another's trade secret" as reflected in the first line of the *Restatement (First) of Torts*, section 757,[57] highlighting the property aspects of trade secret law.[58] It is also clear, based on the language of the

---

53. All of these terms, with the exception of fraud, are listed as "improper means" in the UTSA. UNIF. TRADE SECRETS ACT WITH 1985 AMENDMENTS § 1(1) (UNIF. LAW COMM'N 1985); *cf.* Trade Secret Directive, *supra* note 12 (listing practices that may be used for misappropriation including theft, unauthorized copying, and economic espionage).

54. RESTATEMENT (FIRST) OF TORTS, explanatory notes § 2 cmt. a (AM. LAW INST., Preliminary Draft No. 6, 1938).

55. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. a (1995) (citing Morison v. Moat (1851) 68 Eng. Rep. 492).

56. E. I. duPont deNemours Powder Co. v. Masland, 244 U.S. 100 (1917) ("Whether the plaintiffs have any valuable secret or not the defendant knows the facts, whatever they are, through a special confidence that he accepted. The property may be denied, but the confidence cannot be. Therefore, the starting point for the present matter is not property or due process of law, but that the defendant stood in confidential relations with the plaintiffs, or one of them.").

57. MILGRIM, *supra* note 3, § 1.01 n.82 (noting that under the Restatement (First) of Torts, acquisition by improper means was a predicate act for misappropriation, not a tortious act in itself).

58. *See* Eric R. Claeys, *Private Law Theory and Corrective Justice in Trade Secrecy*, 4 J. TORT L. 1, 9 (2011) (arguing that a property rights view of trade secret law is the theory that best explains the various features of trade secret law).

Restatement (First) of Torts, that the act of acquiring trade secrets and other business information by "improper means" or "improper procurement" has long been seen as an act of unfair competition in the United States. It is just not clear what the requisite harm is in the absence of a subsequent disclosure or use of the information and what justifications and defenses might apply to such behavior.

An early case that appears to be the genesis of the acquisition by improper means theory of trade secret misappropriation is *Tabor v. Hoffman*, in which the defendant acquired copies of patterns for the manufacture of pumps.[59] The question before the court was whether the patterns for a product that was patented and sold publicly could nonetheless qualify as trade secrets. The defendant had not acquired the patterns from public information, but obtained them from a vendor of plaintiff's who copied the patterns and provided them to defendant.[60] Thus, although the vendor was under a direct duty of confidentiality to the trade secret owner, the defendant was not. Under the UTSA, this set of facts would give rise to liability based upon the defendant's knowledge or reason to know of the misappropriation by the vendor, but pursuant to common law, the court focused on the perceived wrongful acts of the defendant. In dicta, the court explained: "But, because this discovery may be possible by fair means, it would not justify a discovery by unfair means, such as the bribery of a clerk, who in course of his employment had aided in compounding the medicine, and had thus become familiar with the formula."[61] It is not clear from the reported case decision, however, whether *Tabor* involved acts of bribery.[62]

Since it was decided in 1889, *Tabor* has been cited in more than 100 cases for four different but related principles: (1) that the public has the right to use information that has been disclosed to the public;[63] (2) that trade secrets may exist even if the goods to which they are related are otherwise exposed to the public;[64] (3) that the circumstances by which trade secrets are

59. Tabor v. Hoffman, 23 N.E. 12, 12–13 (N.Y. 1889).

60. *Id.*

61. *Id.* at 36.

62. *See id.*

63. *E.g.*, Kaylon, Inc. v. Collegiate Mfg. Co., 7 N.Y.S.2d 113, 114 (N.Y. App. Div. 1938).

64. *E.g.*, Edgar H. Wood Assocs. v. Skene, 347 Mass. 351, 364 (1964).

acquired may be actionable, even if the information could have been acquired rightfully;[65] and (4) that trade secret owners may be entitled to permanent injunctive relief even in situations where an award of damages would be an adequate remedy.[66] In keeping with the improper acquisition language of *Tabor*, the statements of subsequent courts about what constitutes improper acquisition usually include a trinity of some type of wrongful acquisition (usually fraud, theft, or bribery), breach of a duty of confidence, and breach of contract, but with little discussion of what might constitute wrongful acquisition not accompanied by a breach of confidence or a subsequent disclosure or use of trade secrets.[67]

The provisions of the *Restatement of Torts* that address trade secret law reflect what the members of the ALI thought was the better reasoned law circa 1939. As a practical matter, they also reflect the case law that the drafters reviewed and relied upon. Significantly, however, none of the cases cited in the Reporter's Explanatory Notes or in the commentary to the *Restatement of Torts*, sections 757–759, involve a wrongful acquisition claim (as that term is defined herein).[68] Instead, the cases cited (less than 40) involve breach of confidence claims, including claims of inducement of breach involving the acquisition of trade secrets by a third party.[69] This is true even with respect to Section 759 of the *Restatement of Torts* which sets forth the wrong (not adopted by the UTSA or the DTSA) of "procuring" the business information of another "for the purpose of advancing a rival business interest." Thus, the comment to section 757, which defines "improper means" to include all means which "fall below the generally accepted standards of commercial morality and reasonable conduct" seems to have come out of thin air, or at least a thin body of reported decisions.[70] Also, in 1939 an act of "discovery by improper means" alone did not result in a cognizable harm unless it was

---

65. *E.g.*, Dr. Miles Med. Co. v. John D. Park & Sons Co., 220 U.S. 373, 402 (1911).

66. *E.g.*, Franke v. Wiltschek, 209 F.2d 493, 497 (2d Cir. 1953).

67. *See, e.g.*, *id.*

68. *See* RESTATEMENT (FIRST) OF TORTS §§ 757–59 (AM. LAW INST. 1939); RESTATEMENT (FIRST) OF TORTS, explanatory notes § 2 cmt. a (AM. LAW INST., Preliminary Draft No. 6, 1938).

