Dumpster Diving and the Ethical Blindspot of Trade Secret Law

Harry Wingo†

"The maintenance of standards of commercial ethics and the encouragement of invention are the broadly stated policies behind trade secret law. 'The necessity of good faith and honest, fair dealing, is the very life and spirit of the commercial world.'"[1]

"The trilogy of public policies underlying trade secret laws are now: (1) the maintenance of commercial morality; (2) the encouragement of invention and innovation; and (3) the protection of the fundamental right of privacy of the trade secret owner."[2]

Trade secret law is complex and still emerging,[3] but throughout its

---

† B.S. U.S. Naval Academy 1984, J.D. Candidate, 1998, Yale Law School. The author wishes to thank Professor Carol Rose, Judge John F. Fader II, and Doug Lichtman for the advice, as well as Lt. Hope Katcharian for her patient support and inspiration.

1. Kewanee Oil v. Bicron, 416 U.S. 470, 481-82 (1974) (quoting National Tube Co. v. Eastern Tube Co., 3 Ohio C.C. (n.s.) 459, 462 (1902).

2. 1 MELVIN F. JAGER, TRADE SECRETS LAW § 1.05, at 1-15 (1997). The *Restatement (Third) of Unfair Competition* recognizes Mr. Jager as a trade secret law authority. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 reporter's notes at 438 ("The principal treatises on the law of trade secrets are M. Jager, Trade Secrets Law and R. Milgrim, Milgrim on Trade Secrets.").

3. This complexity and flux is underscored by the fact that a simple definition of trade secret remains elusive. *Cf.* American Wheel & Eng'g Co. v. Dana Molded Prods, Inc., 476 N.E.2d 1291, 1294 (Ill. App. Ct. 1985) (stating that trade secret definition is elusive "because it includes a wide spectrum of categories subject to variations depending upon the facts of a particular case"). The *Restatement (Third) of Unfair Competition* recently set forth the following comprehensive definition: "A trade secret is any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others." RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 3.03(2) (1995). Before the *Restatement*'s definition, the National Conference of Commissioners on Uniform State Laws commissioned its own definition:

> 'Trade Secret' means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

UNIF. TRADE SECRETS ACT ("UTSA"), 14 U.L.A. 369 (1997). The original version of the UTSA was approved in 1979, and an amended version was approved in 1985. *See* 14 U.L.A. 433 (1985). Despite the widespread adoption of the UTSA as a model for state trade secret statutes, *see* Christopher Rebel Pace, *The Case for a Federal Trade Secrets Act*, 8 HARV. J.L. & TECH. 427, 429 (1995), and the increasing citation of the *Restatement (Third) of Unfair Competition*, *see* Qualitex Co. v. Jacobson Prods. Co., 115 S. Ct. 1300 (1995); Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763 (1992), most courts still rely upon the widely-recognized trade secret definition found in the 1939 *Restatement of Torts*. *See* 1 JAGER, *supra* note 2, § 3.01, at 3-41; MILGRIM ON TRADE SECRETS § 1.01, at 1-3 (1997);

development, trade secret law has consistently promoted minimum standards of commercial ethics.[4] Indeed, promoting commercial ethics is one of trade secret law's fundamental purposes.[5] Consistent with this ethical purpose, trade secret law proscribes the use of improper means[6] to acquire another's trade secrets.[7] Improper means of acquiring trade secrets include familiar methods of industrial espionage, such as wiretapping and eavesdropping,[8] as well as methods that are not so familiar, like aerial surveillance.[9]

However, one simple yet highly effective method of industrial espionage—dumpster diving[10]—is not consistently recognized by courts as an improper means of obtaining trade secrets. As a result, a dumpster diving victim faces the burden of demonstrating that even though her alleged trade secret was in the trash, its secrecy was nonetheless "reasonably" protected.

Note, *Trade Secret Misappropriation: A Cost-Benefit Response to the Fourth Amendment Analogy*, 106 HARV. L. REV. 461, 462 (1992); *see also* William E. Hilton, *What Sort of Improper Conduct Constitutes Misappropriation of a Trade Secret*, 30 IDEA 287, 288 (1990) ("[A] review of trade secret cases reveals that few courts rely on the [state] statutes for authority and most prefer to cite the Restatement of Torts from 1939."). The *Restatement of Torts* defines a trade secret as consisting of "any formula, pattern, device or compilation of information which is used in one's business, and which gives [one] an opportunity to obtain an advantage over competitors who do not know or use it." RESTATEMENT OF TORTS § 757 cmt. b (1939). It further warns that "[a]n exact definition of a trade secret is not possible." *Id.*

4. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. a (1995); 1 JAGER, *supra* note 2, § 1.03, at 1-7 ("The concern for business morality has been a constant theme as the common law of trade secrets has developed in the United States over the last century.").

5. *See supra* text accompanying notes 1 & 2; 1 JAGER *supra* note 2, § 1.02, at 1-7 ("The encouragement of increasingly higher standards of fairness and commercial morality, as noted in *Kewanee*, continues to be the touchstone of trade secret law in the courts.").

6. *See* RESTATEMENT OF TORTS § 757 cmt. f (1939); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 (1995). Proper means of acquiring trade secrets are independent discovery and analysis of publicly available products or information, otherwise known as "reverse engineering." *Id.*

7. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 (1995).

8. *See* Comment, *Corporate Privacy: A Remedy for the Victim of Industrial Espionage*, 1971 DUKE L.J. 391, 398 n.43 ("Eavesdropping was, at any rate, a crime itself at common law.").

9. *See E.I. DuPont deNemours & Co. v. Christopher*, 431 F.2d 1012 (5th Cir. 1970). For a discussion of this case, see *infra* text accompanying note 102. Other improper means include bribery, breach of confidence, and fraud. *Cf. Comment*, *supra* note 8, at 404.

10. As used in this Note, "dumpster diving" refers to clandestine trash searches conducted for the sole purpose of obtaining trade secrets. *See* James M. Atkinson, *Ten Spy-Busting Secrets (The Top 10 Spy-Busting Tips the Snoops Don't Want You To Know)* (visited Dec. 15, 1997) <http://www.tscm.com/murray.html> (*"#1—Trash Trawling* Dumpster diving, waste archeology, or trashing, all refer to rifling garbage in an effort to cull valuable information. This is believed to be the number one method of business and personal espionage . . . . Surprise! In and of itself, stealing garbage is legal."). Outside of the trade secret context, dumpster diving can refer to a broad range of activities. The ranks of harmless dumpster divers include homeless persons seeking food scraps and college students searching for old furniture. *See* JOHN HOFFMAN, THE ART AND SCIENCE OF DUMPSTER DIVING (1993). Harmful dumpster divers include credit card thieves, *see* Ken Fisher, *Cashier Helps Crack Credit Card Scam; Police Say Man Got Cards in Names of Other People*, PITT. POST-GAZETTE, Sept. 12, 1996, at W1 (discussing statement of U.S. Postal Inspector John Wisniewski, Credit Card Task Force Coordinator); *see also Credit Card Scam Spurs Search of Teens' Homes*, HARTFORD COURANT, Sept. 7, 1996, at B3, and paparazzi who engage in invasive searches, *see* California v. Greenwood, 486 U.S. 35, 51-52 (1988) (Brennan, J., dissenting) ("When a tabloid reporter examined then-Secretary of State Henry Kissinger's trash and published his findings, Kissinger was 'really revolted' by the intrusion and his wife suffered 'grave anguish.'").

The weight of this burden becomes nearly insurmountable considering the need to overcome the judicial presumption set forth by the Supreme Court in *California v. Greenwood*,[11] that there is no reasonable expectation of privacy in trash (the "*Greenwood* presumption"). In *Frank W. Winne & Son v. Palmer*,[12] a U.S. district court relied on the *Greenwood* presumption to hold that trade secrets placed in the trash in discernible form are not legally protected (the "*Winne* rationale").[13]

This Note argues that the *Winne* rationale undermines trade secret law's fundamental purpose of promoting commercial ethics[14] by denying protection from predatory trash searches that clearly "fall below the generally accepted standards of commercial morality and reasonable conduct."[15] Part I of this Note discusses the threat posed by dumpster divers and the availability of private security measures. Part II first demonstrates that since most legislatures have not specifically classified dumpster diving as an improper means, courts are likely to fixate on the victim's secrecy precautions[16] but neglect to

---

11. 486 U.S. 35 (1988) (holding that the Fourth Amendment does not prohibit the warrantless search and seizure of garbage left for collection outside the curtilage of a home).

12. No. 91-2239, 1991 U.S. Dist. LEXIS 11183, at *1 (E.D. Pa. Aug. 7, 1991); *see infra* text accompanying note 78.

13. The rationale by which the *Winne* court incorporated the *Greenwood* presumption into trade secret law has been called the Fourth Amendment analogy. *See infra* note 61 and accompanying text.

14. This purpose is the first of what Melvin F. Jager has called the "trilogy of public policies underlying trade secret laws." *See* 1 JAGER *supra* note 2 and accompanying text.

