We’re Friends, Right?
Client List Misappropriation and
Online Social Networking in
the Workplace

ABSTRACT

Social networks, such as Facebook, MySpace, and LinkedIn have grown tremendously over the past decade, and today they claim over 200 million users between the three services. A great number of smaller social networks have also appeared, and new services are constantly being created. With the vast growth of social networking has come the use of social networking in business. As businesses have sought to exploit the wealth of information that social network users share over these networks, businesses have encountered the problem of protecting the compilations of information they have produced. The problem became clear in 2008 when a British recruitment company filed suit against a former employee who allegedly took advantage of information on a social network to start a competing company.

This Note examines the history of trade secret protections in the United States. It begins by examining various bodies of law that are used to protect trade secrets, such as the Restatement of Torts, the Uniform Trade Secret Act, the Restatement (Third) of Unfair Competition, and contract law, including nondisclosure and noncompetition agreements. The Note then compares traditional customer list cases to issues that arise when customer lists exist in or are compiled from an online social network. Finally, this Note suggests that courts should extend existing trade secret protections to online client lists and detailed lists compiled from social networking data, while retaining employee protections that are present in current bodies of law.
Imagine spending countless hours at meetings and social
events networking with potential clients, only to have the most
valuable information you have acquired taken by a departing
employee seeking to profit from your hard work. Not only would this
be frustrating, but it would also be unfair. What if those same
countless hours were spent making contacts online? Surely, the same
feelings would arise. Regardless of whether the contacts were made in
person or online, the law should protect the information that one
obtains by networking with potential clients. Indeed, absent explicit
contractual provisions to the contrary, valuable client information
compiled from online contact lists should be protected by the law.

Legal protection of trade secrets is nothing new. From Roman
businessmen\(^1\) to medieval guilds and modern businesses,\(^2\) holders of

---

1. See Restatement (Third) of Unfair Competition § 39 cmt. a (1995); A.
Arthur Schiller, Trade Secrets and the Roman Law: The Actio Servi Corrupti, 30 Colum. L.

2. See Robert P. Merges et al., Intellectual Property in the New
Technological Age 33-35 (4th ed. 2007) (providing a general overview of the origins of
trade secret protection and its particular importance among small businesses).
secret information have sought to protect this valuable data from disclosure to competitors, and both British and American courts have protected trade secrets for around two hundred years. Modern innovators seek to protect many kinds of trade secrets, such as novel methods of production, secret formulas, and lists of potential clients; indeed, such innovators have a financial interest in preventing competitors from appropriating the fruits of their labor. To this end, the Uniform Trade Secret Act (UTSA), promulgated in 1979 by the National Conference of Commissioners on Uniform State Laws, gives broad scope to the term “trade secret,” defining it as “information, including a formula, pattern, compilation, program, device, method, technique, or process, that . . . derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means . . . .”

Customer and client lists raise unique trade secret issues. Businesses that conduct sales or provide services to a large set of customers typically place great value on the contacts they develop in the course of business. It is often impractical to memorize the contact and client information of every client or customer, so businesses must store lists either in hard copy or digitally. On the other hand, employees may know their clients personally, allowing those employees to remember many details about their clients without documentation. However, with advances in technology, novel methods of storing and misappropriating client information have become commonplace. Just as phone numbers and addresses were once commonly stored as hard copies, today’s businesses often store

---

3. Id.
6. Id. (emphasis added).
7. Merges, supra note 2, at 86 (“Customer lists are generally protectable as trade secrets, but enjoining employees from calling on customers with whom they have had longstanding relationships raises serious concerns about employee mobility.”).
8. See, e.g., Morlife, Inc. v. Perry, 56 Cal. App. 4th 1514, 1521 (1997) (affirming damages award of $39,293.47 for misappropriating confidential customer information in violation of the Uniform Trade Secrets Act where “employer has expended time and effort identifying customers with particular needs or characteristics”).
11. See supra note 9.
easily reproducible client information in their office computers or cellular phones’ internal memories. 12

Another modern development, online social networking, has further complicated the matter of storing client lists. 13 Social networking websites, such as Facebook, MySpace, and LinkedIn, provide users the opportunity to add almost anyone—from social acquaintances to potential business clients—to their contact lists. 14 Each social network emphasizes different features; for example, LinkedIn emphasizes professional networking and claims over 23 million users worldwide, 15 while Facebook, which has over 200 million users, 16 has a more casual feel. Despite the differences between these sites, however, they share the ability to add large numbers of people to one’s personal contact list through the use of simple search features; with a name alone, one can locate contacts and request that they join the user’s contact list. 17 While this characteristic ease in locating contacts may be useful for adding one’s friends or maintaining old relationships, it also raises disclosure issues for businesses trying to keep their customer lists secret. 18

The potential for such abuse in social networking first became apparent in 2008 when a British recruitment company, Hays Recruitment, brought suit against its former employee, Mark Ions, for allegedly copying information from the business’s client lists into his personal LinkedIn contact list before departing. 19 Indeed, Ions allegedly used his LinkedIn contacts to form a competing business

12. Id.
13. See generally infra Part II.A.
19. See Tyler, supra note 15.
three weeks before leaving Hays. The ex-employer successfully obtained an order requiring Ions to disclose his contact list so Hays could discover what contacts, if any, Ions took to form his new business. American courts have not yet faced similar social networking cases, but it is likely that similar issues may arise in the near future. Social networks such as LinkedIn seek to avoid any uses of their websites that may violate the law, so these social networks are paying attention to the liability that their users may potentially face. Surprisingly, few legal scholars have discussed whether online contact lists (as opposed to hard-copy customer lists) should be protectable in light of their unique features.

This Note examines the use of social networks as a means of retrieving and storing client information and also predicts the expansion of contact list protections via tort, trade secret, unfair competition, and contract law into the realm of social networking. The Note is limited to the discussion of contact lists as protectable material, and leaves unexamined various other disclosure risks presented by the proliferation of online social networking. Part I examines American approaches to client lists in trade secret law, including the traditional tort approach, the UTSA approach, the unfair competition approach, and modern contractual approaches. Part II analyzes the secrecy, valuation, employer investment, and precaution elements of a trade secret claim in the context of social

20. Id. Note specifically that Ions claimed he only requested that they confirm him as a friend. Id. This may form the basis for some argument that the contacts were personally known to him, since they did in fact accept his invitation. See id. However, some users routinely accept “friend requests” even when they do not know the requesting user; MySpace user Tila Tequila is a celebrity known in part for her massive friend list (3,535,305 friends as of December 2008); Facebook currently has a 5,000 friend per account limit. See Tila Tequila – Wikipedia, http://www.wikipedia.org/wiki/Tila_Tequila (last visited Mar. 22, 2009); Ryan Singel, Santa Adds Facebook to Naughty List Over Friend Limit, THREAT LEVEL, Sept. 16, 2008, available at http://blog.wired.com/37bsstroke6/2008/09/santa-adds-face.html. Every “friend” on a user’s contact list is not necessarily known personally to the user. See id.

21. See Tyler, supra note 15.

22. See id. (quoting a LinkedIn spokesperson as saying that “[i]t is important that customers abide by their current employment contract and ensure that they have the right to use the information provided”). In emphasizing the role of the employment contract, LinkedIn’s approach to the problem generally reflects the modern contractual approach. See infra Part I.A.4.

23. See generally Research on Social Networking Sites, supra note 18.

networking contact lists. Part III addresses misappropriation and improper acquisition in a social networking contact list context as opposed to traditional forms of client lists, looks at the problems presented when employers encourage social networking, and examines what action specifically triggers disclosure of a trade secret via online contact list. Finally, Part IV presents the Note’s conclusion that courts should extend traditional trade secret protections to information gathered from online contact lists, provided that the current standards protecting employees’ interests remain intact.