69. RESTATEMENT (FIRST) OF TORTS §§ 757–59 (AM. LAW INST. 1939).

70. *Id.* § 757 cmt. f.

accompanied by a subsequent disclosure or use of the subject trade secrets.[71] As explained in *Milgrim*:

> Notably, under the *Restatement of Torts* § 757 . . . the wrongful acquisition (i.e., "discovery by improper means") of a trade secret is not in and of itself misappropriation but rather is simply a predicate for holding the wrongdoer liable for the *later* unauthorized use or disclosure of the secret. By contrast, under the UTSA, wrongful acquisition of a trade secret is independently actionable even if there is no ensuing use or disclosure.[72]

In other words, the recognition of a claim of acquisition by improper means, not followed by a subsequent disclosure or use, did not officially occur until 1979 when the UTSA was adopted and was thereafter enacted by individual states. But it is not clear why the disconnection occurred. Additionally, although wrongful acquisition not followed by disclosure or use may be "actionable" under the UTSA (and now the DTSA), damage remedies remain unavailable in the absence of proof of actual harm.[73]

Noting that the UTSA modified the wording of the *Restatement* to include, for the first time, language of acquisition by improper means not followed by disclosure or use,[74] the author examined records of the American Bar Association (ABA) and the National Conference of Commissioners of Uniform State Laws (now the Uniform Law Commission (ULC)) to determine if there was an explanation for the change.[75] There was none, and consequently, there is no record of a discussion of the nature of the required harm for acquisition by improper means if such act is not accompanied by a subsequent disclosure or use of the subject trade secrets. Indeed, the only relevant information that is contained in the drafting history of the UTSA is a brief discussion of *Christopher*, one of only a handful of reported wrongful acquisition cases that were found as part of this project.

---

71. *Id.* § 757. This is consistent with U.S. patent, copyright, and trademark law which each require some use of the intellectual property rights as a part of the plaintiff's claim of infringement.

72. MILGRIM, *supra* note 3, § 1(2) (citations omitted); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. b (AM. LAW INST. 1995).

73. 18 U.S.C. § 1836(b)(3)(B); UNIF. TRADE SECRETS ACT WITH 1985 AMENDMENTS § 3 (UNIF. LAW COMM'N 1985).

74. UNIF. TRADE SECRETS ACT WITH 1985 AMENDMENTS § 1 (UNIF. LAW COMM'N 1985).

75. Copies of the records are on file with the author; originals remain in the archives of the ABA and ULC.

Finally, the author reviewed *Milgrim on Trade Secrets* and undertook a search of relevant cases cited therein.[76] The Milgrim treatise confirmed that there is a paucity of reported case decisions involving claims that trade secrets were wrongfully acquired.[77] Thus, a review of relevant secondary resources and a search of reported cases from 1837 to present reveals little jurisprudence to support or explain the development of a wrongful acquisition tort within or outside of trade secret law. This may explain why there are few prosecutions under the Economic Espionage Act of 1996 as well.[78] Either there are not a lot of incidents involving the wrongful acquisition of trade secrets and other information, or acts of wrongful acquisition are not being detected.

One explanation for the paucity of wrongful acquisition cases before (and since) 1979 is that most trade secret cases involve parties that are in a confidential relationship and, of those, most involve the employer-employee relationship.[79] Typically, in an employer-employee case, there is no claim of acquisition by improper means because the employer voluntarily disclosed its secrets to its employees.[80] Allegations of wrongful acquisition creep into reported cases with respect to claims not involving employees, but even then, the focus of the cases is often on the existence of a duty of confidentiality between the trade secret owner and a former employee.[81] An explanation for this relates to the struggles of early courts to develop theories to hold third-parties (those not engaged in the initial misappropriation)

---

76. *See generally* MILGRIM, *supra* note 3.

77. *Id.* § 15.01 ("The issue of wrongful taking, however, arises relatively rarely: the vast preponderance of disputes in the law of misappropriation arise from proper acquisition followed by later unauthorized use or disclosure.").

78. *But cf.* Press Release, U.S. Senator Orrin Hatch, Senate, House Leaders Introduce Bipartisan, Bicameral Bill to Protect Trade Secrets (July 29, 2015) ("Current federal criminal law is insufficient. Although the *Economic Espionage Act of 1996* made trade secret theft a crime, the Department of Justice lacks the resources to prosecute many such cases.").

79. For an example of the centrality of the employer-employee relationship in some trade secret cases, *see* Richdale Dev. Co. v. McNeil Co., 508 N.W.2d 853, 855 (Neb. 1993) ("The elements necessary to establish a cause of action for misappropriation of a trade secret are . . . (4) the communication of the secret to the employee while he was employed in a position of trust and confidence and under circumstances making it inequitable and unjust for him to disclose it to others or to use it himself to the employer's prejudice.").

80. *See id.*

81. *See, e.g.*, Comput. Assocs. Int'l v. Altai, Inc., 982 F.2d 693, 718–19 (2d Cir. 1992).

liable for their subsequent disclosure or use of the subject trade secrets.[82] In the U.S., this was done by imposing a duty upon third-parties not to disclose or use trade secrets once they knew or had reason to know of the existence of trade secrets and their misappropriation.[83]

Separate from the few cases that discuss the wrongful acquisition of trade secrets, a body of common law developed that some courts label the "improper procurement" tort.[84] It is reflected in Section 759 of the *Restatement (First) of Torts*, which states: "One who, for the purpose of advancing a rival business interest, procures by improper means information about another's business is liable to the other for the harm caused by his possession, disclosure or use of the information."[85] The significance of this tort for present purposes is that it could protect confidential business information not rising to the level of a trade secret, thereby potentially providing guidance concerning the elements of a non-trade secret based wrongful acquisition tort. However, despite its inclusion in the *Restatement (First) of Torts*, there are not many reported cases before or after 1939 that explain the parameters of the improper procurement tort. This is in part because of the general paucity of cases involving acquisition of information by improper means, but also because such a claim was subsequently precluded by the reasoning of *Kewanee Oil Co. v. Bicron Corporation*.[86] and by the UTSA,[87] both of which limit the availability of tort claims for the misappropriation of information. Moreover, while seemingly covering more business information than trade secrets, the requirement of harm under Section 759 still demanded a level of confidentiality similar to trade secrecy.[88] As explained in Comment b to Section 759: "There are no limitations as to the type of information included except that it relate to matters in his business. Generally, however, if the improper discovery of the information is to cause harm, the information must be of a

---

82. *See* Sandeen, *supra* note 47, at 500.