15. RESTATEMENT OF TORTS § 757 cmt. f (1939). The *Winne* rationale also offends two more of the "trilogy" of public policies underlying trade secret law: the encouragement of innovation and the protection of privacy. *See* 1 JAGER *supra* note 2. The rationale undermines innovation by forcing trade secret owners to devote valuable resources to prevent industrial spies from siphoning off the fruits of costly research and development. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. a (1995) ("More recently, the protection of trade secrets has been justified as a means to encourage investment in research by providing an opportunity to capture the returns from successful innovations."); Comment, *Dead or Alive?: The Misappropriation Doctrine Resurrected in Texas*, 33 HOUS. L. REV. 447, 471-72 n.214 and accompanying text (1996) ("Businesses, unable to discern when a court will consider certain competition unfair, are less likely to compete zealously, slowing down the rate of progress in the business industry."). The *Winne* rationale condones implicitly the violation of the privacy interests of trade secret owners, interests that were recognized in *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141, 155 (1989) ("Finally, certain aspect of trade secret law operated to protect *non-economic* interests outside the sphere of congressional concern in the patent laws. As the Court noted: [a] *most fundamental human right, that of privacy*, is threatened when industrial espionage is condoned or is made profitable.") (citing Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1973)). Trade secret law and privacy interests have been linked in several contexts. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 213 (1890) (arguing that trade secret law embodies natural conceptions of privacy). *But see* Note, *supra* note 3, at 465 (remarking critically that "references to privacy rights in trade secret cases have enticed judges and commentators alike to delve into the law's largest font of privacy jurisprudence—the constitutional protection against unreasonable search and seizure"). The remedies available to trade secret owners who are victimized by industrial espionage might be bolstered by the further development of the right of privacy rationale. *Cf. Corporate Privacy*, *supra* note 8, at 391.

16. *See generally* David W. Slaby et al., *Trade Secret Protection: An Analysis of the Concept "Efforts Reasonable Under the Circumstances to Maintain Secrecy,"* 5 SANTA CLARA COMPUTER & HIGH TECH. L.J. 321 (1989) (discussing the requirements necessary to comply with the secrecy requirements of trade secret law and demonstrating how to develop an effective protection program using a cost-benefit analysis).

carefully examine the propriety of dumpster diving. Part II then discusses the use of the so-called Fourth Amendment analogy to determine the reasonableness of secrecy precautions in two dumpster diving cases, *Tennant Co. v. Advance Machine Co.*,[17] which condemned dumpster diving, and *Frank W. Winne & Son, Inc. v. Palmer*,[18] which allowed it. Part III criticizes the *Winne* rationale for relying on an outdated notion of the nature and value of trash, and for failing to distinguish trash searches by accountable public officials from those conducted by self-interested business competitors. Part IV discusses a second approach, the cost-benefit approach suggested by *E.I. DuPont deNemours & Co. v. Christopher*, 431 F.2d 1012 (5th Cir. 1970), which involved surveillance that, though legal on its face, was nonetheless held to be an improper means of obtaining trade secrets. Part V argues that both the Fourth Amendment analogy and the cost-benefit framework inadequately address trade secret law's purpose of promoting commercial ethics, and advocates the adopting a combined *Tennant* and cost-benefit test that also carefully considers the ethicality of dumpster diving. Part VI briefly highlights two recent reforms: Connecticut's classification of dumpster diving as a form of espionage ("Connecticut solution"),[19] and the Economic Espionage Act ("EEA").[20] This Note concludes that comprehensive reform requires legislatures to designate dumpster diving as an improper means, and courts to consider dumpster diving within an analytical framework that carefully weighs each of the three fundamental public policies underlying trade secret law: commercial morality, the encouragement of innovation, and the protection of privacy. The synthesis of these three fundamental concerns into the continually developing common law of trade secrets should yield more just and predictable decisions in cases involving all forms of industrial espionage, not only dumpster diving.

I. DUMPSTER DIVING AND INDUSTRIAL ESPIONAGE

A. *The Threat*

"The level of sophistication of espionage operations directed against U.S. companies is extraordinary. American companies are like innocent children in

17. 355 N.W.2d 720 (Minn. Ct. App. 1984).

18. No. 91-2239, 1991 U.S. Dist. LEXIS 11183 (E.D. Pa. Aug. 7, 1991).

19. *See* CONN. GEN. STAT. § 35-51, *as amended by* Pub. Act No. 97-110. The author of this Note proposed the original bill and testified on its behalf before the Connecticut Judiciary Committee. *See* Thomas Scheffey, *The Legal Spawning Ground*, CONN. LAW TRIB. (Mar. 31, 1997) NEWS at 1.

20. 18 U.S.C. § 1831-1839, *enacting* P.L. 104-294 (Oct. 11, 1996); S. Rep. No. 104-359 (1996). The EEA is the first federal statute that directly addresses misappropriation of trade secrets. *See* Chaim A. Levin, *Economic Espionage Act: A Whole New Ball Game*, N.Y. L.J., Jan. 2, 1997, at 5 (outlining the provisions and effect of the new law).

the forest. They have no idea how many wolves are after them."[21]

Dumpster diving is part of a larger industrial espionage problem that costs U.S. businesses billions of dollars each year.[22] As the relative importance of intellectual property with respect to other corporate assets has increased, so has information piracy. A survey of 325 U.S.-based companies by the American Society for Industrial Security (ASIS) revealed that between 1992 and 1995, breaches of corporate security climbed by 323%.[23] And those were just the reported breaches—corporate victims are often silent about successful raids against their intellectual property.[24] Considering undetected and unreported thefts, ASIS estimates that U.S. industry loses two billion dollars per month to intellectual property pirates.[25] This figure is alarming since proprietary knowledge makes up more than half of a typical manufacturer's total market value.[26] Accordingly, industrial espionage, especially when conducted by foreign governments,[27] seriously threatens our nation's economic well-

---

21. Reinhard Vogler, former East German intelligence officer. Mr. Vogler is based in Berlin and advises multinational companies on economic espionage. *See* Ronald E. Yates, *Corporate Cloak and Dagger: Spying—Either by Rival Businesses or Foreign Governments—Can Cut Right to the Heart of a Vulnerable Corporation, But Congress Is Considering Ways To Strike Back*, CHI. TRIB., Sept. 1, 1996, at C1.

22. *See* Alan Farnham & Jeanne C. Lee, *How Safe Are Your Secrets?: In the Infotech Age They're Less Safe Than You Think. Now a New Law Protects Them—But Watch Out. If You Learn Another Company's Trade Secrets, Even Inadvertently, It Can Land You in Jail*, FORTUNE, Sept. 8, 1997, at 114 ("FBI director Louis Freeh says more than $24 billion a year in proprietary information is being pinched."). Concern about trade secret law's inability to deal adequately with industrial espionage is not new. *See* Comment, *Theft of Trade Secrets: The Need for a Statutory Solution*, 120 U. PA. L. REV. 378, 401 (1971) [hereinafter *Statutory Solution*] ("[I]nvestments in technological progress, coupled with ever more rapid obsolescence, have led to an increased reliance on trade secrets and know-how licensing on a national and international scale, and a corresponding rise in industrial espionage. The present patchwork of confused common law doctrines and state criminal statutes is inadequate to protect the first and prevent the second.").

23. This represents an increase from about 10 breaches per month to 32. *See* H. Garrett DeYoung, *Thieves Among Us: If Knowledge Is Your Most Important Asset, Why Is It So Easily Stolen?*, INDUSTRY WEEK, June 17, 1996, at 12. One quarter of these breaches did not involve company insiders. *Id.*

24. *See* Levin, *supra* note 20 ("Moreover, in certain larger disputes, the negative public relations resulting from an admission to the loss of valuable trade secrets, or of interference with proprietary technologies, make litigation wholly undesirable.").

25. *See id.*; *cf.* 1 JAGER, *supra* note 2, § 1.03 at 1-8 n.23 (stating that in 1978 trade secret thefts in the U.S. were estimated to cost $4 billion annually).

26. *See* John Brandt, *Theft in (Your) Office*, INDUSTRY WEEK, June 17, 1996, at 6; *see also* DeYoung, *supra* note 23.

27. Foreign intelligence agents, like those of France's *Direction Generale de la Securite*, actively target American companies. *See* Roderick P. Deighen, *Welcome to Cold War II*, CHIEF EXECUTIVE, Jan. 1993, at 42; Farnham & Lee, *supra* note 22 ("The FBI reports that 23 foreign governments are systematically vacuuming U.S. corporations of their intellectual assets."); Ronald J. Ostrow & Paul Richter, *Economic Espionage Poses Major Peril to U.S. Interests*, L.A. TIMES, Sept. 28, 1991, at A1. In July, 1991, a French consular officer was spotted dumpster diving outside the house of a high-tech industry executive in Houston, Texas. *See* Jeff Augustini, *From Goldfinger to Butterfinger: The Legal and Policy Issues Surrounding Proposals to Use the CIA for Economic Espionage*, 26 LAW & POL'Y INT'L BUS. 459 (Jan. 1995).

being.[28] Unfortunately, U.S. businesses have been slow to defend properly themselves against the threat of foreign industrial espionage.[29] By one estimate, fewer than 5% of U.S. companies have a business counterintelligence system in place, as compared with close to 100% of all Japanese companies.[30]

Trade secrets are a primary target of industrial spies, a fact reflected in both the growing number of trade secret misappropriation cases,[31] and Congress' enactment of the EEA.[32] But in their efforts to address the threat of industrial espionage, courts and legislatures have generally overlooked one pervasive method of industrial espionage: dumpster diving.