I. BACKGROUND: FOUR APPROACHES TO TRADE SECRET MISAPPROPRIATION

A. Legal Approaches to Protecting Client Lists

The American judicial system lacks a unified approach to trade secrets because the federal government does not regulate how they must be protected, allowing each state to apply its own law.25 Several common approaches to the trade secret law, however, have been promoted in the Restatement of Torts, the Restatement (Third) of Unfair Competition, and the UTSA.26 Some form of these approaches, or combination thereof, has been adopted into law in nearly every state.27 Furthermore, many businesses choose to protect their client lists by contracting with their employees in the form of nondisclosure and noncompetition agreements in their employment contracts.28

1. The Tort Approach

The traditional analysis for misappropriation of trade secrets defines disclosure of a trade secret as a unique tort.29 The older common law is codified in the Restatement of Torts, originally published in 1939.30 The Restatement of Torts defines a trade secret as “any formula, pattern, device, or compilation of information which is used in one’s business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it.”31

25. See MERGES, supra note 2, at 35-36.
26. Id.
27. Id. at 36.
29. See MERGES, supra note 2 at 35.
30. See id.; RESTATEMENT OF TORTS (1939).
31. Id. § 757, cmt. b (emphasis added).
The Restatement of Torts specifically mentions customer lists as a form of trade secret.\textsuperscript{32} It further provides that “[o]ne who discloses or uses another’s trade secret, without a privilege to do so, is liable to the other if: (a) he discovered the secret by improper means, or (b) his disclosure or use constitutes a breach of confidence reposed in him by the other in disclosing the secret to him . . . .”\textsuperscript{33} Additionally, the comments to the Restatement of Torts indicate that “protection is afforded only by a general duty of good faith and that the liability rests upon breach of this duty; that is, breach of contract, abuse of confidence, or impropriety in ascertaining the secret.”\textsuperscript{34}

In \textit{Metallurgical Industries Inc. v. Fourtek, Inc.}, the U.S. Court of Appeals for the Fifth Circuit described the requisite elements for a trade secret to exist under the Restatement of Torts approach, including actual secrecy, value in the secret, and cost to develop the secret.\textsuperscript{35} The court held that other elements may be relevant if they appear necessary after an equitable, case-by-case assessment.\textsuperscript{36} Such additional elements may include those provided by the Restatement of Torts itself, which provides six factors: (1) the extent to which the information is known outside the particular secret-holding business, (2) the extent to which it is known within that business, (3) the measures taken to guard the secret, (4) the value of the information to the business and to its competitors, (5) the effort expended in developing the secret, and (6) the ease or difficulty required to properly acquire the information in question.\textsuperscript{37}

The sixth factor in the Restatement of Torts analysis—ease of proper acquisition of the secret—is particularly relevant to the protection of client lists because information compiled from the Internet is often considered easily accessible, and thus not considered secret.\textsuperscript{38} The general rule, according to the Fifth Circuit, is that a customer list “of readily ascertainable names and addresses will not be protected as a trade secret.”\textsuperscript{39} However, in \textit{Zoecon Industries}, the
court found that the information contained in a customer list,\textsuperscript{40} such as type and color of products purchased by the customer, dates of purchase, amounts of purchase, and certain names and addresses, were not known or available to the public.\textsuperscript{41} The court found that even if the names of the customers were readily ascertainable, the large amounts of accompanying information in the list “could be compiled only at considerable expense,” distinguishing a detailed client list from a mere list of names.\textsuperscript{42} Thus, improper disclosure of the detailed list implicated the policy objectives of trade secret protection—namely, protecting those who create valuable compilations of information.\textsuperscript{43} Because all approaches of identifying trade secrets retain the sixth factor of the Restatement of Torts analysis, the inclusion of ancillary client information alongside the list of client names remains an important factor in determining the existence of trade secrets in client lists.\textsuperscript{44}

Some trade secret misappropriation decisions rely on underlying tortious behavior—such as breaking into an employer’s office—in their arguments for finding that a trade secret has been stolen.\textsuperscript{45} However, many cases involve trade secrets taken or distributed by “improper means” that might not otherwise constitute tortious behavior but are still considered improper due to their “devious” nature.\textsuperscript{46} This approach is also embodied in more recent

\footnotesize{Burbank Grease Servs. v. Sokolowski, 693 N.W.2d 89 (Wis. Ct. App. 2005), review granted 700 N.W.2d 271 (Wis. 2005) (finding a list of potential customers readily ascertainable from the Internet, trade associations, and by asking customers whom to contact).}

\textsuperscript{40} See Zoecon Indus., 713 F.2d at 1179. Whether the information in a list is “readily ascertainable” is often a fact-intensive inquiry. Id. Many customer list cases involve specific details of the case, including what information is attached to the customer list and the availability of that information in connection to the names and contact information within the list. See, e.g., id.

\textsuperscript{41} Zoecon Indus., 713 F.2d at 1179.

\textsuperscript{42} Id.; see also Mercer v. C.A. Roberts Co., 570 F.2d 1232 (5th Cir. 1978) (finding that a “mere list of customers,” including information readily ascertainable from other sources, was not protectable as a trade secret).

\textsuperscript{43} See Zoecon, 713 F.2d at 1174.

\textsuperscript{44} See, e.g., Amoco Prod. Co. v. Laird, 622 N.E.2d 912, 918-19 (Ind. 1993) (emphasizing the importance of ease of proper acquisition in granting trade secret protection to plaintiff).

\textsuperscript{45} See RESTATEMENT OF TORTS § 757, cmt. f at 10 (1939).

\textsuperscript{46} See, e.g., Phillips v. Frey, 20 F.3d 623, 631-32 (5th Cir. 1995) (finding implied confidential relationship in the course of negotiations, despite failure by disclosing party to even request confidentiality); E.I. DuPont deNemours & Co. v. Rolfe Christopher, 431 F.2d 1012 (5th Cir. 1970) (finding “improper means of obtaining another’s trade secret” where third party hired aerial photographers to photograph plaintiff’s unfinished plant). Contra Bateman v. Mmnemonic, 79 F.3d 1532 (11th Cir. 1996) (rejecting allegation of implied confidential relationship because parties were unclear as to expectations). For an attempt
treatments of trade secret law, including the UTSA and the Restatement (Third) of Unfair Competition. The history of equity in trade secret law is especially relevant in the context of trade secrets found in online contact lists, since some acts of misappropriation or improper disclosure do not constitute tortious or otherwise illegal behavior.

2. The Uniform Trade Secrets Act Approach

The UTSA is the most common approach used to determine whether certain information constitutes a trade secret. Using language similar to that of the Restatement of Torts, the UTSA defines a trade secret as:

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.

The UTSA provides for injunctive relief, compensatory and exemplary damages, and attorneys fees in cases of “willful and malicious misappropriation.” Furthermore, the UTSA explicitly allows for the provision of alternative remedies by contractual provision.

Applying the UTSA, a California court upheld an award of damages to a former employer, Morlife, against ex-employees who took contact lists to form a competing business. Recognizing both the competing interests of employees’ mobility in employment and a business’s value in its customer list, the court held that employees were only entitled to general skills and knowledge acquired in the

to explain such relationships in terms of “commercial morality,” see 1 MELVIN JAGER, TRADE SECRETS LAW, § 1.03, 1-5.


49. See MERGES, supra note 2, at 36 (noting that the UTSA is adopted in some form or another by forty states and the District of Columbia).

50. See supra Part I.A.1.


53. Id. at § 7(b)(1) (“This act does not affect . . . contractual remedies, whether or not based on misappropriation of a trade secret.”).

course of employment, not specific trade secrets, such as a contact list, that are neither generally known nor readily ascertainable. The court noted that the employer had taken steps to ensure the confidentiality of its customer information, including limiting the circulation of customer lists among its employees and advising them as to the confidentiality and value of the lists through an employment contract and employment handbook. The court found that the former employees misappropriated trade secrets under the UTSA definition by using knowledge of Morlife’s customers to solicit customers for their competitor company. Although the decision in Morlife contrasts with other decisions involving contractual freedom to compete, it emphasizes the importance courts still place on protecting valuable trade secrets, especially where an explicit contractual agreement provides for their protection. Even California, one of the most receptive states to notions of employee mobility, recognizes that taking a contact list from an employer is a taking of valuable property.