83. UNIF. TRADE SECRETS ACT WITH 1985 AMENDMENTS § 1(2)(ii)(B) (UNIF. LAW COMM'N 1985).

84. *E.g.*, DeWoody v. Ripley, 951 S.W.2d 935, 948 (Tex. Ct. App. 1997).

85. RESTATEMENT (FIRST) OF TORTS § 759 (AM. LAW INST. 1939).

86. *See* Sandeen, *supra* note 47, at 515–17.

87. UNIF. TRADE SECRETS ACT WITH 1985 AMENDMENTS § 7 (UNIF. LAW COMM'N 1985).

88. RESTATEMENT (FIRST) OF TORTS § 759 cmt. b (AM. LAW INST. 1939).

secret or confidential character."[89] Importantly, Section 759 does not reflect a decision to do away with the traditional requirement of actual harm for tort claims related to the wrongful acquisition of information and is inconsistent with a trespassory theory of harm.

The drafting history of the UTSA, consisting of hundreds of pages of source documents obtained from the ABA and the ULC, also does not contain a robust discussion of the wrongful acquisition type of trade secret misappropriation, even though the UTSA's definition of misappropriation is a departure from the language of the *Restatement (First) of Torts* in that it defines "acquisition . . . by improper means" as a wrong disconnected from a subsequent disclosure or use.[90] The impetus behind the UTSA was multifaceted, but was primarily a desire to fix perceived abuses in the interpretation and application of the common law of trade secrecy by limiting the scope of trade secret protection in numerous respects.[91] The drafters of the UTSA were particularly concerned about the assertion of tort claims not requiring proof of the existence of viable trade secrets and the likelihood that such claims were preempted by federal law as explained in *Kewanee*.[92] This explains why Section 759 of the *Restatement (First) of Torts* was not carried over into the UTSA or the *Restatement (Third) of Unfair Competition*,[93] but it does not explain why "acquisition . . . by improper means" was included as a potential wrong without a requirement of a subsequent disclosure or use and what the required "harm" might be in the absence of disclosure or use.[94]

As stated in *Milgrim*:

> The Uniform Trade Secrets Act provides a somewhat different test than trade secret common law. While in the great preponderance of

89. *Id.*

90. UNIF. TRADE SECRETS ACT WITH 1985 AMENDMENTS § 1(2) (UNIF. LAW COMM'N 1985).

91. *See* Sandeen, *supra* note 47, at 507.

92. *See id.* at 527–29.

93. *Compare* RESTATEMENT (FIRST) OF TORTS § 759 (AM. LAW INST. 1939) ("One who, for the purpose of advancing a rival business interest, procures by improper means information about another's business is liable to the other for the harm caused by his possession, disclosure or use of the information."), *with* UNIF. TRADE SECRETS ACT WITH 1985 AMENDMENTS § 1(4) (UNIF. LAW COMM'N 1985) (defining trade secret), *and* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (AM. LAW INST. 1995) (defining trade secret).

94. UNIF. TRADE SECRETS ACT WITH 1985 AMENDMENTS § 1(2) (UNIF. LAW COMM'N 1985).

> cases, the wrongful conduct consists of unauthorized use or disclosure, it should not be overlooked that unauthorized access or acquisition alone may give rise to a cause of action . . . However, where access is authorized, the issue of claimed trade secret misappropriation will turn upon whether the recipient engaged in wrongful use or disclosure. In other words, mere access or acquisition without wrongful conduct will not generate trade secret liability.[95]

This change, while not discussed in the drafting history of the UTSA, appears to have been influenced by *Christopher*,[96] which was decided in 1970 during the early stages of the UTSA drafting project.[97]

As in *Tabor*, a critical fact of *Christopher* is that the defendants who were sued owed no duty of trust or confidence to the plaintiff, but unlike *Tabor*, none of the actors who facilitated the acquisition of DuPont's trade secrets owed any duty of trust or confidence.[98] Thus, the "wrong" was the acquisition of trade secrets without any duty of confidence in the first or second degree.[99] Characterizing the defendants acts as "industrial espionage"[100] and "school boy's tricks,"[101] and applying a cost benefit analysis, the court explained: "Commercial privacy must be protected from espionage which could not have been reasonably anticipated or prevented."[102] Significantly, however, the court was careful not to impugn all acts of information collection, explaining:

> We do not mean to imply, however, that everything not in plain view is within the protected vale, nor that all information obtained through every extra optical extension is forbidden. Indeed, for our industrial competition to remain healthy there must be breathing room for observing a competing industrialist. A competitor can and must shop his competition for pricing and examine his products for quality, components, and methods of manufacture.[103]

---

95. MILGRIM, *supra* note 3, § 15.01 (2017) (citations omitted).

96. E. I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012 (5th Cir. 1970), *cert denied*, 400 U.S. 1024 (1971).

97. *See* Sandeen, *supra* note 47, at 510–13 (describing aspects of the drafting history of the UTSA).

98. *See Christopher*, 431 F.2d at 1016.

99. *See id.* ("DuPont has a valid cause of action to prohibit the Christophers from improperly discovering its trade secret and to prohibit the undisclosed third party from using the improperly obtained information.").