Dumpster diving is one of the easiest and safest ways of gathering confidential information,[33] and yields secrets ranging from corporate executives' travel itineraries to descriptions of company merger plans.[34] The predatory nature of dumpster diving is demonstrated by the case of an international shipping company that got started by dumpster diving for the telex spools of an established company, then used customer lists on the spools to lure away clients.[35] As the value of intangible information rises exponentially, so too does the sophistication of modern day trash pickers. Some companies even specialize in combing trash for valuable items and information,[36] and may privately contract with trash collectors to obtain "recycled" computer paper and whatever is printed on it.[37] While dumpster diving may not always yield trade secrets directly, sophisticated corporate spies employ trash searches as part of larger collection campaigns. Indeed, one security expert believes that dumpster

---

28. *See* DeYoung, *supra* note 23; *cf.* Rockwell Graphic Sys. v. DEV Indus., 925 F.2d 174, 180 (7th Cir. 1991) ("The *future of the nation* depends in no small part on the efficiency of industry and the efficiency of industry depends on no small part on the protection of intellectual property.") (emphasis added).

29. While businesses should be encouraged to take more precautions, denying trade secret owners legal remedies against dumpster diving is not the best way to do so. *See supra* text accompanying note 10.

30. *See* Yates, *supra* note 21.

31. A Circuit Court Judge for Baltimore County, Maryland remarked that "[i]n the past three to five years these [trade secret misappropriation] cases have been coming out of our ears." Telephone Interview with John F. Fader, II, Circuit Court Judge for Baltimore County (Jan. 2, 1997); *see also Rockwell Graphic Sys.*, 925 F.2d at 180 ("This is an important case because trade secret protection is an important part of intellectual property, a form of property that is of growing importance to the competitiveness of American industry."); Levin, *supra* note 20 ("The volume of trade secret misappropriation disputes has taxed many courts.").

32. *See* 18 U.S.C. §§ 1831-1839, *enacting* P.L. 104-294 (Oct. 11, 1996); *supra* note 20, 131 and *infra* Section VI.B.

33. *See* Atkinson, *supra* note 10 ("[Dumpster diving] is believed to be the number one method of business and personal espionage.").

34. *See* DeYoung, *supra* note 23.

35. *See* Zachary Coile, *Better Shred Than Read*, S.F. EXAM., Aug. 29, 1994, at D1.

36. *See* Novell, Inc. v. Weird Stuff, Inc., No. C92-20467 JW/EAI, 1993 U.S. Dist. LEXIS 6674, at *5 (N.D. Cal. May 14, 1993) (noting that the defendant's business of salvaging and reselling discarded software literally involved diving into dumpsters); Coile, *supra* note 35.

37. DeYoung, *supra* note 23.

diving is the most common form of industrial espionage.[38]

B. *Available Private Security Measures*

"Ever since 1988 when the Supreme Court ruled that trash is public domain, simply tearing up and throwing away important documentation is not enough."[39]

Available market solutions to the dumpster diving threat include heightened physical security (e.g., fences, locks, and security guards) and thorough trade secret disposal (through the use of paper shredders or incinerators). While physical security measures such as fences and locks thwart dumpster diving by limiting access to trash, these methods may not be possible if the trade secret owner's trash bin is not located on her own property. Even if the trash bin is located on a trade secret owner's property, the trash within the bin will still be removed to a larger waste facility at some point, usually via a trash truck. During this transport phase, and until the trash becomes irreversibly commingled with other trash, the trade secret owner's physical security measures offer no protection. Accordingly, in the absence of laws prohibiting dumpster diving, a trade secret owner's protection during the post-dumpster phase of trade secret disposal depends on the extent to which her trade secrets have been rendered indiscernible.

To render trade secrets indiscernible, trade secret owners must turn to methods of trade secret disposal. Trade secrets requiring destruction are commonly found in the form of written documents, drawings or equations that may be stored on paper or in electronic form. Trade secrets that are stored electronically are more easily destroyed than those that are stored on paper (or microform). The former may be erased literally at the push of a button, but the latter require more deliberative and careful destruction.

Some trade secret owners may turn to recycling services for document destruction, but these services are a poor substitute given the prevalence of low-salaried workers and unsecured conditions in these services.[40] Furthermore, trash is often not shredded finely enough at recycling centers, and can be put together adequately enough to find numbers and other potentially harmful information. Worse still is the risk that the recycler may deliver the

38. *See* Atkinson, *supra* note 10 ("[Dumpster diving] is believed to be the number one method of business and personal espionage.").

39. Cut-Shred-Co Paper Shredder Consultants, *#1 in Paper Shredders* (Internet advertisement) (last modified Dec. 15, 1997) <http://www.cutshred.com>.

40. *See* Jeff Louderback, *Paper Chase: Every Business is Susceptible to Theft and Espionage and the Danger Lurks in the Places You'd Least Expect*, SMALL BUS. NEWS-DAYTON, Aug. 1996, at 6.

trade secret owner's trash directly to a competitor.[41]

Trade secret owners who choose to destroy their trade secrets that are fixed on paper increasingly use paper shredders to do so. Paper shredding solutions range from using small shredders as inexpensive as twenty dollars[42] to hiring sophisticated document destruction firms[43] to handle every aspect of document destruction. An on-site shredding policy might require employees to shred trade secret materials in their offices or deposit them in special containers from which documents will be collected and shredded elsewhere on the premises. To avoid the cost and administrative burden of training permanent employees to destroy trade secrets on-site, a trade secret owner may choose instead to hire a document destruction company to destroy documents on or off-site with truck-mounted mobile shredders.[44] Cautious trade secret owner may further decide to send an employee to verify that the outside contractor is actually destroying the secret documents entrusted to her. Similar precautions may be necessary with firms that destroy corporate trash completely off-site. Given trade secret owners' understandable concerns, some large shredder companies destroy their clients' trade secrets behind a screen of obsessive security that can include barbed wire fences and armed guards. One shredder company in California conducts strip searches of its employees before and after every shift and will fire employees on the spot for reading any documents before destroying them.[45] Despite such precautions, the private market may fall short of providing adequate comfort to trade secret owners if document destruction firms refuse to insure their customers up to the value of the trade secrets to be destroyed. If the shredding company's negligence results in trade secret revelation or theft, it is uncertain whether, in the absence of an express contract, the trade secret owner would recover the full value of her intellectual

---

41. Such a conveyance occurred in the *Drill Parts* case. *See* Drill Parts & Serv. Co. v. Joy Mfg. Co., 439 So.2d 43, 46 (Ala. 1983) (stating that the defendant had arranged to receive scrap metal and discarded papers from the plaintiff's machine shop without the latter's knowledge). In *Drill Parts*, however, the court implied that the scrap dealer who delivered the plaintiff's trash to the defendant did not know the trash contained valuable trade secrets. *Id.*

42. *See NBC Nightly News: Increase in Identity Thefts through Information Taken from Junk Mail and Other Personal Documents Has Caused a Rise in Paper Shredder Sales* (NBC television broadcast, Nov. 19, 1997) ("Now you can buy one for $20 and it fits in the palm of your hand . . . . Next year, a record million and a half people are expected to buy one . . . ."). Unfortunately, $20 shredders are likely to shred paper into single strips that can, with patience, be reassembled enough to discern important information. *Cf.* United States v. Scott, 776 F. Supp 629 (D. Mass 1992) (holding that federal agents did not a need warrant to seize shredded trash discarded by a tax-evasion suspect since the latter had no reasonable expectation of privacy by society's standards in such trash); *Curbside Trash—Reconstruction of Shredded Documents*, MASS. LAW. WKLY., Nov. 11, 1991, at 13.

43. *See* Tim Urbonya, *Rohn Industries Makes Sure That the Paper Trail Stops Here*, MINNEAPOLIS-ST. PAUL CITY BUS. DATELINE, Oct. 23, 1989, at 1. Private shredding companies are so numerous that they even have their own trade organization—the National Association for Information Destruction. *See* Coile, *supra* note 35.

44. *See* Wayne Tompkins, *Shredders Working Overtime to Protect Privacy, Especially Financial*, FLA. TODAY, Sept. 13, 1996, at S12.

45. *See* Coile, *supra* note 35.

property.