3. The Unfair Competition Approach

In another approach to trade secret misappropriation, some courts have emphasized unfair competition rationales based upon principles set forth in the Restatement (Third) of Unfair Competition, published by the American Law Institute in 1993. Liability under this approach is similar to previous approaches; for example, the

---

55. *Id.* at 1519-21 (noting that, had the employees taken only information about contacts known to them, the taking would not have been actionable).

56. *Id.* at 1521.

57. *Id.* at 1522.

58. *See generally, infra* Part I.A.4. States vary widely their approaches to enforcing noncompetition and nondisclosure covenants. *Id.* Further, some states will enforce such contracts differently based upon the job. *Id.* Georgia, for example, does not protect client lists among professionals, even when governed by contractual agreement. *Id.*

59. *See* id.


62. *See*, e.g., Del Monte Fresh Produce Co. v. Dole Food Co., 136 F. Supp. 2d., 1271, 1292-1293 (S.D. Fla. 2001) ("It is not possible to state the precise criteria for determining the existence of a trade secret. The status of information claimed as a trade secret must be ascertained through a comparative evaluation of all the relevant factors. . ."); Wright Med. Tech. v. Grisoni, 135 S.W.3d 561, 588 (Tenn. Ct. App. 2001); see also Ed Nowogroski Ins., Inc. v. Rucker, 971 P.2d 936, 942 (Wash. 1999) (giving a general background of and citing the Restatement (Third) of Unfair Competition with approval); *see generally* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 38 et seq.,(1995).
comments to the Restatement (Third) of Unfair Competition specifically reference the earlier approach adopted in the Restatement of Torts. While the Restatement (Third) of Unfair Competition is specifically intended to update the earlier concepts put forth in the Restatement of Torts, it has yet to be widely adopted, as many states continue to use either the Restatement of Torts or the UTSA.

One peculiar aspect of the Restatement (Third) of Unfair Competition’s approach is its definition of a trade secret as “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.” By including any information that is simply valuable and secret enough to give its possessor a potential economic advantage, this short definition gives a much broader scope to trade secrets than previous attempts to create much more detailed definitions of the term, such as those made in Restatement of Torts and the Uniform Trade Secrets Act. The broader scope afforded by this approach may be advantageous to plaintiffs if they are able to persuade courts to adopt it; however, many courts have not yet been receptive to such an argument, preferring the UTSA statutes, which preempt common law approaches such as the Restatement (Third) of Unfair Competition.

Furthermore, the Restatement (Third) of Unfair Competition recognizes that some contractual approaches protect information that may go beyond the definition of a trade secret. The existence of a trade secret is not necessarily determinative in these contractual cases, so long as the goals of protecting secret and valuable information are accomplished by reasonable contractual means.

63. Id. at § 41, cmt. a (noting, for example, that “[d]isclosure or use of another’s trade secret in breach of a duty of confidence was recognized as a basis of liability in Restatement of Torts § 757(b) (1939). Similar principles are applicable under § 1(2) of the Uniform Trade Secrets Act”); see also JAGER, supra note 46, § 5.043b; ROGER MILGRIM, MILGRIM ON TRADE SECRETS, § 4.03.
64. JAGER, supra note 46, § 3.05.
69. Id. § 41; id. at cmt. d.
4. Confidentiality Agreements and Noncompetition Agreements

Almost every employee must sign an employment agreement of some kind, many of which include confidentiality agreements and noncompetition agreements. These contracts seek to protect confidential information that employees may obtain during the course of their employment as well as to prevent employees from using knowledge obtained from their employer to compete against that employer. While confidentiality agreements are generally enforceable, most jurisdictions limit the scope of these agreements to protect employees.

While many state courts—including those of, most notably, California—have refused to enforce confidentiality and noncompetition agreements, they have found exceptions in certain circumstances. In Moss, Adams & Co. v. Shilling, a California court found that employees did not engage in unfair competition when they used a company rolodex to obtain client addresses for announcing their new business, despite an employment contract providing that such names and addresses were confidential trade secrets. The holding turned in part upon the fact that the defendant ex-employees personally knew their contacts and could not “wipe clean the slate of their memories.” The court found that the defendants only used the rolodex to “obtain some of the addresses of clients whose names they already knew from having personally provided accounting services during the previous year.” Even though it would have been actionable to use trade secrets to solicit former clients, the people named in the rolodex were personally known to the defendants, and thus their identities were not protectable trade secrets under

---

70. MERGES, supra note 2, at 82.
71. Id.
72. Id.; see also RESTATEMENT (THIRD) OF UNFAIR COMPETITION, § 41, cmt. d (1995); MILGRIM supra note 63, at 1.4 (discussing contractual means of protecting trade secrets). For further discussion of noncompetition agreements, which have received a less favorable reception in some states, see supra note 58 and infra note 85.
73. See supra note 58 and infra note 85. California is well known for being particularly protective of employee interests in employment contract disputes. See id.
74. See MERGES, supra note 2.
76. Id. at 129. The holding also turned on the fact that the clients’ addresses and phone numbers, the only ancillary client information found in the rolodex taken by defendants, were readily ascertainable once one knew the clients’ names. Id.
77. Id. at 129-30 (noting that about 600 client names and addresses were in the rolodex, about 29 clients switched to the new business, and no more than 100 clients were contacted).
California law.\textsuperscript{78} Similarly, a Pennsylvania court denied recovery against a former employee salesman partly because he personally developed client contacts.\textsuperscript{79} Since the plaintiff could not prove the list was disclosed in violation of a confidentiality agreement, and since the information was not communicated to the employee by the employer, the court found that it was not inequitable or unjust for the employee to disclose the information to others.\textsuperscript{80}

However, in cases where employees have taken lists of clients not personally known to them, courts have been less sympathetic.\textsuperscript{81} In another California case, an employer obtained damages and an injunction against former employees who memorized a customer list to solicit customers for their competing business.\textsuperscript{82} The court distinguished between an employee’s ability to continue a relationship with a known client and the use of a detailed customer list that included information beyond names and addresses to solicit business from previously unknown clients.\textsuperscript{83} An Illinois court also granted relief to an employer whose former employee memorized client contact information and used that information to solicit business for a competitor.\textsuperscript{84}

In addition to protecting customer lists under confidentiality agreements, some courts have enforced covenants not to compete with former employers, so long as the restrictions therein were reasonable.\textsuperscript{85} In \textit{Comprehensive Technologies Intl. v. Software Artisans, Inc.}, the U.S. Court of Appeals for the Fourth Circuit laid out a three-factor test to determine whether a noncompetition agreement was reasonable, stating that the restraint on the employee must be (1) no greater than necessary to protect the employer’s legitimate business interests, (2) not “unduly harsh and oppressive” in

\begin{itemize}
\item\textsuperscript{78} \textit{Id.} at 130.
\item\textsuperscript{79} \textit{Fidelity Fund, Inc. v. Di Santo}, 500 A.2d 431, 433, 436-37 (Pa. Super. Ct. 1985). The court also found that the customers solicited by Di Santo were not “of special concern or the result of great concentration by plaintiff.” \textit{Id.}
\item\textsuperscript{80} \textit{Id.} at 436-37.
\item\textsuperscript{82} \textit{Klamath-Orleans Lumber, Inc.}, 87 Cal. App. 3d at 458.
\item\textsuperscript{83} \textit{Id.} at 464.
\item\textsuperscript{84} \textit{See Stampede}, 651 N.E.2d at 216-17.
\item\textsuperscript{85} \textit{See MERGES, supra} note 2, at 92. Jurisdictions are divided as to the enforceability of noncompetition agreements. \textit{Id.} For example, California, Alabama, Florida, Louisiana, Montana, and North Dakota all refuse to enforce noncompetition agreements. \textit{Id.} Colorado, Delaware, Massachusetts, and Tennessee refuse to enforce noncompetition agreements in professional settings. \textit{Id.}
curtailing the employee’s legitimate efforts to earn a livelihood, and (3) reasonable in terms of public policy.86

While contractual approaches vary across jurisdictions, they are united in that they allow employers to exercise some degree of control over their employees’ use of client information. In some jurisdictions, contracts may be used to determine whether specific information is a trade secret. In others, they might only serve as notice to employees that the employer intends the information to be secret. Furthermore, they sometimes allow employers to avoid client list misappropriation issues by prohibiting competition after the employee leaves the employer. Regardless of how a jurisdiction acts upon a specific contract, contracting generally allows employers to communicate their expectations to employees formally and specifically.