100. *Id.*

101. *Id.*

102. *Id.*

103. *Id.*

Also, given the procedural posture of the case (an appeal from an interlocutory order denying a motion to dismiss), the court did not consider the nature and extent of DuPont's harm, other than to point out that there was evidence that the defendants disclosed the information to a third-party.[104]

In keeping with the paucity of wrongful acquisition cases, *Christopher* has been cited in only fifty-three reported cases in the United States.[105] The case has been cited mostly for one of two propositions: (1) that improper means of acquiring trade secrets need not amount to a crime or tort; and (2) that trade secret owners are only required to engage in "reasonable efforts" to protect their trade secrets and are not required to institute extreme and unduly expensive security measures.[106] *Christopher* is cited more often in secondary sources (402 times) as an example of an acquisition by improper means form of trade secret misrepresentation case, proving its influence despite its lack of details.[107] The problem with relying upon *Christopher* to define a wrongful acquisition tort (if one is to be further developed), is that it does not discuss all the elements of such a tort. While the court recognized that DuPont had to prove the existence of a trade secret and its misappropriation, it does not discuss the classic tort elements of causation and harm, specifically what constitutes a cognizable harm if the trade secrets are not subsequently disclosed or used.

Reported cases since *Christopher* involving wrongful acquisition claims are few and typically fail to discuss the elements of such a claim in detail. Most of the cases listed in *Milgrim* are cited for the proposition that, in the absence of a claim that the plaintiff's trade secrets were disclosed or used, a

---

104. *Id*. at 1012.

105. *See E. I. duPont deNemours & Co. v. Christopher*, WESTLAW, https://1.next.westlaw.com/ (from the page displaying text of the case for *Christopher*, 431 F.2d 1012, follow hyperlinks to "Citing References" and then to "Cases.").

106. *See, e.g.*, Phillips v. Frey, 20 F.3d 623, 630 (5th Cir. 1994) (citing *Christopher* for the proposition that a higher standard than "the law of the jungle" applies when evaluating improper means); Sheet v. Yamaha Motors Corp., U.S.A., 849 F.2d 179, 182 (5th Cir. 1988) (citing *E. I. duPont deNemours & Co. v. Christopher*, among others, to explain the "relative secrecy" standard which requires reasonable efforts to maintain secrecy).

107. *See E. I. duPont deNemours & Co. v. Christopher*, WESTLAW, https://1.next.westlaw.com/ (from the page displaying text of the case for *Christopher*, 431 F.2d 1012, follow hyperlinks to "Citing References" and then to "Secondary Sources").

trade secret owner can state a claim for relief by alleging that it owns trade secrets that were acquired by improper means.[108] In such cases, the plaintiff has the burden of pleading and proving the existence of trade secrets and their improper acquisition, but it is unclear how the requisite harm would be shown. If trade secret misappropriation is viewed as a type of property claim, then it might be argued that the harm is the invasion of a property interest, similar to the harm recognized for a trespass to real property.[109] But if it is viewed as a form of unfair competition, then a non-property based theory of harm must be articulated. Of course, the lack of discussion of cognizable harm becomes more critical when a claim of wrongful acquisition concerns information that does not qualify for some form of legal protection.

With respect to the common law development of a wrongful acquisition tort, the conundrum is that if information is wrongfully acquired but not subsequently disclosed or used, there is no harm to the information nor an argument of unjust enrichment on which to base a claim for monetary damages. If the information is not protected as a property right by some body of law, such as trade secret law, then a theory of harm based upon trespass does not work either. Additionally, unlike personal information that is the focus of privacy or rights of publicity claims, businesses do not have an interest in their information that might support an allegation of dignitary harm. Thus, even in trade secret cases involving the alleged wrongful acquisition of information, there may be a wrong but no protectable trade secrets and, therefore, no remedy. Other areas of information law involve similar weaknesses. In the case of patent and copyright law, for instance, the wrongful behavior must constitute a violation of a limited list of exclusive rights

---

108. *See* MILGRIM, *supra* note 3 ("Misappropriation . . . includes unauthorized acquisition, use and disclosure. The two principal claims that are asserted in a misappropriation civil case are breach of contract and breach of confidence."); *see also* Comment, *Theft of Trade Secrets: The Need for a Statutory Solution*, 120 U PA. L. REV. 378, 383 n.34 (1971) (claiming that "the exhaustive list of cases dries up when the discussion reached industrial espionage without subversion of employees or trespass.").

109. *See* Claeys, *supra* note 58, at 37 (discussing the right to a trade secret as "conceptual property" and explaining how "trespass ordinarily embodies and declares a normative interest that owners may exclude all unconsented entries for virtually any reason").

and the subject information must meet the definition of protected information.[110]

IV. SHOULD A SEPARATE TORT OF WRONGFUL ACQUISITION BE RECOGNIZED?

The possibility that unprotected or non-owed information held by a business or individual may be wrongfully acquired suggests the need for a wrongful acquisition tort either developed at common law or by statute, but it does not answer the question whether such a tort should be recognized. Our laws do not currently provide remedies for all perceived wrongdoing but, instead, reflect policy choices that usually involve a weighing of competing interests. As noted previously, it is generally understood that competition and the free flow of unprotected information is the rule and that intellectual property protections (including trade secret laws) are limited exceptions to the rule designed to benefit society in some way.[111] Thus, it must be asked what society would gain from a law that restricts the acquisition (and the disclosure or use) of otherwise unprotected information, and what might it lose? Assuming (as the definition of "wrongful acquisition" used herein does) that an act of wrongful acquisition does not involve a recognized property interest or a cognizable harm, there is no property interest to be protected or harm to be rectified that relates to the information itself.

The rhetoric of "theft" that pervades trade secret law and accusations of cyber-hacking suggests that many assume that all acts leading to the unauthorized acquisition of information should be deemed "wrongful." However, as the court in *Christopher* recognized, a commitment to free enterprise and a competitive market environment requires a more nuanced view; one that recognizes the value of information flows, particularly for information that is not protected by an existing body of law.[112] This is particularly true if the subject information was

---

110. *See, e.g.*, WORLD INTELL. PROP. ORG., INTRODUCTION TO INTELLECTUAL PROPERTY: THEORY AND PRACTICE 3 (1997) ("Generally speaking, intellectual property law aims at safeguarding creators and other producers of intellectual goods and services by granting them certain time-limited rights to control the use made of those productions.").

111. *See supra* Section II.