At first glance, choosing private protection over legal reform might appear to be the best solution to dumpster diving since trade secret owners are more motivated than society to protect their intellectual property and have better information about the exact level of protection their respective secrets require. However, adopting this view may force trade secret owners to spend excessive amounts on private security and then recoup to costs by charging consumers more for their products. Furthermore, forcing trade secret owners to rely exclusively on private security measures implicitly endorses the very law of the jungle among business competitors that has been condemned by trade secret law.[46] Dictating that trade secret protection turn solely on an owner's efforts to protect herself is the moral equivalent of dismissing burglary charges on the grounds that the victim's door was unlocked or secured by a cheap lock. An even closer analogy can be drawn between dumpster diving and trash searches for credit card information. Denying legal recourse against dumpster divers is the moral equivalent of allowing thieves who root through garbage piles for receipts and records with personal data[47] to freely use the credit card numbers they obtain. These trash searching thieves have become such a menace that they were the focus of a recent story on the NBC Nightly News.[48] Ordinary citizens are so afraid of having their personal information stolen by such dumpster diving "identity thieves" that they are buying personal paper shredders in record numbers.[49] The problem of credit card dumpster diving is so wide-spread that many small businesses are taking extra precautions to avoid negligently disclosing sensitive information about their customers or employees.[50]

Incredibly, our society chooses to punish credit card dumpster divers,[51] but allows trade secret dumpster divers to steal freely those asserted trade secrets that their corporate victims did not completely destroy before disposal. This seemingly unjust result stems from the application of the ethics-neutral *Greenwood* presumption to the trade secret law's reasonable precautions

---

46. *See* E.I. DuPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970) ("[I]ndustrial espionage of the sort here perpetrated has become a popular sport . . . . However, our devotion to free-wheeling competition must not force us into accepting the law of the jungle as the standard of morality. . . ."); *see also Corporate Privacy*, *supra* note 8, at 420 & n.161.

47. *See* Fisher, *supra* note 10; *Credit Card Scam*, *supra* note 10.

48. *See NBC Nightly News*, *supra* note 42 ("[Identity thieves] steal more than half a billion dollars a year, often starting with something called *dumpster diving* . . . .") (emphasis added).

49. *See id.*

50. *See* Louderback, *supra* note 40 (based on interviews with James Lang, owner of Professional Security Associates in Beavercreek, Ohio and Curtis Slaton, a corporate-law attorney at Bogan, Patterson and Bowman in Dayton, Ohio). Such unintended disclosure may expose such businesses to criminal and civil liability, as well as the costly loss of business.

51. *See* Fisher, *supra* note 10.

requirement.[52]

II. THE PRIVACY ANALOGY: *WINNE* AND *TENNANT* RATIONALES

Despite dumpster diving's prominent role in the growing industrial espionage threat and the considerable cost (private and public) of private security measures, dumpster diving has not been designated an improper means of acquiring trade secrets.[53] Accordingly, a court's focus shifts away from the defendant's possible improper conduct and towards examining the victim's action to protect her trade secrets. One crucial determination that dictates whether the plaintiff has a cause of action is whether or not the information allegedly stolen was a trade secret at all. The Achilles' heel of a dumpster diving victim's claims is that to be a trade secret, information must have been secret even though it was in the trash.[54] Though absolute secrecy is not required, the *Greenwood* presumption that there is no reasonable expectation of privacy in trash undermines victims' claims of secrecy.

In ascertaining whether an owner took reasonable steps to protect her trade secret, the fundamental question should be whether the precautions forced the competitor to use improper, unethical or illegal means.[55] But unless dumpster diving is statutorily designated an improper means, courts will probably fail to balance more fairly the reasonable precautions requirement and the improper means provisions asserting that trade secrets may not be legally obtained by means that are extreme, illegal, or unethical. Unfortunately, since most courts considering dumpster diving cases are not guided by the presumption that dumpster diving is against public policy, they will focus almost exclusively on the nature of the victim's defenses against dumpster divers. Specifically, courts will seek to determine whether the trade secret owner took reasonable secrecy precautions.[56]

When a court emphasizes the secrecy precautions requirement in a trade secret case, it is forced to "make a factual determination as to whether the owner used reasonable precautions" because it is impossible to articulate a

---

52. *Cf.* Don Wiesner & Anita Cava, *Stealing Trade Secrets Ethically*, 47 MD. L. REV. 1076, 1119 (1988) (stating that the courts' failure to frame their examination of security in terms of equitable notice makes evaluations of commercial morality difficult).

53. There is one exception: the Connecticut legislature classified dumpster diving as an improper means by designating it a form of espionage. *See* CONN. GEN. STAT. § 35-51, *as amended by* Pub. Act No. 97-110. See *infra* text accompanying note 126 for a discussion of the law.

54. According to the first *Restatement of Torts*, the plaintiff need only have maintained a substantial level of security so that "except by the use of *improper means*, there would be difficulty in acquiring the information." RESTATEMENT OF TORTS § 757 cmt. b (emphasis added).

55. *See* Slaby, *supra* note 16, at 331.

56. *See id.* at 325-26 ("[T]he law requires the trade secret owner to undertake actual efforts which are rigorous enough to force another to use improper, unethical or illegal means to discover the trade secret.").

standard independent of a particular set of facts.[57] As a result, courts have tried to fill what one commentator has called "this standardless void"[58] by drawing an analogy to the Fourth Amendment conception of reasonable privacy expectations.[59] As demonstrated by the decisions in *Tennant Co. v. Advance Mach. Co.*[60] and *Frank W. Winne & Son, Inc. v. Palmer*,[61] the First Amendment analogy has, respectively, both supported and undermined dumpster diving claims.

A. *The* Tennant *Rationale*

The Fourth Amendment analogy has not always been applied to dumpster divers' benefit. For example, in *Tennant*,[62] the Minnesota Court of Appeals condemned a floor cleaning equipment manufacturer's use of dumpster diving to discover a competitor's confidential sales information.[63] In this case, the court applied California law since the dumpster diving occurred in that state. The plaintiff Tennant Co. ("Tennant") sued its competitor the Advance Machine Co. ("Advance") after some of Advance's employees "rummaged through the trash in a dumpster behind Tennant's western regional sales office

---

57. Note, *Trade Secret Misappropriation*, *supra* note 3, at 464.

58. *See id.* at 464.

59. *See id.* ("[C]ommentators implicitly suggest that if the owner of a trade secret has secured a Fourth Amendment reasonable expectation of privacy, he has used reasonable precautions in protecting his trade secret. Consequently, any violation of a trade secret owner's reasonable expectation of privacy must constitute misappropriation.").

60. 355 N.W.2d 720 (Minn. Ct. App. 1984).

61. No. 91-2239, 1991 U.S. Dist. LEXIS 11183, at *1 (E.D. Pa. Aug. 7, 1991)

62. 355 N.W.2d 720 (Minn. Ct. App. 1984). *Tennant* was based on Fourth Amendment analogy as applied under the then ruling case of *People v. Krivda*, 486 P.2d 1262 (Cal. 1971) (invalidating a warrantless police search on the grounds that the defendant held a reasonable expectation that searched trash would be taken by authorized collectors and mixed with trash from other sources) *vacated*, 409 U.S. 33, *reaffirmed*, 504 P.2d 457 (1973), *cert. denied*, 412 U.S. 919; *see also* United States v. Kahan, 350 F. Supp. 784, 796 (S.D.N.Y. 1972) (invalidating a warrantless police search on grounds that "the undisputable expectation of an employee who discards items in his own wastebasket is that they subsequently will be disposed of and destroyed without prior inspection by others."). After the ruling in *Greenwood*, *Tennant* and *Kahan* were of no avail to trade secret owners.

63. *Tennant* was not the only case to condemn dumpster diving as a trade secret theft. An Alabama court found that it was not a "plain and palpable abuse of discretion to find a misappropriation of a trade secret although evidence was presented that plaintiff's drawings had been found in a trash bin." Drill Parts and Serv. Co. v. Joy Mfg. Co., 439 So.2d 43 (Ala. App. Ct. 1983). More recently, two dumpster diving cases in California were resolved through settlement. *See* Silvaco Data Sys., Inc. v. Technology Modeling Assoc., 896 F. Supp. 973, 974 ("The events leading to the current litigation began in the summer of 1991 when TMA started to suspect that someone was illicitly stealing trade secrets by 'dumpster diving' in the trash bins behind their offices . . . . After substantial discovery was completed, the parties agreed to a settlement on July 27, 1992."); *"Dumpster Diving" Presents Questions of Fact*, 3 Mealey's Litigation Reports, Jan. 13, 1995 (discussing a Santa Clara County Superior Court judge's refusal to dismiss a trade secret claim on the grounds that dumpster diving presents a question of fact to be resolved by the jury); Nancy Rivera Brooks, *Ethics at Work: Gathering Competitive Intelligence on Your Rivals Is Fine, Experts Agree, As Long As You Follow the Law. Just Watch Out for those Gray Areas*, L.A. TIMES, Nov. 3, 1997, at D2 (discussing dumpster diving lawsuit by Balboa Capital in Los Angeles that was settled but "raise[d] a host of ethical questions").

in California"[64] for nearly six months. These dumpster dives against Tennant were organized by Advance's West Coast sales manager, George McIntosh. McIntosh, who enlisted the help of Advance's San Francisco sales manager, sent "memos summarizing information from stolen documents" back to Jerry Rau, Advance's vice president for industrial sales.[65] Mr. Rau testified that when he learned about McIntosh's memos he took them lightly, thinking it was a joke because he had not imagined that dumpster diving could be useful in any way. However, once Tennant sued Advance, the president of Advance, Mr. Pond, fired McIntosh. During trial in the lower court, Mr. Pond was asked "whether he thought raiding the dumpster and rifling through a competitor's trash was unethical."[66] Mr. Pond "equivocated"[67] but the *Tennant* court did not: Judge Parker's opinion raised the issue of ethics once more by pointing out that "the president of Advance, who personally hired the individuals responsible for illegal activity, was indifferent to the ethics of their behavior."[68]

Judge Parker could designate McIntosh's dumpster diving illegal because of the rule set forth by *People v. Krivda*[69] that "an owner retains reasonable expectation of privacy in the contents of a dumpster 'until the trash [has] lost its identity and meaning by becoming part of a large conglomeration of trash elsewhere.'"[70] Unfortunately for trade secret owners in the future, Judge Parker went on to proclaim that "One has the same expectation of privacy in property regardless of whether the invasion is carried out by a law officer or by a competitor."[71] This statement could easily be interpreted as manifesting Judge Parker's commitment to coupling permanently industrial espionage cases to the Fourth Amendment rationale. However, given the ethical language that Judge Parker used in other parts of his opinion, he might have written his decision differently if *Greenwood* had been decided previously.