II. NECESSARY ELEMENTS OF A TRADE SECRET CLAIM

To determine whether taking a contact list is actionable under any of the legal rationales discussed in Part I, one must consider the tort, UTSA, unfair competition, and contractual rationales for protection separately. There are many similarities between the elements of each legal approach to protecting trade secrets, but each has its own nuances.87

There are two critical elements to any claim of trade secret misappropriation: first, whether the subject matter is actually protectable as a trade secret, and second, whether the trade secret was in fact misappropriated.88 Contractual claims, on the other hand, turn largely on whether the state will enforce the type of contract in question and, if so, whether the state finds the specific terms of that contract to be reasonable.89

86. Comprehensive Technologies Int’l., Inc. v. Software Artisans, Inc., 3 F.3d 730, 738 (4th Cir. 1993) (citing Blue Ridge Anesthesia & Critical Care, Inc. v. Gidick, 389 S.E.2d 467, 371-72 (1990), vacated pursuant to settlement) (noting that “reasonable in terms of public policy” includes limitations on the scope, duration, and geographic area of the noncompetition agreement). Furthermore, the Virginia court places the burden of demonstrating reasonability on the employer. Id.

87. See supra Part I. Note particularly the similarities between the trade-secret-as-tort rationale and the unfair competition rationale, as discussed above and as discussed in MERGES, supra note 2. See id. Contrast these with contractual rationales. See supra Part I.A.4.

88. See supra Part I.

89. See supra text accompanying notes 62-76.
A. Is the Subject Matter of Online Contact Lists a Trade Secret?

As a preliminary matter, it must be determined whether the subject matter of online contact lists actually amounts to a trade secret under any of the four approaches discussed in Part I. While other means may exist for protecting information contained in online contact lists, employers may seek to use trade secret protections if applicable, since various conceptions of trade secret law are well established and known to the courts. There are four factors common to each of the three traditional approaches to consider in determining whether an online contact list constitutes a trade secret. First, the information contained in the list must be secret. Second, the information contained in the list must be of value. Third, the owner must have expended resources in developing the list. Fourth, the owner must have taken reasonable precautions to protect the secrecy of the list. Furthermore, the contractual approaches also contain many similar elements.

1. Actual Secrecy

Trade secrets can only exist when the information is actually secret, and not when it is readily ascertainable from information that is generally known. Whether a claimed trade secret is actually secret and whether it can be readily ascertained from general knowledge are fact-intensive inquiries; however, courts have laid out some general rules to help answer these questions. Recall that one important factor is the amount of ancillary client information included in the list beyond a simple iteration of names and addresses. Online contact lists vary greatly from traditional client lists in that

90. See, e.g., Liberty Life Ins. Co. v. Commercial Union Ins. Co., 857 F.2d 945, 947 (4th Cir. 1988) (alleging several causes of action in misappropriation of customer list, including breach of fiduciary duty and conversion); see generally, Kremen v. Cohen, 325 F.3d 1035, 1036 (9th Cir. 2003) (detailing the arguments as to whether intangible property could be the subject of the tort of conversion and certifying the question to the California Supreme Court for a statement of that state’s law).
91. See RESTATEMENT OF TORTS (1939); supra text accompanying note 51.
92. RESTATEMENT OF TORTS, §757, cmt. b (1939).
93. Id.
94. Id.
95. Id.
98. See Metallurgical Indus. Inc. v. Fourtek, Inc., 790 F.2d 1195 (5th Cir. 1986).
99. Id.
100. Id; See Part I.A.1.
they generally include a great deal of ancillary client information.\textsuperscript{101} For example, a Facebook profile may contain information about a user’s recent activities, mood, tastes, pictures, political positions, and other specific characteristics about that person.\textsuperscript{102} Even the more limited LinkedIn profile often contains information about a user’s past educational and employment history, recommendations from coworkers and clients, and associations to which the user belongs.\textsuperscript{103} Furthermore, both sites allow contacts to view each others’ contact lists, making users aware of who knows who.\textsuperscript{104}

While the information contained in a social network profile goes far beyond what is readily ascertainable from a name, address, and phone number,\textsuperscript{105} this alone does not qualify it for trade secret protection.\textsuperscript{106} As in Metallurgical Industries, where information was held to be secret despite limited disclosure to other businesses, the information in question must be a diligently guarded, actual secret, even though complete, or absolute, secrecy is not required.\textsuperscript{107} While LinkedIn and Facebook allow users the option of making their profiles open to the public, recent concerns about privacy have prompted many users to make their profiles accessible only to their immediate contacts or limiting access to certain specified users.\textsuperscript{108} Where profiles

\begin{itemize}
\item \textsuperscript{101} See id. at 1195; Zoecon Indus. v. American Stockman Tag Co., 713 F.2d 1174, 1179 (5th Cir. 1983). As discussed in Part I.A.1, the customer list included purchase order information and other information about the customers, unlike a simple client list only containing names, numbers, and addresses. Id. There are some notable distinctions between the list involved in Zoecon and online contact lists—the purchase order information held by Zoecon was much more specific than what is on an online profile; however, both lists involve information that is not readily ascertainable by the public and can be of considerable value. Id.; see infra notes 102-03. Contrast the detailed customer list in Zoecon Industries with client lists in cases discussed in Part I.A.4, such as Moss, where the unprotectable list simply included names and addresses. Zoecon Indus., 713 F.2d at 1179; Moss, Adams & Co. v. Shilling, 179 Cal. App. 3d 124, 129 (1986). Cf. Burbank Grease Serv. v. Sokolowski, 693 N.W.2d 89 (Wis. Ct. App. 2005) (finding customer list readily ascertainable from the Internet, trade associations, and by asking customers who to contact).
\item \textsuperscript{102} Can You Find the Problems with This Example of a Facebook Profile?, http://sa.uwrf.edu/sa/documents/frednet.facebook-example-profiles.pdf (last visited Feb. 18, 2009).
\item \textsuperscript{103} Allison Doyle, Use Your LinkedIn Profile as a Resume, ABOUT.COM, http://jobsearch.about.com/od/networking/a/linkedinprofile.htm.
\item \textsuperscript{104} See infra notes 166-69. Note that this feature can be disabled, as in the case of employers who wish to keep their contacts secret. Id.
\item \textsuperscript{106} See Metallurgical Indus., 790 F.2d at 1200 (“Although the law requires secrecy, it need not be absolute.”).
\item \textsuperscript{107} Id.
\item \textsuperscript{108} See, e.g., Ian Byrnside, Note, Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants, 10 VAND. J. ENT. &
are specifically made private, so that only contacts authorized by users to view their profiles can see them, the information in those private profiles should be considered actually secret and, thus, should be given trade secret protection.\textsuperscript{109}

Actual secrecy is also important under the UTSA and unfair competition approaches to tortious misappropriation of trade secrets, since the requirements for protection of trade secrets under the UTSA and Restatement (Third) of Unfair Competition are largely the same as those of the traditional tort approach.\textsuperscript{110} Much like other requirements in such cases,\textsuperscript{111} the actual secrecy requirement is a stringent requirement that does away with the potential harshness of punishing employees for unfair competition when they are merely taking advantage of readily ascertainable, public information.\textsuperscript{112}

Under the contractual approaches, courts are divided as to the importance of actual secrecy.\textsuperscript{113} Even publicly known “secrets” may remain protected under contractual approaches, so long as the restrictions are reasonable in scope.\textsuperscript{114} Under a confidentiality or nondisclosure agreement, it may seem harsh to punish an employee for disclosing information that is publically known, but some authorities hold that these disclosures constitute an actionable breach.