112. E. I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970), *cert denied*, 400 U.S. 1024 (1971).

acquired for a salutary purpose, such as revealing criminal behavior, sharing unprotected information, or enhancing competition. As things currently stand, U.S. law makes a rough distinction between acquisition of information for improper versus beneficial purposes by providing a claim for relief for only trade secrets and other categories of protected information.[113] If the United States and other countries wish to create a standalone wrongful acquisition tort for otherwise unprotected information, then the resulting claim for relief should be limited in other ways.

Under tort law, not all wrongful behavior results in a claim for relief. Rather, whether tort liability is imposed usually depends upon the ability to articulate some "fault" of the defendant that society wishes to sanction and that caused actual harm to the plaintiff. Ordinarily, fault is defined by some combination of: (1) the nature of the defendant's acts; (2) the defendant's mental state; and (3) the type of resulting harm.[114] Thus, the first step in the development of a wrongful acquisition tort requires that the bad acts of the defendant be defined. With respect to other types of information torts, including trade secret law, the bad acts relate directly to the existence of a property-like right.[115] And, as explained in *Demetriades v. Kaufmann*, the property right exists independently and at the inception of the wrongful acquisition; it is not created by the mere taking of the information itself.[116]

The foregoing suggests that one means of fashioning a wrongful acquisition tort for information that is not otherwise protected by law is to expand the definition of protectable information to include all forms of information held by an individual or company.[117] The problem with this approach, however, is that it would be inconsistent with the important policy choices that have already been made concerning the protection and dissemination of information.[118] It would also be inconsistent with the desire to rid the law of the hodge-podge of information-related claims that existed at common law and was a principal motivating factor behind the enactment of the UTSA,

---

113. *See, e.g.*, *id.* at 1014.
114. DAN B. DOBBS ET AL., THE LAW OF TORTS §§1–2 (2d ed. 2011).
115. *See supra* note 29.
116. Demetriades v. Kaufmann, 698 F. Supp. 521, 527–28 (S.D.N.Y. 1988).
117. *Id.*
118. *See supra* Section II.

explaining why section 7 of the UTSA was adopted to preclude all pre-existing tort and equitable claims related to the misappropriation of "competitively significant" information.[119] Moreover, recognizing property-like rights with respect to wide swaths of information would likely quell the use of information that is part of the public domain and is inconsistent with the rejection of the "sweat of the brow" doctrine in the United States.[120] Additionally, while such an approach might be welcomed by database owners that have their information taken, it would be unwelcomed when they are sued for allowing the hacking of the customer information they hold. Currently, database owners benefit from the limits that are placed upon their potential liability by the very tort principles that make recognition of a wrongful acquisition tort difficult.[121]

Ordinarily, when new torts are developed to address gaps in existing law, different or additional elements are added so that the new tort is not simply a lesser included tort with fewer elements to be proven.[122] Instead, the missing element is replaced with another and more exacting element.[123] Consider, for instance, the torts of conversion and trespass to chattels: although both concern interferences with personal property, they have different required elements with the "lesser" tort of trespass to chattel having a more exacting element of harm.[124] Another example is the tort of "misappropriation" as defined in

---

119. UNIF. TRADE SECRETS ACT WITH 1985 AMENDMENTS § 7 cmt. (UNIF. LAW COMM'N 1985). But note that not all UTSA states have enacted section 7 as is worded in the UTSA.

120. Feist Publications, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 353 (1991) ("The 'sweat of the brow' doctrine had numerous flaws, the most glaring being that it extended copyright protection in a compilation beyond selection and arrangement—the compiler's original contributions—to the facts themselves.").

121. *See* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 275 (2005) (discussing how the lack of a relationship between database owners and the individuals whose data is contained in the databases limits tort liability).

122. *See generally* Int'l News Serv. v. Associated Press, 248 U.S. 215, 234–35 (1918) (explaining that there was a need for a new theory of wrongdoing and using unfair competition law as a basis for devising the new theory); Intel Corp. v. Hamidi, 71 P.3d 296, 302–03 (Cal. 2003) (explaining that the torts of trespass to chattels and conversion have similar elements but are also different in that a trespass to chattels has a more demanding requirement for harm).

123. *See Intel*, 71 P.3d at 302–03.

124. *See id.* at 302 (comparing the two torts—trespass to chattel and conversion—and quoting Prosser who called trespass to chattel the "little brother of conversion").

International News Service v. Associated Press.[125] In that case, the Supreme Court, sitting in equity, devised a theory of wrongdoing that did not alter the policy concerning the freedom to use public information, but still provided a remedy for what the Court perceived as improper behavior.[126] The Court did this by focusing on the unfair competition aspects of defendant's behavior, defining the defendant's acts as "taking" the material of complainant "and selling it as its own."[127] The wrong was acquiring the plaintiff's time-sensitive information for the specific purpose of re-selling it in competition with the complainant, coupled with misrepresenting the source of the information.[128] The reasoning of *Christopher* has a similar, but perhaps unappreciated, structure: the court defined the wrong as "industrial espionage" with an intent to acquire the information for the specific purpose of sharing it with a third-party.[129] For a wrongful acquisition tort that is separate from a trade secret claim, what would substitute for the missing property-like interest?

Of course, courts and lawmakers could be direct and intentional about defining the required wrongful acts, state of mind, and harms of a wrongful acquisition tort so that they are sufficiently robust to substitute for the usual requirement of protectable information. But a question for policymakers is: How precise should the tort be in defining the required wrongful behavior? Currently, at least under the principles expressed in *International News Service* and *Christopher*, courts have some leeway to decide what constitutes "unfair competition" and "the standard of morality expected in our commercial relationships," but these are malleable standards that would not be appropriate for a claim which would not involve information that is otherwise protected by law.[130] Under the existing information torts, including trade secret law, the existence of an identifiable

---

125. *See Int'l News Serv.*, 248 U.S. at 241. Although the "hot news" tort continues to be discussed in information law circles, arguably, it was effectively overruled by the U.S. Supreme Court's subsequent decision in Erie Railroad Co. v. Tompkins, 304 U.S. 64 (1938).

126. *Int'l News Serv.*, 248 U.S. at 241.

127. *Id.* at 231.