Tennant arguably touched on two of the three underlying purposes of trade secret law—promoting commercial morality and protecting privacy interests. One might even argue that the hint of cost-benefit analysis is implied in Judge Parker's conclusion that it was enough that Advance "disposed of its waste in a manner that would assure secrecy except to someone *particularly intent on finding out inside information.*"[72]

---

64. *Tennant*, 355 N.W.2d at 723.
65. *Id.*
66. *Id.*
67. *Id.*
68. *Id.*
69. 486 P.2d 1262 (Cal. 1971). *Krivda* was overruled by *Greenwood v. California*, 486 U.S. 35 (1988). *See infra* text accompanying note 76.
70. *Tennant*, 355 N.W.2d at 725 (citing *Krivda*, 486 P.2d at 1268 (1971)).
71. *Id.*
72. *Id.* (emphasis added).

B. *The* Winne *Rationale & The* Greenwood *Presumption*

Unfortunately for dumpster diving victims, the implications of the Fourth Amendment analogy for dumpster divers were changed profoundly when *People v. Krivda*[73] was overruled by the Supreme Court's 6-2[74] decision in *Greenwood v. California*.[75] In *Greenwood*, Justice White proclaimed that because there is no reasonable expectation of privacy in sealed trash bags put out for collection, police may search such trash without a warrant.[76] White supported this holding by asserting that there is no privacy interest in trash that is left on the curb for collection since it is "common knowledge" that trash placed beyond the curtilage of an individual's home is "readily accessible to animals, children, scavengers, snoops, and other members of the public."[77] The damage caused by this presumption that trash is in the public domain (the "*Greenwood* presumption") became apparent when it was incorporated into trade secret law by a Pennsylvania federal district court in *Frank W. Winne & Son, Inc. v. Palmer*.[78] As in *Tennant*, dumpster diving was the central issue in the *Winne* case. The defendant, Jared Palmer, was the president of the Twi-Ro-Pa rope manufacturing and vending business that was in direct competition with the plaintiff, Frank W. Winne & Son, Inc. Palmer allegedly ordered one of his Philadelphia salesmen to "collect the trash which [Winne] had 'put out for collection' and to forward all office documents therein to Palmer."[79] This Palmer's salesman did as ordered for over a year until Winne discovered that its trash was being taken and sued Palmer for trade secret theft.[80]

Early in its opinion, the *Winne* court stated that there was no litmus test for what constitutes a trade secret; this issue was generally a fact for the jury.[81] Nonetheless, the court summarily asserted that there was no trade secret protection for confidential business information that was placed in the trash since "[t]here are a number of Fourth Amendment cases holding that there is

---

73. 486 P.2d 1262 (Cal. 1971).

74. Justice Kennedy took no part in the consideration or decision of the case.

75. 486 U.S. 35 (1988).

76. *Greenwood* paved the way for often unpopular warrantless police searches of trash. News reporters' searches through trash cans constitute an equally unpopular activity, but one reporter's recent search of police trash in Connecticut probably struck *Greenwood*'s detractors as poetic justice. *See* Bill Keveney & Lynn Tuohy, *TV Journalists Halted at Dumpster: Prosecutor Reviewing Law for Possible Violation at Courthouse*, HARTFORD COURANT, Sept. 13, 1996, at B9.

77. *Greenwood*, 486 U.S. at 40.

78. No. 91-2239, 1991 U.S. Dist. LEXIS 11183, at *1 (E.D. Pa. Aug. 7, 1991). However, for an example of one of the few ways through which the *Greenwood* presumption might actually further intellectual property rights, see *Guilty in Industrial Spying Case*, UPI, Oct. 18, 1996, *available in* LEXIS, Nexis Library, CURNWS file (discussing the FBI's use of dumpster diving to crack a Silicon Valley industrial espionage case against David Biehl, President of the now defunct Semiconducter Spares, Inc.).

79. *Winne*, 1991 U.S. Dist. LEXIS 11183 at *2.

80. *See id.*

81. *See id.* at *4.

no reasonable expectation of privacy in trash which is placed out for collection."[82] However, the court did point out that it did "not appear from the complaint whether the documents placed in the trash were intact or shredded and then reconstructed, or whether they were retrieved from an area generally accessible to others or exclusively under plaintiff's ownership and control."[83] The court then remarked: "[t]hus, the record must be more fully developed regarding how the trash was stored, where it was placed and what other precautionary measures may have been taken."[84] The *Winne* court did not hold that a trade secret could *never* exist in trash, but it did refuse to decouple the privacy interests of trade secret owners from those of suspects subjected to Fourth Amendment searches.[85]

III. THE *WINNE* RATIONALE'S MISPLACED RELIANCE ON THE *GREENWOOD* PRESUMPTION

There are two problems with the *Winne* rationale's reliance on the *Greenwood* presumption. First, unlike law enforcement officers who are public officials sworn to uphold the law, dumpster divers are self-interested, unregulated parties with no legitimate, publicly sanctioned justification for their trash searches. Second, modern trash is no longer the uniformly worthless material that it was considered to be before the advent of recent advances in information technologies.

A. *The Value of Trash: Towards A Modern View*

The *Winne* court's reliance on the *Greenwood* presumption that there is no expectation of privacy in trash is based on antiquated notions about the nature and value of trash in the modern business world. The *Greenwood* majority commented that "having deposited their garbage 'in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it,' respondents could have had no reasonable expectation of privacy in the inculpatory items that they discarded."[86] Contradicting this conclusion is the fact that in today's information society there are two kinds of trash: (1) trash that is abandoned to the world, and (2) trash that is meant to be kept secret until destroyed. Trade secrets that may be gleaned from discarded office paper, diskettes, and the like fall into the second category.

Old notions about trash overemphasize its tangible aspects. However,

82. *Id.* at *10 (citing California v. Greenwood, 486 U.S. 35 (1988)).
83. *Id.* at *12.
84. *Id.*
85. *Id.* at *11.
86. *Greenwood*, 486 U.S. at 41.

dumpster divers target intangible wealth. Such intangible wealth increasingly drives our economy as more goods and services are transferred via electrons and microwaves. As Nicholas Negroponte proclaims, intangible electronic bits of information are becoming increasingly more important than atoms.[87] Earlier in U.S. history, society's reluctance to revise its views about garbage led to health epidemics.[88] Once again, short-sightedness about the evolving nature of trash threatens the public well-being, this time by supporting a legal policy that condones industrial espionage. We should modify our legal views of trash to better fit this changing aspect of our economy.

If the law does not protect trade secrets at all points in the public disposal process, businesses will be forced to adopt a separate, private, system of waste disposal. Such a private system may already exist, given the exponential growth in paper shredders and document destruction services. However, the shift towards such private systems does not dictate that trade secret law should deny protection from dumpster divers any more than the growth of the home security industry dictates that the law should deny protection from burglars.

B. *Official Versus Unofficial Trash Searches*

While the *Winne* court admitted that *Greenwood* was not a trade secret case,[89] it nonetheless relied on *Greenwood* to conclude that "it is rather difficult to find that one has taken reasonable precautions to safeguard a trade secret when one leaves it in a place where, as a matter of law, he has no reasonable expectation of privacy from prying eyes."[90] However, this assertion does not address the fact that the police are subject to checks and balances that do not apply to dumpster divers. For example, though the police may surreptitiously extract evidence from trash, at some point they will announce the results of their trash search. In contrast, dumpster divers will seek to keep their searches permanently secret. Additionally, official trash searches are ostensibly conducted for the public good, while dumpster dives intentionally avoid the beneficial alternative of reverse engineering or publicly available information. Accordingly, the *Winne* rationale overlooks the fact that police, and even trash collectors, are public servants entrusted with carrying out official functions for the public good. Dumpster divers are self-interested parties who choose, unethically, to siphoning off the intellectual efforts of others. *Dow Chemical Co. v. EPA*[91] suggests that *Greenwood*'s characteriza-

---

87. *See* NICHOLAS P. NEGROPONTE, BEING DIGITAL 4 (1995). Mr. Negroponte is a Professor of Media Technology at MIT and the Founding Director of the MIT Media Lab.