\textsuperscript{109} See Smith v. Dravo Corp., 203 F.2d 369, 371-72 (7th Cir. 1953) (protecting information as secret even where owner revealed the secret to others); see also Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 176 (7th Cir. 1991) (finding actual secrecy even where thousands of drawings were in the hands of unauthorized users, in large part because of the reasonable efforts taken to maintain the secrecy of the drawings). These cases raise some interesting issues as to what level of privacy can be expected from a Facebook friend. See Byrnside, supra note 108. One might expect less privacy from Facebook friends than from a potential buyer of secret materials, but more privacy than from a social acquaintance who does not participate in one’s online social network. Cf. Rockwell Graphic Sys., 925 F.2d at 176; Byrnside, supra note 108. Further, the potential for making one’s contacts private may render this discussion moot. See infra Part II.A.4.

\textsuperscript{110} See supra text accompanying notes 57-61.

\textsuperscript{111} See infra Part II.A.2-4.

\textsuperscript{112} See RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 41 (1995). Misappropriation as an act of unfair competition involves many of the same elements as the traditional tort of misappropriation, the relevant element here being secrecy of the information in question. See id.

\textsuperscript{113} See infra text accompanying notes 114-15.

\textsuperscript{114} Cybertek Computer Prod., Inc. v. Whitfield, No. 23911, 1977 Cal. App. LEXIS 2140, at *12 (Cal. Super. Ct. 1977) (“A former employee may be liable for breach of contract if he uses confidential information gained while employed with a former employer, even though such information was not itself a trade secret.”); See also Moss, supra note 75 (finding actual secrecy required, despite a confidentiality agreement in employment contracts).
of confidentiality.\textsuperscript{115} Under noncompetition clauses or nonsolicitation agreements, it should not matter whether the information is public; the terms of the agreement might bar the employee from doing business with the contacts in question.\textsuperscript{116} However, since contract law is the domain of the states and varies widely across jurisdictions, the conditions necessary to protect trade secrets in any given jurisdiction might not include actual secrecy.\textsuperscript{117} Additionally, contractual protections may serve as one indicator that employers made reasonable efforts to maintain secrecy of the information available on their profiles, especially the contents of their contact lists.\textsuperscript{118}

2. Valuable Information

Trade secrets can only exist where the information sought to be protected is of value.\textsuperscript{119} Customer lists have generally been accepted to be of value.\textsuperscript{120} The value of customer lists should extend to online contact lists and compilations of information derived from online contact lists.\textsuperscript{121} The value of online contact lists is clear for many

\begin{footnotesize}
\begin{itemize}
\item[\textsuperscript{115}]
\item[\textsuperscript{116}]
MILGRIM, supra note 63, § 4.02 ("A reasonable covenant, however, restricting solicitation of the employer's customers subsequent to termination of employment may moot the trade secret status of the information since, as a practical matter, the matter may effectively be protected by virtue of 'reasonable' contract rather than trade secret considerations.").
\item[\textsuperscript{117}]
Id. § 4.01 (citing Aronson v. Quick Point Pencil Co., 440 U.S. 257, 262 (1979)) ("Commercial agreements traditionally are the domain of state law. State law is not displaced merely because the contract relates to intellectual property which may or may not be patentable; the states are free to regulate the use of such intellectual property in any manner not inconsistent with federal law."); see also supra note 114.
\item[\textsuperscript{118}]
Schalk v. State, 823 S.W.2d 633, 638, 644 (Tex. Crim. App. 1991); MILGRIM, supra note 63, § 4.02 ("A written agreement can make express and clarify, in an otherwise ambiguous situation, the fact that information is being disclosed, used or developed in the context of a confidential relationship . . . . For parties reluctant to rely upon prediction as to how a court will define a relationship, it is advisable to contractually define the relationship and to state whether it is a confidential one.").
\item[\textsuperscript{119}]
Metallurgical Indus., Inc. v. Fourtek, Inc., 90 F.2d 1195, 1201 (5th Cir. 1986).
\item[\textsuperscript{120}]
See MERGES, supra note 2.
\item[\textsuperscript{121}]
\end{itemize}
\end{footnotesize}
businesses, since conducting business often involves identifying the people who might be customers. The issue is a bit more complicated in service industries, where personal customer contact is often a part of business and employees are more likely to know their clients personally instead of finding them through a centralized contact list. Depending on the particular industry, the information contained in a social networking profile may be more or less valuable; in the Hays-Ions case, for example, the information itself was highly valuable to the departing employee, Mark Ions, who attempted to start a competing recruitment company that would rely on its contacts to generate business.

The value of the information taken is also important under the unfair competition approach; it is precisely because the improperly taken information is valuable that employees are able to compete unfairly against their former employers. Under the contractual approach, the value of the information is much less important because value does not factor into whether a breach occurs. If a court in a particular jurisdiction enforces agreements not to disclose information, the value of that information would not factor into whether the agreement was broken; it might be relevant only insofar as damages are concerned.

Employers and employees often fail to recognize the value in online contact lists. Employers, especially those that are less technologically adept, might view the use of online social networking

---

122. See Tyler, supra note 15.
123. See Moss, Adams & Co. v. Shilling, 179 Cal. App. 3d 124, 129 (1986); see also supra notes 76-77 (detailing different jurisdictional approaches to contacts made in a professional setting, especially protections for personal relationships).
124. See Social Network Service – Wikipedia, supra note 15. In the Hays-Ions case, for example, Ions worked for a recruitment company, where knowing the educational and employment history of clients would be highly valuable. See Tyler, supra note 15. Such information might be less valuable to a propane salesman, although sections of the social networking profile such as “interests” and “activities” might include relevant information such as “grilling” or “scouting troop leader,” which indicate demand for propane. See Social Network Service – Wikipedia, supra note 15. A salesman also might know of private social networking groups or associations that catered to the subject of his sales, giving him a large audience of potential customers that would not be accessible by a general search. Id.; see, e.g., LinkedIn: Mountaineers, http://www.linkedin.com/groups?gid=59765&amp;trk=anetsrch_name&amp;goback=gdr_1235691886202_1 (last visited Mar. 22, 2009).
126. See MILGRIM, supra note 63.
128. See supra text accompanying notes 121, 123-24.
as a waste of company time or as an improper use of Internet resources. However, as the Hays-Ions case and the increasing use of social networking websites by employers has shown, employees create value for their employers when they use social networking sites productively, as Ions did when he used LinkedIn at Hays’ request to find clients for Hays’ recruiting business. Furthermore, even technologically adept employees may fail to recognize the value present in their contact lists. While employees may refer to their social networking time on the job humorously as “notworking,” they fail to see the inherent value in maintaining a form of social contact with distant peers and potential customers who might otherwise be forgotten. The law should recognize the value inherent in such contact lists, even if employers and employees have not yet done so.

3. Investment or Expenditure in Development

Protectable trade secrets generally require some investment or expenditure in their development; at the very least, expenditure in development is an equitable factor weighed by the court. At first glance, it appears questionable whether employers are investing in the development of information on their employees’ and customers’ profile pages. However, some social expenditure is necessarily required to develop a strong contact list—including spending time contacting and communicating with other users to build enough rapport to gain acceptance onto the contact list. Further

129. See Employee Internet Monitoring Could Save Online Reputation, 3AMI, May 8, 2008, http://www.3ami.com/pr-employee-internet-monitoring.htm (advising that not all use is counterproductive, and that monitoring employee Internet usage may help). But see EmployersFriend, http://www.employersfriend.com/managing-emails.htm (last visited Feb. 19, 2009) (finding that social networking costs UK businesses approximately 100 million pounds per year, and arguing that “any company internet policy should” ensure “that staff are not to use social networking sites in working time”).