128. *Id.* at 230–31.

129. E. I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970), *cert denied*, 400 U.S. 1024 (1971).

130. *See Christopher*, 431 F.2d at 1015–16; *Int'l News Serv.*, 248 U.S. at 234–35.

property right is an important grounding principle.[131] Without it, other, more precise, concepts of wrongdoing are needed.[132] When balanced against the strong public interest in the diffusion of non-confidential information, including the importance of information diffusion in the development of knowledge and innovation, it seems that making the wrongful acquisition tort an intentional tort that requires specific behaviors would be the best course of action, if such a tort is created at all.

An example of this approach is provided in the EU Database Directive which defines a wrong that goes beyond the mere acquisition of protected data to require the "extraction and/or re-utilization of the whole or a substantial part" of a qualifying database.[133] In keeping with this approach, the required bad acts of a wrongful acquisition tort might require specific "bad" behaviors. For instance, the requisite bad acts might be defined by reference to existing crimes or torts. This is consistent with the part of the definition of "improper means" under the UTSA and DTSA which refers to specific tortious and criminal behaviors,[134] but since a wrongful acquisition tort would be disconnected from an existing property interest, something more should be required, like a heightened intent or harm requirement.

Every tort claim includes a required mental state, ranging from the specific to the general, that helps determine and define the culpability of an actor.[135] Even in cases where strict liability

---

131. *See generally* Claeys, *supra* note 58.

132. *E.g.*, Database Directive, *supra* note 10, art. 7 (giving an example a precise concept of wrongdoing in re-utilizing of at least a majority of a database).

133. *Id.*

134. 18 U.S.C. § 1839(5)(A) (2012); UNIF. TRADE SECRETS ACT WITH 1985 AMENDMENTS § 1 (UNIF. LAW COMM'N 1985).

135. *See* DOBBS ET AL., *supra* note 114, § 2 (categorizing torts as intentional, or negligent, while noting that some courts recognize a category of tort between intentional and negligent, referred to as "willful or wanton"). Intentional and willful or wanton torts clearly implicate a mental state. *Id.* (indicating that these categories require at least awareness of the act). Even negligent torts, which do not require tortfeasors to be subjectively aware that their conduct is creating unreasonable risk, *see id.*, require some degree of culpability. *See, e.g.*, Breunig v. Am. Family Ins. Co., 173 N.W.2d 619, 623 (Wis. 1970) (recognizing that a person cannot be liable in negligence for loss of consciousness while driving if that loss of consciousness resulted from forces that were "not attended with sufficient warning or should not have been reasonably foreseen"). *See generally Tort*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/tort (last visited Jan. 27, 2018) (giving examples of the elements of a number of torts, which show that some type of mental intent is required).

is imposed, there is at least the required mental state of engaging in the activity to which strict liability attaches.[136] Thus, for instance, although both patent and copyright law do not require proof that the defendant intended to infringe the plaintiff's rights, they do require proof that the defendant volitionally engaged in infringing behavior.[137] Requiring a more exacting and specific mental state of the defendant in a wrongful acquisition case would be one way to create balance where a wrongful acquisition tort is defined so as not to require a protectable property interest. It is also consistent with the rhetoric surrounding cyber-hacking, which seems to assume that all cyber-hackers are acting with evil intent.[138] If it is bad acts coupled with evil intent that is at the heart of the concerns about cyber-hacking and other forms of wrongful acquisition, then we should require both if designing a separate wrongful acquisition tort.

The critical question with respect to an intent requirement is: what degree of knowledge or intent by the defendant should be required? In the case of U.S. trade secret law, liability is conditioned on proof that the defendant knew or had reason to know of the existence of trade secrets and the act of misappropriation.[139] To substitute for a missing property right, a wrongful acquisition tort should require a more demanding type of knowledge or intent. This is the approach taken by the CFAA which, in part, defines the required wrongdoing as: "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby

---

136. *See* DOBBS ET AL., *supra* note 114, § 437 (stating that strict liability rests on a defendant's creation or introduction of some abnormally dangerous condition, thus suggesting the defendant must choose, on some level to engage in behavior creating that abnormal risk).

137. *See* 35 U.S.C. § 271(a) (2012) (describing patent infringing acts as "mak[ing], us[ing], offer[ing] to sell, or sell[ing]" a patented invention without permission—all volitional acts); Peter Keros, *Volitional Conduct: An Element of Copyright Infringement*, BEJIN BIENEMAN: THE SOFTWARE IP REP. (Feb. 21, 2017), https://www.b2ipreport.com/swip-report/volitional-conduct-an-element-of-copyright-infringement/ (citing a recent case that supported the proposition that volitional conduct is required for copyright infringement).

138. *See generally* Paul Gil, *What Are 'Black Hat' and 'White Hat' Hackers?*, LIFEWIRE (Jan. 22, 2018), https://www.lifewire.com/black-hat-hacker-a-white-hat-hacker-4061415 (explaining that 'black hat' hackers are the hackers we view as having evil intentions when performing hacking online).

139. UNIF. TRADE SECRETS ACT WITH 1985 AMENDMENTS § 1(2) (UNIF. LAW COMM'N 1985).

obtain[ing] . . . information from any protected computer" or "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and . . . further[ing] the intended fraud and obtain[ing] anything of value."[140] Both *INS* and *Christopher* provide some guidance on a state of mind requirement because of the courts' reference to the purposes for which the defendants engaged in the challenged behaviors.[141] So too the common law tort specified in *Restatement (First) of Torts*, which required that the defendant act "for the purpose of advancing a rival business interest."[142] The problem with the purposes defined in those sources, however, is that they tread close to the purpose of engaging in robust competition, which numerous cases have held is appropriate behavior in a free market economy.[143] This is particularly true with respect to information that has been publicly disclosed. Businesses frequently acquire information about their rivals, and it is not improper or morally wrong to use such information to compete with a rival, so long as the information is not otherwise protected by law.[144]

The required bad acts of wrongful acquisition, either a tort or a crime, may include intent requirements that could be incorporated into a wrongful acquisition tort, requiring the same proof of intent as is required for the subject tort or crime. Short of this approach, if wrongful acquisition can be established upon proof of an act not amounting to a tort or crime (the *Christopher* scenario), an intent to engage in the wrongful acquisition for a very specific purpose, such as harming the information owner or its customers, might be required. This would limit potential liability for the acts of those who access non-protected information for their personal, non-commercial, or

---

140. 18 U.S.C. § 1030(a)(2), (4) (2012).