88. *See* MARTIN V. MELOSI, GARBAGE IN THE CITIES: REFUSE, REFORM, AND THE ENVIRONMENT, 1880-1980, at 19-20 (1981).

89. *Winne*, 1991 U.S. Dist. LEXIS at *11.

90. *Id.*

91. 476 U.S. 227 (1984) (holding that the EPA may take aerial photographs of plaintiff's facilities for purposes of enforcing environmental laws).

tion of the public domain as extending to trash should be limited to Fourth Amendment searches by government officers and other public officials.[92]

A case can be made that individuals should not receive greater privacy from private actors than from government officials.[93] This argument might emphasize that the Fourth Amendment protects citizens from arbitrary or oppressive governmental intrusions that, because they have the force of the state behind them, are particularly invasive and harmful. However, the ranks of dumpster divers include powerful multi-national corporations and foreign nations that can devote considerable resources towards surreptitious trash searches.[94]

Finally, *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*[95] elevated the "fundamental human right of privacy . . . . to the position of significant additional public policy reason for the protection of trade secrets by state law."[96] Accordingly, the development of a separate privacy jurisprudence tailored to trade secret law is preferable to the rigid coupling to Fourth Amendment law that the *Winne* rationale represents,[97] undergirded by the *Greenwood* presumption that threatens to undermine the principle that efforts to protect trade secrets need not be spy-proof.[98]

---

92. *See id* at 239 n.6 (1984) ("[O]ther protections such as trade secret laws are available to protect commercial activities from private surveillance by competitors."); *see also* Lariscey v. United States, 949 F.2d 1137, 1141-43 (Fed. Cir. 1991) (holding that an imprisoned inventor took reasonable precautions to maintain secrecy under the circumstances of his incarceration, and therefore had a protectable trade secret).

93. A possible argument was set up by one commentator as a straw man: "All invasions of a reasonable expectation of privacy thus would be considered improper means of securing a trade secret, but not all constitutionally permissible activity would be considered proper means." Note, *Trade Secret Misappropriation: A Cost-Benefit Response to the Fourth Amendment Analogy*, 106 HARV. L. REV. 461, 472 (1992). In dismissing this argument, the commentator states that courts would be left "without guidance in determining when, and to what extent, trade secret law should provide greater protection than the Fourth Amendment." *Id.* This point does not consider the fact that prevailing standards of the business community may be considered in determining each case under an ethical framework depending, of course, on the factual context of each case. The commentator above, however, precludes such an ethical framework by dismissing the ethical component of the *Christopher* case as "moralistic rhetoric." While it is true that the Fifth Circuit in *Christopher* used a kind of cost-benefit rationale, this test was not the only basis of the court's decision. Such arguments fail to adequately account for trade secret law's migration to the law of unfair competition. In this new field, courts and commentators should reconsider any past attempts to pin trade secret law under any crisp rules or bright line tests. *See* Robert C. Denicola & Harvey S. Perlman, *A Foreword to the Symposium on the Restatement of Unfair Competition*, 47 S.C. L. REV. (1996). ("Much of the Restatement's so-called 'black-letter' law takes the form of broad standards and catalogs of relevant factors rather than crisp rules and bright line tests. Although not new to the Restatements, we think this approach is particularly appropriate in a field such as unfair competition where context is so often everything.").

94. *See supra* note 27 and accompanying text.

95. 489 U.S. 141 (1989).

96. 1 JAGER, *supra* note 2, § 1.05, at 1-15.

97. *See Corporate Privacy*, *supra* note 8, at 400-01 ("Since [*United States v.*] *Morton Salt* [, 338 U.S. 632 (1950)], limited to its facts, held only that a corporation has no right of privacy vis-a-vis governmental regulatory inquiries, it is not necessarily authority for the denial of a corporate right of privacy in other contexts.") (citations omitted).

98. *See* E.I. DuPont deNemours v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970).

IV. *CHRISTOPHER* AND THE COST OF ABSOLUTE SECRECY

"[T]hou shalt not appropriate a trade secret through deviousness under circumstances in which countervailing defenses are not reasonably available."[99]

"Perfect security is not optimal security."[100]

To warrant legal protection, a trade secret must be secret, but not absolutely so.[101] Indeed the common law has promoted relative rather than absolute secrecy since the discussion of secrecy in *Peabody v. Norfolk*.[102] Under the Fourth Amendment analogy, relative secrecy hinged on reasonable expectations of privacy. However, one commentator has argued that the reasonableness of security measures should be determined through cost-benefit analysis.[103] Like the Fourth Amendment analogy, a cost-benefit approach would not require that secrecy precautions be absolute.

For example, in the famous "spy-in-the-sky" case, *E.I. DuPont deNemours v. Christopher*,[104] the Fifth Circuit held that secrecy precautions need not be spy-proof. The plaintiff, the DuPont chemical company, was constructing a new chemical plant that would use valuable new trade secrets to produce methanol. DuPont took extensive precautions to restrict access to and view of its plant. However, parts of the uncompleted facility were not covered by a roof. The defendants, the Christophers, took advantage of this fact, and, under the employ of DuPont's competitor, flew over the unfinished chemical plant in an airplane. Appropriately disturbed by the plane's presence, DuPont investigated immediately and discovered that the Christophers had taken photographs of the plant for a competitor. When the Christophers refused to reveal the name of their client or to yield the pictures, DuPont sued the Christophers for trade secret theft.

DuPont charged that the Christophers had wrongfully obtained the

---

99. *Id.* at 1017 (holding that aerial spying on a competitor's trade secret through otherwise legal means nonetheless constituted improper means).

100. Rockwell Graphics Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 180 (7th Cir. 1991).

101. Secrecy is the threshold issue in every trade secret case. *See* RESTATEMENT OF TORTS, § 757 cmt. b (1939) ("The subject matter of a trade secret *must be secret.*"); 1 JAGER, *supra* note 2, § 5.05, at 5-58.1 ("The single most important requirement of the trade secret law is the obvious one which deserves continuous emphasis—that the trade secret must in fact be secret."). However, any cases requiring absolute secrecy are in a "distinct minority." MILGRIM, TRADE SECRETS, *supra* note 3, at 2-75 through 76.

102. 98 Mass. 452, 461 (1868).

103. *See* Note, *Trade Secret Misappropriation*, *supra* note 3, at 472-73. ("Instead of the Fourth Amendment analogy, which primarily promotes privacy interests, courts should use a cost-benefit analysis to determine whether an owner has taken reasonable precautions.").

104. 431 F.2d 1012 (5th Cir. 1970).

photographs and sold them to a third party. The photos, DuPont argued, could be used by an expert engineer to discern DuPont's secret methanol manufacturing process. In response to DuPont's claim of trade secret theft, the Christophers argued that neither flying over DuPont's plant nor taking pictures from an airplane was illegal. Although the Chrisptophers' activity, like dumpster diving that does not involve trespass, was legal on its face, it was condemned as an improper means of obtaining DuPont's trade secret. In holding that DuPont had taken reasonable precautions despite the Christophers' successful surveillance, the Fifth Circuit proclaimed: "Perhaps ordinary fences and roofs must be built to shut out incursive eyes, but we need not require the discoverer of a trade secret to guard against the unanticipated, the undetectable, or the unpreventable methods of espionage now available."[105] The court went on to explain that requiring DuPont "to put a roof over the unfinished plant would impose an enormous expense to prevent nothing more than a schoolboy's trick . . . . Reasonable precautions against predatory eyes we may require, but an impenetrable fortress is an unreasonable requirement."[106]

The language in *Christopher* about "unanticipated" espionage suggests that if the case were decided today on the same facts, the court might deny relief on the grounds that it is common knowledge that industrial spies use aerial photography. If the court rejected the idea that the espionage could not be detected, the rationale of *Christopher* might collapse into an argument about the cost of detectability and prevention. While the promotion of innovation requires that the law prevent the redirection of valuable resources away from productive invention and towards inefficient self-protection, the promotion of innovation is only one of the policies underlying trade secret law.[107] The promotion of commercial morality and the protection of privacy are the others.[108] Accordingly, the public policy of promoting commercial morality mandates that courts address the ethicality of allowing "predatory eyes" and the cost of private prevention alone to dictate which particular schoolboy's tricks the courts will protect trade secrets from.[109]

Though *Christopher* suggests that courts must consider the cost[110] of preventing unpredictable or undetectable espionage, a cost-benefit analysis should not be the sole measure for determining the existence of a trade secret.