130. See supra text accompanying notes 32, 108.

131. See supra note 120.


133. See, e.g., Hoover, supra note 24 (discussing several companies’ top-down implementation of social networking).

134. See supra note 2.

135. See generally LinkedIn, About Invitations & Connecting, http://www.linkedin.com/static?key=pop%2Fpop_more_iwe_invitations (last visited Mar. 22, 2009). Adding online contacts involves more than simply adding names to a contact list; the potential contacts must accept the invitation. Id. Some social networking sites particularly stress the importance of having a personal relationship before adding someone as a contact. Id. For example, LinkedIn provides a disclaimer stating, “Important: Only invite people you know well and who know you.” Id. The site also includes a penalty for
expenditure comes through the compilation of the information within the contact list into a cohesive customer list containing ancillary client information beyond a mere listing of names and contact information. In the case of employers who encourage social networking, expenditures may come in the form of paying employees while those employees develop appealing profiles or maintain contact with clients or potential clients through the social network.

Furthermore, as in Zoecon Industries, the cost of creating a client list may come through the process of compiling the information found on clients’ social network pages into a readily usable product. In that case, the court held that “even if the names and addresses were readily ascertainable . . . the other information could be compiled only at considerable expense.” The court valued the employer’s work in compiling its customer list enough to warrant trade secret protection. A similar situation exists when a company compiles a master list of social network contacts and attributes associated with those contacts, with the primary difference being that online lists involve new technologies that have only recently been adopted. Like the list in Zoecon Industries, the expenditure occurs when contact information is provided to the company by third parties but compiled by the company at its own expense.

Nevertheless, trade secret protections for contact lists might be attacked on the grounds that employers make only marginal expenditures to gather the information contained in the lists. After all, the users themselves largely generate the content of social networks, not the company seeking to compile the information. However, recall that, as in previous cases like Zoecon Industries, what

inviting remote contacts; if recipients indicate that they do not know you, you must provide email addresses to add new contacts. Id.

136. See supra text accompanying note 44.
137. See supra notes 56-61.
139. Id.
140. Id.
141. See id.
142. See id. Admittedly, the investment made by the company is not exactly the same in each case; gathering details from social networking contacts would presumably involve transcribing relevant details from the profiles of potential customers rather than creating a specific list aligning customers with prior purchases. See generally Wikipedia – Social Network Service, supra note 15.
143. See id. This argument appears to fail, however, since there are many ways in which an employer invests in the production of a compiled contact list, especially in time paid to employees who compile such lists. See, e.g., Stampede Tool, 651 N.E.2d at 217.
is being protected as a trade secret is not the list of contacts' names alone, but rather the valuable compilation of names and relevant data conducted by the company.145

One counterargument asserts that employees, not employers, spend their resources developing social networking contacts; therefore, employers have no right to trade secret protection in the contact lists generated by their employees.146 This may be particularly problematic where employers encourage employees to develop contact lists on their own personal accounts, as it may be difficult to determine if the networking activity occurred during the employee's personal time or if the activity occurred at the employer's expense.147 However, if employees develop a company profile as a part of their normal work duties, then the company should be able to claim that the employees' social networking was a part of their job, much like any other work employees choose to take home or complete during their free time.148

Alternatively, even if the employer does not invest in the development of the information contained within contact lists, thus disqualifying the lists from trade secret protection, contracts may still protect contact lists made for company use from disclosure or employees' personal use.149 There is no reason why a nondisclosure contract should be contingent upon the employer's expenditures in developing the information the contract seeks to protect.150 Courts should protect client lists compiled from online data by affording such lists trade secret and contractual protections.

4. Reasonable Precautions

The holder of a protectable trade secret must also have taken reasonable precautions to protect the secret.151 In the traditional context of offline customer lists, an employer must have protected the

145. Zoecon Indus., 713 F.2d at 1179; see also E.I. DuPont deNemours & Co., 244 U.S. at 102; Metallurgical Indus., Inc. v. Fourtek, Inc., 90 F.2d at 1199-1202; Zoecon Indus. v. American Stockman Tag Co., 713 F.2d at 1179; Gaal v. BASF Wyandotte Corp., 533 S.W.2d at 155.
146. See supra note 144.
147. See id. If the majority of the content in social networks is user-generated, and employee-users generate that content on their personal profiles, employers may face proof problems in demonstrating that substantial content was generated by employees at work as a part of their job duties. Id.
148. See infra note 154.
149. See supra notes 116-18. However, this is largely dependent on jurisdictional enforcement of such contracts. Id.
151. See, e.g., Rockwell Graphic Sys., 925 F.2d 174, 179 (7th Cir. 1991).
secret through some combination of physical security, list access limitations, and employee contracts that require secrecy.\footnote{152} Several factors complicate the determination of what constitute reasonable precautions in protecting online contact lists.\footnote{153}

First, determining what reasonable precautions are often depends upon the value of the information and the means that would be required to protect the information.\footnote{154} For example, a company building a new type of factory would not be required to enclose its construction to guard against aerial photography; ground-level security would be a reasonable precaution.\footnote{155}

Many employers have begun to encourage their employees to use social networking as a means of client and business development.\footnote{156} An employer that encourages employees to participate in social networking as a means of developing client contacts runs some risk of those employees becoming personally acquainted with the clients, which ends trade secret protection for the contact list in many jurisdictions.\footnote{157} To obtain trade secret protection while encouraging employees to engage in online social networking, employers must exercise control over their employees' online activity, such as specifying what types of contact employees are allowed to make when developing a personal or company profile for company purposes.\footnote{158} For example, a salesman authorized to use a combination of company information and social networks to interact with customers may have a greater deal of leeway in developing personal relationships via social networks than administrative personnel

\footnote{152}{See supra Part I.A.1-2.}
\footnote{153}{See infra text accompanying notes 154-59.}
\footnote{154}{See generally E.I. DuPont de Nemours & Co. v. Rolfe Christopher, 431 F.2d 1012 (5th Cir. 1970). In this case, the court found misappropriation where an aerial photographer took pictures of a production facility that was still under construction. \textit{Id.} at 1013. The court stated that “requir[ing] DuPont to put a roof over the unfinished plant to guard its secret would impose an enormous expense to prevent nothing more than a school boy’s trick.” \textit{Id.} at 1016. Despite the presumably large value of the photos of the unfinished plant, the court found constructing a temporary roof to be too great an expense, and ultimately favored greater protection of business interests over imposing stricter burdens on the business to protect its secrets. \textit{Id.} at 1017.}
\footnote{155}{\textit{Id.}}
\footnote{156}{See Tyler, supra note 15.}
\footnote{157}{See supra text accompanying notes 58, 85. Many jurisdictions do not protect customer information where the customers are personally known to the employees, as in a professional setting. \textit{Id.} Employees who improperly solicit customers that they know only from a central contact list, however, may be found liable for misappropriation of trade secrets.}
\footnote{158}{See infra Part III.}
authorized to update social networking pages and make mass friend requests on behalf of the company and its employees.\textsuperscript{159}

Second, there is some dispute regarding the precise point that an online contact becomes disclosed to the public as non-secret information, giving rise to a dispute about what protective precautions are reasonable.\textsuperscript{160} If courts consider contact disclosed upon invitation to join the employee user's contact list, then the employee user would control disclosure.\textsuperscript{161} If courts considered the contact disclosed upon acceptance of a friend request or contact request by a client, and not the employee, reasonable precautions as to disclosure appear much more difficult to implement, as they would involve controlling the social networking behavior of clients.\textsuperscript{162} However, if privacy features of social networking sites are able to prevent disclosure altogether, it seems reasonable to simply require employees to use these privacy features, avoiding the issue.\textsuperscript{163}

Reasonable precautions are not as important in the contractual approach to protection, again because the contract dictates the employee's behavior.\textsuperscript{164} In general, if the employees contract that they will not disclose contacts as secrets, then those employees bear the burden of keeping those secrets.\textsuperscript{165}

5. Precautions Available on Social Networks

There are some means of protection available for employers seeking to keep their employees' social networking client lists secret.\textsuperscript{166} For example, employers who encourage their employees to use social networking websites could also encourage the creation of

\textsuperscript{159} See See Klamath-Orleans Lumber, Inc. v. Miller, 87 Cal. App. 3d at 462-66; Stampede Tool Warehouse, Inc. v. May, 651 N.E.2d at 214, 216-17; Fidelity Fund, Inc. v. DiSanto, 500 A.2d at 436-37; see also supra note 15.