141. *See* E. I. duPont deNemours & Co. v Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970), *cert. denied*, 400 U.S. 1024 (1971) ("[T]he Christophers deliberately flew over the DuPont plant to get pictures of a process which DuPont had attempted to keep secret. The Christophers delivered their pictures to a third party who was certainly aware of the means by which they had been acquired . . . .").

142. RESTATEMENT (FIRST) OF TORTS § 759 (AM. LAW INST. 1939).

143. *See generally* N. Pac. Ry. Co. v. United States, 356 U.S. 1 (1958); Berkey Photo, Inc. v. Eastman Kodak Co., 603 F.2d 263, 272 (2d Cir. 1979).

144. *See generally* Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 144–46 (1989); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 (AM. LAW INST. 1995).

whistleblowing uses and would be consistent with notions of "fair use" under U.S. copyright law.[145] Additionally, because much of the information that today's businesses collect and store does not originate with them and is not owned by them (because it was gleaned from public sources or collected from their customers),[146] a mental state requirement should require something more than the defendant's intent to acquire information held by another. Like the improper procurement tort of Section 759 of the *Restatement (First) of Torts*, a wrongful acquisition tort might require the acquisition of identifiable holder-generated information for the specific purpose of establishing a competing database. Or, analogizing to the crime of burglary, it might require the entering into a computer system with a specific intent to engage in additional wrongful behavior.

Failing to get the state of mind element right could result in a wrongful acquisition tort that is over- or under-inclusive; under-inclusive in that it does not provide a remedy for bad behavior that society wishes to deter, or over-inclusive for providing a remedy for behavior that was engaged in without culpable intent, for instance for a beneficial or altruistic purpose. The CFAA has been criticized for being unclear and not getting the balance right.[147] One problem with the language of the CFAA is that it is often difficult for users of computers to know when their authorization to access and use information begins and when it ends because they never read the limitations that are embedded in lengthy employment agreements or terms of use agreements or because those limitations are written in

---

145. *See* 17 U.S.C. § 107 (2012) (explaining the factors that determine fair use).

146. *See* Andrew McAfee & Erik Brynjolfsson, *Big Data: The Management Revolution*, HARV. BUS. REV., Oct. 2012, https://hbr.org/2012/10/big-data-the-management-revolution.

147. *See, e.g.*, Lee Goldman, *Interpreting the Computer Fraud and Abuse Act*, 13 PITT. J. TECH. L. & POL'Y 1, 15–19 (2012); Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1563–71 (2010); Note, *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 HARV. L. REV. 751 (2013); Andrew Trombly, *Right for the Wrong Reasons: The Ninth Circuit Excludes Misappropriation from the CFAA's Ambit in* United States v. Nosal, 54 B.C.L. REV. E-SUPPLEMENT 129, 140 (2013); Garrett D. Urban, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 WM. & MARY L. REV. 1369, 1373 (2011).

ambiguous language.[148] However, for torts and crimes to act as deterrents (presumably, the chief purpose of a wrongful acquisition tort), individuals and companies should be able to discern the required intent and prohibited behaviors. Additionally, where such behaviors hew too closely to desired behaviors, particularly the collection, dissemination, and use of publicly available information, we should err on the side of limiting potential liability.

Under longstanding principles of tort law, ordinarily there can be no tort recovery without a wrongful act that causes cognizable injury. Yet, the focus of much of the rhetoric about the wrongful acquisition of information, particularly cyber-hacking, relates to the act of acquiring information, and not on any resulting harm.[149] Ironically, the absence of cognizable harm is the argument that defendants in data breach litigation often use to avoid liability to their customers, arguing that the mere hacking and holding of information by the wrongdoers is not a cognizable harm.[150] As the Court explained in *Spokeo*: "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'"[151] Thus, defendants in data breach cases understand that the cognizable harm requirement of tort theory has the effect of reducing the number of lawsuits that are brought since, even though someone may have engaged in otherwise-tortious behavior, no recovery will be granted unless the plaintiff suffered actual harm.

---

148. *See* United States v. Nosal, 676 F.3d 854, 860 (9th Cir. 2012) ("Significant notice problems arise if we allow criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read.").

149. *See, e.g.*, Kwikset Corp. v. Superior Court, 246 P.3d 877 (Cal. 2011) (overturning *Silvaco*'s decision confining standing under Cal. Bus. & Prof. Code § 17204 to those who are eligible for restitution); Silvaco Data Sys. v. Intel Corp., 109 Cal. Rptr. 3d 27, 56 (Cal. Ct. App. 2010) (assuming harm, for purposes of federal standing doctrine, satisfied by impeding further use, but requiring a plaintiff to show eligibility for restitution in order to establish standing under California law).

150. *See* Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 366–67 (M.D. Pa. 2015); *see also* Whalen v. Michael Stores Inc., 153 F. Supp. 3d 577, 577–78 (E.D.N.Y. 2015).

151. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016) (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)).