---

105. *Id.* at 1017.
106. *Id.*
107. *See supra* text accompanying note 4.
108. *See supra* text accompanying note 2.
109. *See infra* text accompanying note 109.
110. *See* Note, *Trade Secret Misappropriation*, *supra* note 3, at 465; *see, e.g.*, Rockwell Graphic Sys. v. DEV Indus., 925 F.2d 174, 180 (7th Cir. 1991) ("Obviously [the plaintiff] could have taken more precautions. But at a cost, and the question is whether the additional benefit in security would have exceeded that cost."); USM Corp. v. Marson Fastener Corp., 393 N.E.2d 895, 902 & n.12 (Mass. 1979) (suggesting optimization rather than the maximization of security measures and concluding on that basis that the plaintiff's precautionary measures were sufficient).

Although one commentator has argued that a cost-benefit approach would yield more predictable decisions than those made under the Fourth Amendment analogy, a cost-benefit approach alone does not adequately address the oldest purpose of trade secret law—upholding a minimum level of commercial ethics.[111] If a trade secret owner fails the cost-benefit analysis, she will lose her right to legal protection no matter how egregiously unethical the methods used by her competitors to obtain them. For this reason, courts should consider an approach that supplements privacy and cost-benefit analysis with careful consideration of commercial ethics.

V. TRADE SECRET LAW'S ETHICAL BLINDSPOT (ESPIONAGE IS UNETHICAL)

When asked whether he thought raiding the dumpster and rifling through a competitor's trash was unethical, Pond equivocated by saying that he did not have enough information to make a judgment on those practices.[112]

I have three tests: the newspaper test, the child test and the skunk test.[113]

Dumpster diving is sleazy.[114] Both the Fourth Amendment analogy and cost-benefit framework overlook the ugly truth that dumpster diving[115] offends the generally accepted standards of commercial morality. Despite predictable cynicism,[116] members of the business world—with the exception of animals, children, scavengers[117]—are expected to follow[118] minimum

---

111. Early American cases on trade secret misappropriation emphasized enforcing business morality among competitors over the encouragement of innovation. *See, e.g.*, Eastman Co. v. Reichenbach, 20 N.Y.S. 110, 115 (N.Y. Sup. Ct. 1892) (holding that the efforts of two employees to start a photographic film business with their former employer's trade secrets was "not legitimate competition, which it is always the policy of the law to foster and encourage, but it is *contra bonos mores*. . . ."); *see also* Note, *Trade Secret Misappropriation*, *supra* note 3, at 464.

112. Tennant Co. v. Advance Machine Co., 355 N.W.2d 720, 723 (Minn. Ct. App. 1984).

113. Nancy Rivera Brooks, *Ethics at Work: Gathering Competitive Intelligence on Your Rivals Is Fine, Experts Agree, As Long As You Follow the Law. Just Watch Out for those Gray Areas*, L.A. TIMES, Nov. 3, 1997, Part D2, at 9 (quoting W. Michael Hoffman, executive director of the Center for Business Ethics, Bentley College). Mr. Hoffman's statement was offered as advice to well-meaning companies seeking to navigate ethical gray areas:

> "The newspaper test is: Would you want to see it printed the next morning in the newspaper? Would it embarrass you? The child test: What would you tell your child to do if he or she came to you and asked for your advice? And the skunk test: Does it smell?" Hoffman said. "If it doesn't feel right, smell right, taste right, then you probably should find out what makes it seem like a skunk."

Id.

114. One business ethics consultant warns businesses that typical violations of fair trade laws include "obtaining a competitor's trade secrets in a sleazy manner." DANIEL A KILE, BUSINESS CONDUCT AND ETHICS: HOW TO SET UP A SELF-GOVERNANCE PROGRAM at 8-15 (1995).

115. And indeed industrial espionage in general. *See* Brooks, *supra* note 111.

116. One commentator argues that the notion of "'[g]enerally accepted standards of commercial morality' provides little if any guidance." *Statutory Solution*, *supra* note 22, at 388 n.58.

117. *See supra* text accompanying note 77.

ethical standards.[119] Dumpster diving falls below these ethical norms, but courts have not condemned dumpster diving.[120] Instead, as demonstrated by *Winne* and *Christopher*, courts have avoided assessing whether dumpster diving is ethical by focusing exclusively on either the victim's expectation of privacy or the effectiveness of their secrecy precautions.[121]

Perhaps the courts' failure to consider the unethical nature of industrial espionage can be explained by the law's long-standing focus on cases involving breaches of trust. Though many industrial spies are not in a position of confidence,[122] courts must rely on precedent that focuses on breaches of trust by insiders who were in such positions. Nonetheless, early trade secret cases used flexible equity rationales and emphasized the enforcement of commercial morality.[123] In 1939, the *Restatement (First) of Torts* addressed espionage in Section 757, and set forth that improper means are "means which fall below the generally accepted standards of commercial morality and reasonable conduct."[124] Furthermore, the new *Restatement (Third) of Unfair Competition* suggests that the only proper way to obtain trade secrets, in the absence of their owners' consent, is by independent discovery or through the "examination

---

118. *See, e.g.*, GEORGE D. CHRYSSIDES & JOHN H. KALER, AN INTRODUCTION TO BUSINESS ETHICS, (1993); THOMAS M. GARRETT, BUSINESS ETHICS 99 (1966) ("Technological advance has created new gray areas. While the present writer is almost instinctively against the use of devices which violate privacy with or without trespass, there are many cases which can only be settled by careful legislation. In the absence of such law, companies will have to take increasing care of their secrets."); WALTER W. MANLEY II, CRITICAL ISSUES IN BUSINESS CONDUCT: LEGAL, ETHICAL, AND SOCIAL CHALLENGES FOR THE 1990S (1990).

119. In a general sense, ethics represent a "systematic attempt, through the use of reason to make sense of our individual and social moral experience, in such a way as to determine the rules that ought to govern human conduct and the values worth pursuing in life." Business ethics focus specifically on the relationship of business goals and techniques to specifically human ends. *See* Wiesner & Cava, *supra* note 52, at 1082 (quoting GARRETT, *supra* note 114, at 4 (1966)).

120. *See* Tennant Co. v. Advance Machine Co., 355 N.W.2d 720 (1984), came the closest to addressing the unethical nature of dumpster diving. *See id.* at 723 ("When asked whether he thought raiding the dumpster and rifling through a competitor's trash was unethical, Pond equivocated by saying that he did not have enough information to make a judgement on those practices."). Two scholars have criticized the courts' failure to adequately analyze trade secrets within an ethical framework. *Cf.* Wiesner & Cava, *supra* note 52, at 1081 ("The courts are not overly analytical in their pursuit of the ethical issue, but they espouse ethical intentions.").

121. The unsuccessful Unfair Commercial Activities Act would have enjoined persons who engaged in "acts or practices which violate reasonable standards of ethics." *See* Comment, *Industrial Espionage: Piracy of Secret Scientific and Technical Information*, 14 UCLA L. REV. 911, 926 n.79 (1967) [hereinafter *Industrial Espionage*] (citing H.R. 10038, 87th Cong. (1962) *reprinted in* 23 OHIO ST. L.J. 110, Annex (1962)). If successful, the Act might have been used to justify the courts' focus on the act of surveillance rather than upon the act of piracy. *See Industrial Espionage*, *supra*, at 926 n.79.

122. *See, e.g.*, E.I. DuPont deNemours & Co. v. Christopher, 431 F.2d 1012 (5th Cir. 1970); *cf. Corporate Privacy*, *supra* note 8, at 406 ("[T]he typical industrial espionage situation involves no confidential relationship.").

123. *See* Pace, *supra* note 3, at 435 n.23 (citing Eastman Co. v. Reichenbach, 20 N.Y.S. 110, 116 (N.Y. Sup. Ct. 1892); KIM L. SCHEPPELE, LEGAL SECRETS: EQUALITY AND EFFICIENCY IN THE COMMON LAW 240-41 (1988).

124. RESTATEMENT OF TORTS § 757 cmt. f (1939).

of a publicly available product."[125]

The examination of such publicly available products is a means of achieving the ethically acceptable goal of gathering competitive intelligence. Competitive intelligence has become so common place that it is considered an industry complete with its own professional association—the Society of Competitive Intelligence Professionals ("SCIP").[126] However, there is a gray area between competitive intelligence and industrial espionage. Dumpster diving, like the aerial surveillance in *Christopher*, falls into this gray area.

Because dumpster diving is an unethical and destructive practice, trade secret owners should not be abandoned to protect themselves exclusively through security measures such as guards, electronic surveillance and paper shredders.[127] To abandon trade secret owners to such private protection is the moral equivalent of abandoning homeowners to private protection against burglary. Society should make the moral statement that dumpster diving is wrong and will not be tolerated, even though it, like burglary, can be prevented through private security measures. Judges and state legislators should not be swayed by arguments that bolstering laws against dumpster diving will encourage underinvestment in proper security measures. As with homeowners, trade secret owners will use private security measures regardless of laws against dumpster diving—laws against burglary do not affect appreciably the sales of locks and keys. More difficult questions than whether or not to enact laws against dumpster diving is whether those laws should be criminal or civil, and whether they should be newly drafted, or simply a modification of existing law.