\textsuperscript{160} See Tyler, supra note 15 (discussing Ions's argument for this defense).

\textsuperscript{161} There may be some difficulty in ascertaining who initiated the friend request; however, when the employer has a list of contacts previously unknown to an employee, and those contacts suddenly appear on the employee's contact list, courts may presume the contact was misappropriated. See, e.g., Klamath-Orleans Lumber, Inc. v. Miller, 151 Cal. Rptr. 118, 120, 122 (Cal. Ct. App. 1978).

\textsuperscript{162} See Tyler, supra note 15. However, in the Hays-Ions case, the British court specifically found that the contacts were disclosed when Ions requested to add the contacts. Id. It is uncertain whether such a disclosure would be found where the contacts were “hidden,” and thus unavailable for unauthorized users to view, through the use of the social network's privacy features. See id.

\textsuperscript{163} See infra Part III.

\textsuperscript{164} See supra Part I.A.4.

\textsuperscript{165} See supra Part I.A.1-2 (detailing general contract rules for confidentiality agreements).

\textsuperscript{166} See infra note 169.
new accounts specifically for use in the workplace; when the employee left the employer, he would not face the same problems of abandoning a profile developed on personal time.\(^{167}\) Furthermore, the employer could easily determine which contacts were located on that account’s contact list, in contrast to a contact list on an employee’s personal account—an account which might be subject to greater privacy protections.\(^{168}\)

On the other hand, employees whose work-related social networking accounts become more popular than their personal accounts may still be disadvantaged when they are forced to leave their work accounts behind. While there may be some employee interest in protecting the fruits of his labor in producing the contact list for the employer, any of the approaches would allow an employee to concede any claim to ownership rights in this work to the employer.\(^{169}\)

Social networking sites’ privacy features provide another possible safeguard against improper disclosure.\(^{170}\) Both Facebook and LinkedIn allow users to adjust the privacy settings on their profiles as desired.\(^{171}\) This includes the ability to restrict the visibility of an employee’s contact list to certain users, perhaps those within the company, or to keep the employee’s contact list completely private.\(^{172}\) This feature would be especially helpful in preventing any wrongful disclosure of the contact list developed on the social network.\(^{173}\)

Creating a private contact list goes beyond simply making the profile viewable only to contacts; using this feature restricts access to

---

\(^{167}\) There have been some questions as to whether employees would be willing to develop separate company profiles. See Hoover, supra note 24 (discussing this issue).

\(^{168}\) See Tyler, supra note 15. Such “personal list protection” was not available for Ions; the court ordered that he disclose the contacts of his list so that his employer could determine which contacts were taken from the workplace. Id.

\(^{169}\) See MERGES, supra note 2, at 82; see generally U.S. v. Dubilier Condenser Corp. 289 U.S. 178 (1933); John C. Stedman, Employer-Employee Relations, in FREDRIK NEUMEYER, THE EMPLOYED INVENTOR IN THE UNITED STATES 29, 40-41 (Fredrik Neumeyer ed., 1971).


\(^{171}\) See supra notes 157-60, 167. Admittedly, this would be somewhat tedious in Facebook where hiding one’s friends list involves adding each excluded user individually. See Facebook – Profile Privacy, http://www.facebook.com/home.php?/view=profile&tab=basic.

\(^{172}\) See supra notes 157-60, 167.

\(^{173}\) See id. Since the privacy feature allows restricted access to one’s contact list and such restrictions are helpful in preventing disclosure of contacts, social networks’ privacy features are helpful in preventing disclosure of the information gathered from the social network, particularly one’s contact list. Id.
everyone but the users themselves. As in other cases where customer list misappropriation has been successfully proven in litigation, only authorized users, in this circumstance, would have access to the trade secret in the contact list.  

Contractual safeguards might be employed as well; these would enhance employers’ claims that they took reasonable precautions to prevent the disclosure of their contact lists. Typical contracts for enforcing these precautions would include nondisclosure agreements, which would prevent outright leaking of the contact list, and also noncompetition agreements, which would preclude departing employees from more discreet forms of disclosure.

In summary, online social networking contact lists should be considered trade secrets because the information found therein is not readily ascertainable, has value, is compiled at the employer’s expense, and reasonable precautions can be taken to safeguard the lists. Admittedly, there are strong arguments that employers do not expend significant resources to develop contact lists and that the nature of online networking precludes employers from taking reasonable protective measures. However, in the balance, these arguments depend on the particular facts of a case, and can often be overcome. In many cases, contact lists should qualify for trade secret protection as customer lists.


175. See Kremen v. Cohen, 325 F.3d 1035, 1036 (9th Cir. 2003) (detailing the arguments as to whether intangible property could be the subject of the tort of conversion, and certifying the question to the California Supreme Court for a statement of that state’s law); Liberty Life Ins. Co. v. Commercial Union Ins. Co., 857 F.2d 945, 947 (4th Cir. 1988) (alleging several causes of action in misappropriation of customer list, including breach of fiduciary duty and conversion); supra notes 62-75 and accompanying text.


177. See supra Part II.A.1.

178. See supra Part II.A.2.

179. See supra Part II.A.3.

180. See supra Part II.A.4.

181. See supra Part II.A.3-4.

182. See Burbank Grease Servs., L.L.C. v. Sokolowski, 693 N.W.2d 89 (Wis. Ct. App. 2005) (finding a list of potential customers readily ascertainable from the Internet, trade associations, and by asking customers who to contact), aff’d in part, rev’d in part, 717 N.W.2d 781 (Wis. 2006).
III. WRONGFUL ACQUISITION AND MISAPPROPRIATION OF CONTACT LISTS

Once the threshold question of whether a trade secret exists has been answered, courts must determine whether that secret was wrongfully acquired or misappropriated. Employees may develop a large contact list in the course of their work. Where the employees personally know the contacts, they may have a right to the contacts; however, where the employees simply appropriate lists wholesale from work accounts to parallel or personal accounts, employees may be liable for wrongful acquisition and misappropriation.

A. Wrongful Acquisition

A departing employee might copy or memorize contacts before leaving his employer. This is a common way for employees to take contact lists; for example, employees might simply copy, print, or memorize their contact lists from their workplace account before leaving. Alternatively, an employee might log onto his work-related social networking account and his personal account in separate web browser windows, moving down the list to send contact requests to his work contacts from his personal account.

One can also imagine a more complicated situation in which an employee does not have distinct accounts, but only has a “personal” account, which includes potentially hundreds of contacts given to him by his employer but hardly known to him. It seems unlikely that the employee would personally know hundreds of customers, which would qualify him for the personal relationship exemption to customer list misappropriation.

183. See generally supra Part I.A.1-4.
184. See supra Part I.A.4. See also notes 58, 85 and accompanying text.
186. See Tyler, supra note 15 and accompanying text. This raises an issue that is not discussed in depth in this Note: at what point is the contact disclosed? Id. Some have argued that the contact is disclosed only when accepted by the contact; however, in the Ions case, the British court found that Ions disclosed contacts by contacting them with requests to join his network. See Tyler supra note 15; Part II.A.4.
187. See supra text accompanying note 20.
188. See supra note 109. Recall that personal knowledge of a customer often exempts an employee from charges of stealing the customer. See Klamath-Orleans Lumber, 151 Cal. Rptr. at 120-21; see also supra note 85.
There are a number of objections to the notion of contact list theft. First, social networking websites reinforce the idea that one’s contacts are personally known to them through the use of terms such as “friends” and “connections.” However, courts should not be persuaded by these terms, considering the relative ease with which contacts are added to an account, regardless of whether they are called “friends,” “connections,” or “customers” on the specific social network. While there is some implication of personhood theories of intellectual property favored by continental theorists, wherein one’s intellectual creations are an expression of the self, inherent to that person, it seems that employees’ interests in hundreds of contacts not personally known to them would be minimal, and outweighed by their employers’ interests in protecting their valuable client lists.