While harm is always a required element of a tort, sometimes the tort defines the harm, as is the case with false imprisonment (wherein the harm is the very confinement that is also the tortious wrong); the principal issue being the dollar value associated with the emotional distress and lost time associated with the confinement.[152] Similarly, the development of causes of action designed to protect information, including copyright and trade secret law, did not ignore the essential requirement that the defendant's actions cause cognizable harm. Instead, they broadened how harm could be conceived and measured and provided non-monetary remedies to prevent threatened harm.[153] Thus, for instance, trade secret law under both the UTSA and DTSA allows for injunctive relief even in the absence of actual harm if it can be shown that there is a threatened disclosure or use of the subject trade secrets.[154] Where a trade secret claimant wishes to recover monetary damages, actual harm must be proven, but pursuant to statutorily defined measures of damages that are broader than what was allowed under common law.[155] Conceivably, the same approach could be followed with respect to a wrongful acquisition tort, but any measure of damage typically relates to some actual effect upon the defendant.[156]

Typically, the harm associated with information torts relates directly to the property nature of the information, with the harm measured by the loss of income that could have been derived from authorizing use of the property, the unjust enrichment derived by the defendant from using the information, or, in the case of trade secrets, by the loss of the property rights themselves.[157] A theory of trespass that would

---

152. *See generally* BARRY A. LINDAHL, MODERN TORT LAW: LIABILITY AND LITIGATION § 41:3 (2d ed., 2017).

153. *See* R. Clifton Merrell, *Trespass to Chattels in the Age of the Internet*, 80 WASH. UNIV. L. REV. 675, 679 (2002).

154. Sharon K. Sandeen & Christopher B. Seaman, *Toward a Federal Jurisprudence of Trade Secret Law*, 32 BERK. TECH. L.J. 829, 900–02 (2018) (describing differences between the remedies provisions of the UTSA and DTSA with respect to the scope of available injunctive relief).

155. Defend Trade Secrets Act of 2016, 18 U.S.C. § 1836(b)(3)(B); UNIF. TRADE SECRETS ACT WITH 1985 AMENDMENTS § 3 (UNIF. LAW COMM'N 1985).

156. *See generally* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 (AM. LAW INST. 1995).

157. *See, e.g.*, NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 158 (2015) ("All of these 'informational torts'

give rise to, at least, nominal damages, is not a feature of information laws.[158] This limitation means that the use of a trade secret law to deter cyber-hacking is sub-optimal because there is too much beyond the act of hacking (misappropriation) that must be proven for relief to be granted.[159] However, if a *sui generis* wrongful acquisition tort is created to provide a claim for relief without proof of a protectable property interest, the requirement of a cognizable harm becomes even more important.

The CFAA provides a potential model, but one that does not make the element of harm more exacting than it is under common law or the expanded remedies provisions of other information torts. Instead, the CFAA is remarkable for not only *not* requiring that the subject information be within a legally protected class of information, such as trade secret or even confidential and proprietary information, but for defining possible harms broadly.[160] According to the CFAA, "damage" means "*any* impairment to the integrity or availability of data, a program, a system, or information."[161] Even more broadly, "loss" is defined to mean: "*[A]ny reasonable cost to any victim*, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[162] While this broad conception of harm was obviously designed to address the perceived bad acts of cyber-hacking, it can be criticized for not giving sufficient deference to the non-protectable status of some hacked information, as well as the strong public policy that favors information diffusion.

Finally, another policy lever that is available to courts and policymakers who wish to create a wrongful acquisition tort that appropriately balances the interests of the public and the

---

share some (but not all) of a relatively small number of elements, including . . . harm to emotions, harm to a property interest, or reliance on trust.").

158. *See* Merrell, *supra* note 153, at 677–87, 689 ("[T]respass to land does not requires harm and allows for nominal damages.").

159. *See, e.g.*, *id.* at 681 n.53 (discussing a situation in which the Washington Supreme Court "relied on a criminal statute prohibiting hacking, as opposed to a civil case of trespass based on common law," because of its limited applicability).

160. *See generally* 18 U.S.C. § 1030 (2012).

161. 18 U.S.C. § 1030(e)(8) (2012) (emphasis added).

162. 18 U.S.C. § 1030(e)(11) (2012) (emphasis added).

information holder relates to possible defenses. All defenses that currently exist with respect to other information-related torts should be considered, including the reverse engineering defense of trade secret law and the fair use defense of copyright law.[163] Indeed, it is such defenses which, in large part, prevent state information claims from conflicting too much with U.S. patent and copyright law and from being unconstitutional on First Amendment grounds. An additional defense may be fashioned relating to the nature and value of the information that was acquired, for instance, if the original source of the information was a public record. There is something odd and troubling about taxpayers paying for the collection and maintenance of public records, providing those public records to third-parties (usually for a modest price), and then paying for the enforcement of a third-party's alleged rights to such information. Thus, in designing a wrongful acquisition tort, its remedies, and its defenses, the original source and nature of the subject information should matter. This should particularly be the case if the originator of the information who provided the information to the person or entity from whom it was "wrongfully acquired" does not care if the information is shared.

V. CONCLUSION

It is possible to design a tort to deter acts of wrongful acquisition including cyber-hacking, but it is not easy. One reason for the difficulty is the need to distinguish such claims from existing information-related torts, such as copyright infringement and trade secret misappropriation, by adding extra elements to the proposed cause of action. Simply creating what amounts to a "lesser included" wrongful acquisition tort would risk undermining the balance between information protection and information diffusion that is reflected in existing U.S. patent, copyright, trade secret, and unfair competition law, and may be deemed preempted by federal patent and copyright law. Moreover, recognizing property-like rights with respect to wide swaths of information would likely quell the use of information that is part of the public domain and hamper invention and

163. *See, e.g.*, 17 U.S.C. § 107 (2017); UNIF. TRADE SECRETS ACT WITH 1985 AMENDMENTS § 1 cmt. (UNIF. LAW COMM'N 1985) (stating that reverse engineering is a "proper means" of acquiring a trade secret). *See generally* DOBBS ET AL., *supra* note 114, §§ 734–41 (discussing the requirements for a number of torts relating to unfair competition and intellectual property).

competition. As experience with the CFAA has shown, it is difficult to fashion laws to preclude the alleged wrongful acquisition of information without putting legitimate uses of information at risk. Thus, given the importance of the free-flow of information and knowledge to our society and economy, including it being the key to invention and creativity, it may be that we should simply learn to tolerate the gaps in the law that currently exist and instead enjoy the rewards that come from the dissemination and sharing of unprotected information. The fact that a robust wrongful acquisition (or misappropriation) tort has not already developed, even since *Christopher*, strongly suggests that such a policy choice has already been made.