VI. THE CONNECTICUT SOLUTION AND THE EEA

A. *The Connecticut Solution: Dumpster Diving As Espionage*

On June 6, 1997, the State of Connecticut designated dumpster diving as a form of espionage and therefore an improper means of obtaining trade secrets.[128] This revision of Connecticut's trade secret law (the "Connecticut solution") tipped the balance of advantage in litigation in favor of trade secret owners by making it less likely that courts applying Connecticut law will simply dismiss dumpster diving claims for failing to state a claim. The Connecticut solution does not greatly disrupt the legal status quo since it was woven into existing trade secret law. Connecticut's new law does not relieve

125. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. f (1995).

126. *See* Brooks, *supra* note 111. SCIP has nearly 6,000 members and a code of ethics. *Id.*

127. Such an abandonment would clearly offend the oldest purpose of trade secret law—upholding a minimum level of business ethics. *See supra* note 4.

128. *See* CONN. GEN. STAT. § 35-51, *as amended by* Pub. Act No. 97-110; *supra* note 19.

trade secret owners of the responsibility to take precautions since Connecticut courts will still continue to weigh, in dumpster diving cases, the extent of *other* measures taken to guard the secrecy of the information. Furthermore, Connecticut's new law affords trade secret owners more protection without curtailing the activities of harmless trash pickers like the homeless.

By classifying dumpster diving as espionage, Connecticut clarified, in light of the sixth factor in the *Restatement's* famous six-factor test for trade secret misappropriation—the ease with which information could be *properly* acquired—that dumpster diving is *never* proper acquisition. The new law underscores that the issue of whether a defendant's conduct is improper should be determined under the "existing standards of the business community."[129] The 1939 *Restatement of Torts* defined improper means as those "means which fall below the generally accepted standards of commercial morality and reasonable conduct."[130] An Alabama Court found that it was not a "plain and palpable abuse of discretion to find a misappropriation of a trade secret although evidence was presented that plaintiff's drawings had been found in a trash bin."[131]

The Connecticut solution is necessary to guide courts away from the *Greenwood* presumption, which courts were likely to adopt absent the legislature's conclusion that dumpster diving should be discouraged as a matter of public policy.[132]

As mentioned above, the *Winne* rationale leads courts to conclude that discarding trash from which trade secrets may be discerned is equivalent to intentionally abandoning the trade secrets themselves. The cost-benefit analysis focus suggested in *Christopher* relies too much on trade secret owners' efforts to protect themselves as opposed to how competitors seek to obtain them improperly. The Connecticut solution to this dilemma lies between the two extremes of: (1) forcing trade secret owners to rely solely on private prevention through increased security or civil suits brought under the current law, and (2) altering the law to mandate public prevention by criminalizing dumpster diving. Classifying dumpster diving as industrial espionage, and therefore an improper means, is a straightforward solution that indirectly addresses the immorality of dumpster diving campaigns without requiring considerable tinkering with the status quo. Nonetheless, although Connecticut offers trade secret owners considerably more legal protection against dumpster divers, it does not clearly mandate that courts incorporate an ethical analysis into trade secret opinions.

---

129. RESTATEMENT OF TORTS § 757 cmt. f (1939).

130. *Id.* Examples of such means include "fraudulent misrepresentations to induce disclosure, tapping of telephone wires, eavesdropping or other espionage." *Id.*

131. *Drill Parts & Serv. Co. v. Joy Mfg. Co.*, 439 So.2d 43 (App. Ct. Ala. 1983).

132. *See* Interview with Judge Fader, *supra* note 31.

B. *The Economic Espionage Act*

Congress' enactment of the Economic Espionage Act of 1996[133] (EEA)—the first national law designed to crack down on economic espionage by foreign and domestic companies—sent a clear signal that trade secret theft is a serious problem worthy of national attention. With the EEA, Congress radically departed from the tradition of state-prescribed trade secret laws,[134] and involved federal resources in the fight against trade secret theft. During the years of debate, testimony and investigation that led to the EEA, FBI Director Freeh and other experts pointed out that state trade secret laws, which have no criminal liability attached to them, lacked the reach or power to deal with foreign-sponsored economic espionage. Furthermore, experts said that civil suits are difficult to win and seldom recoup the damage done, because the trade secret thief's financial resources are often inadequate, especially if the thief has been indemnified by his principal.[135] While the EEA is an important reform, one commentator remarks that it is unclear whether "[f]ederal authorities will be inclined to prosecute as criminal violations those matters that were traditionally resolved as private commercial disputes."[136]

Criminal statutes enacted on the state level arguably would do more to deter dumpster diving than the EEA, which will probably be applied only in sensational cases involving trade secrets worth large amounts of money.[137] Criminal statutes like those forbidding eavesdropping, wiretapping, or even stalking would greatly bolster the protection of trade secrets from dumpster divers. For example, wiretaps have been forbidden for so long that courts instinctively associate such activity with unethical behavior. Indeed, the impropriety of wiretapping is so widely accepted that one seldom stops to reflect on the ethical purposes underlying laws against intercepting communications. If laws specifically forbidding credit card dumpster diving were enacted, such laws might soon loosen the intellectual bonds that couple trade secret privacy interests to the Fourth Amendment analogy. Accordingly, state

---

133. *See* 18 U.S.C. §§ 1831-1839, *enacting* P.L. 104-294 (Oct. 11, 1996); *see also* S. Rep. No. 104-359 (1996). Under provisions of the EEA, an individual convicted of economic espionage may be fined up to $250,000 and sentenced to 15 years in prison. Corporations that sponsor such activity may be fined up to $10 million. *See* Levin, *supra* note 20, at 5; Yates, *supra* note 21.

134. *But cf. Pace*, *supra* note 3 (discussing the proposal of federal trade secret regimes).

135. *See Economic Espionage: Hearings Before the Senate Intelligence Comm. and Senate Judiciary Comm.*, 104th Cong. 103 (Feb. 28, 1996) (statement of Raymond Damadian, M.D., President and Chairman of Fonar Corp. and inventor of the MRI medical scanning machine); *cf.* Holly Emrick Svetz, *Japan's New Trade Secret Law: We Asked For It Now What Have We Got?*, 26 GEO.WASH. J. INT'L L. & ECON. 413, 440 (1992) ("Criminal punishment of misappropriating individuals, without also prosecuting or enjoining the users or buyers of the trade secrets, is an inadequate remedy for industrial espionage.").

136. Levin, *supra* note 20.

137. *See id.* ("Ordinarily . . . only extremely egregious trade secret misappropriation, such as those alleged in General Motors v. Lopez, have warranted intervention of federal law.").

criminal laws addressing dumpster diving for trade secrets could be an even better deterrent than the Connecticut solution. Conceivably, those opposing criminalization might argue that criminalization would commit scarce public resources to protecting trade secret owners from foreseeable threats that they could avoid with private security measures. This argument, however, is the moral equivalent of arguing that public monies could be saved by cutting police patrols in high-crime neighborhoods since private citizens can buy Rottweilers, home security systems, pepper spray, handguns, and bullet proof vests on the open market. In light of this last analogy, the appropriate question for dumpster diving is: What kind of commercial community do we want to promote?

VII. CONCLUSION

Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.[138]

The Fourth Amendment analogy and the cost-benefit framework lead judges to focus narrowly on the extent of the precautions taken by trade secret owners to keep their intellectual property out of dumpster divers' reach, and to ignore the important ethical question of whether dumpster diving is *ever* a reasonable means of obtaining trade secrets. Given trade secret law's clearly stated purpose of maintaining minimum levels of business ethics, the latter question should be asked using the "generally accepted standards of commercial morality and reasonable conduct."[139] Trade secret law's failure to make a clear unified statement about the ethicality of dumpster diving campaigns encourages this unethical behavior, thereby undermining trade secret law's ethical purpose. The Connecticut solution, which designates dumpster diving as a form of espionage was an important reform and may serve as an example for other states. Triggering the "espionage" provisions of current trade secret laws is a good solution under the current regime, even if it does no more than prevent judges from dismissing causes of action against dumpster divers for failure to state a claim. Furthermore, the Connecticut solution requires private prevention of dumpster diving without abdicating society's responsibility to condemn and discourage unethical business practices. Likewise, the EEA may afford trade secret owners protection against the most egregious dumpster diving attacks, especially those conducted by foreign governments. Nonetheless, since much of trade secret remains a patchwork of widely varying state law, true reform should include evolution of the common law of trade secrets

138. Samuel D. Warren & Louis D. Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193, 193 (1890).

139. RESTATEMENT OF TORTS § 757 cmt. f (1939).

to address dumpster diving.

Admittedly, this solution may depend heavily on legal uniformity of the sort that would result from adopting a Federal Trade Secrets Act. Even without effecting such fundamental change, however, the national intellectual property bar might influence lawmakers and judges nationwide to subscribe to this view, though this would be an uphill battle. Currently, courts are likely to rely almost exclusively on the *Winne* rationale and cost-benefit model to resolve dumpster diving cases. Absent a clear statement from state legislatures or Congress, courts may increasingly rely on these frameworks alone. In doing so, the courts will promote a policy that undermines commercial ethics, ignores privacy interests, and discourages innovation.