A further argument arises over the issue of whether the online contacts can actually belong to either employer or employee rather than to the social network itself, thus mooting an employer’s claims of wrongful acquisition by an employee. One could argue that the social networking website actually owns these contact lists and the information therein, since users disclaim any ownership interest in them when they sign up to use the website. Such arguments would find support in the terms of service (TOS) of websites such as Facebook. Under the subsection of the TOS entitled “Proprietary

189. See infra text accompanying notes 187, 191, & 198.
190. See supra note 109. For example, Facebook and MySpace refer to one’s contacts as “friends,” and LinkedIn emphasizes adding only contacts who are personally known to the user. See Can You Find the Problems with This Example of a Facebook Profile?, http://sa.uwrf.edu/sa/documents/frednet.facebook-example-profiles.pdf, supra note 102; A Sample Profile – with TMI (Too Much Information), MSNBC, http://www.msnbc.msn.com/id/12210237/; supra note 133. However, in an age where some users have thousands of “friends,” it appears that there is a large potential for the addition of contacts not personally known to the user. See supra note 20.
191. Cf. Moss, Adams & Co. v. Shilling, 224 Cal. Rptr. 456 (Cal. Ct. App. 1986). In this case the clients took a customer list of approximately 600 customers, got 100 hits, and then eventually developed client relationships with 25 of these. Id. Contrast the results in a situation where the customer must simply click to accept someone’s “friendship.” See id.
192. See Margaret Jane Radin, Property and Personhood, 34 STAN. L. REV. 957 (1982) (discussing continental philosophical bases for intellectual property protection as an expression of personhood). Similar personhood rationales for protection might be relevant to an online contact list on one’s own social networking profile. Id.
193. See generally supra notes 37-43.
195. Id.
196. Id. Nevertheless, there are many instances of Facebook use that are intended to generate business or are otherwise commercial; many businesses have groups, profiles, and networks. See, e.g., Facebook – TacoBell, http://www.facebook.com/pages/TacoBell
Rights in Site Content; Limited License,” users of Facebook agree that all property on the site, other than personally generated content, is the property of Facebook and is only licensed to users for personal, non-commercial use; since contact lists would be compiled from information generated by other users, it would belong to Facebook.\textsuperscript{197} However, these restrictions fail to address the situation of the employer and employee as both taking information belonging to the network; the TOS are silent as to an employee’s ability to take information from an employer who breaches the agreement with Facebook by using Facebook’s information to compile detailed customer lists.\textsuperscript{198} The employee in this case might not be able to grant compiled information to his employer, since he only holds a non-commercial license to use the information.\textsuperscript{199} This argument loses force when applied to the more business-oriented LinkedIn website, which only requires users to license information to LinkedIn for use on its website and which actively contemplates use of a user’s contacts in soliciting business.\textsuperscript{200}

Another argument against protection of online contact lists as trade secrets is that the contacts have already been made public by virtue of being posted in an online social network and are thus not sufficiently secret to be wrongfully acquired.\textsuperscript{201} However, considering the available privacy features of networking websites, this argument could only be applied in cases where users chose not to make their information private.\textsuperscript{202} Therefore, this argument largely turns on whether an individual’s contacts have been disclosed simply by being entered into the user’s contact list.\textsuperscript{203} The answer to this question is probably no—depending on the facts of the case—since users have a great deal of discretion in privacy settings.\textsuperscript{204}

\textsuperscript{197} Terms of Use – Facebook, supra note 194.
\textsuperscript{198} See id. Compare Rockwell Graphic Sys., Inc. v. DEV Indus. Inc., 925 F. 2d 174 (7th Cir. 1991), where even though thousands of copies of secret information were held by non-authorized users, the developer did not forfeit trade secret protection against copiers.
\textsuperscript{199} See supra note 194 and accompanying text.
\textsuperscript{201} See Tyler, supra note 15.
\textsuperscript{202} See supra Part II.A.4.
\textsuperscript{203} Id.
\textsuperscript{204} Id. There is no guarantee that privacy settings will remain the same. See Terms of Use – Facebook, supra note 194. It is difficult to predict whether privacy settings on Facebook, LinkedIn, or any social network will become more or less restrictive at some point in the future. See id.
B. Misappropriation

Other than in the course of a traditional tort, another common means of trade secret misappropriation occurs when ex-employees take customer lists by breaching their confidential relationships with their former employers. As noted previously, such confidential relationships may exist either by contract or from an implicit understanding of a confidential relationship between the parties, as is often found in implied in the employer-employee relationship.\(^{205}\) While judicial approaches to contractual duties vary widely across jurisdictions,\(^{206}\) it is difficult to believe that employees would not understand the importance of maintaining secrecy in their employers’ customer lists.\(^{207}\)

As for contractual means of protecting online contact lists, employers may wish to incorporate noncompetition, nondisclosure, or nonsolicitation clauses into employment agreements.\(^{208}\) In jurisdictions that enforce contractual protections for customer lists, the similarities between traditional customer lists and contact lists seem too great to deny enforcement.\(^{209}\) Noncompetition clauses could also be used to reduce the likelihood of employees taking online contact lists from employers.\(^{210}\) If employees could not compete with their previous employers, they would be less likely to want that employer’s contact lists. If treated as a matter of noncompetition, the use of the contact list would probably not factor significantly because the former employee would not be allowed to compete in the same field.\(^{211}\) However, in the case of a breach of the noncompetition agreement, the former employer would want to know which contacts were used by the former employee in forming his competitor

\(^{205}\) See Metallurgical Indus., 790 F.2d at 1200; Zoecon Indus. 713 F.2d at 1178 (“A confidential employment relationship can be established expressly by contract or can be implied from the nature of the relationship. When an employee has an intimate knowledge of the employer’s business, a confidential relationship will be implied.”); see also supra note 109 and accompanying text.

\(^{206}\) See supra text accompanying notes 58-77.

\(^{207}\) See supra note 121. There may be some argument that employees do not recognize the value of secrecy in contact lists. Id. Also, the relative newness of social networking alone may not alert employees to the inherent value of a contact list. See id. Furthermore, questions of who actually developed the contact list may lead employees to argue that the contact list is actually their property. See id; Tyler, supra note 15.

\(^{208}\) See supra Part I.A.4.

\(^{209}\) See supra note 76; supra Part II.A.

\(^{210}\) See supra text accompanying notes 85-86.

\(^{211}\) See id.
company. As in the Hays-Ions case, the disclosure of the former employee's contact list would provide a great deal of evidence for the former employer to make its case for breach of contract. Contractual nondisclosure clauses would face different issues. Once the departed employee left the company, any disclosure of the contacts on his list might be treated as a breach of contract. A breach might occur in a variety of ways; for example, an employee might change the privacy settings on his LinkedIn account, thereby disclosing the formerly secret contacts and allowing competitors to see with whom he has been doing business.

However, the contractual approach to trade secret protection does face certain problems. Objections to enforcing strict contractual obligations include their reasonability and potential effects upon employment and innovation. Furthermore, many jurisdictions, including California, will not enforce many of the contractual provisions discussed. Those jurisdictions see serious policy issues underlying the dispute between enforcement of restrictive employment covenants that are beyond the scope of this Note.

A breach of confidence can also occur without an explicit contractual confidentiality agreement. Whether an employee breaches his employer's confidence implicitly turns on the existence of an implied confidential relationship, which comes about when parties have a reasonable expectation of confidence, often determined by prevailing business standards. Even when competitors freely disclose business information, this disclosure occurs in a context where both parties understand they are discussing a secret subject matter. As argued above, there is not a great enough difference between online contact lists and traditional customer lists to warrant restricting protections to the traditional lists. To be fair, no one should expect employees to give up their real friends and

212. See Tyler, supra note 15; Who Owns Your Online Networking Contacts?, supra note 18; supra text accompanying notes 15 & 18.
213. See supra text accompanying notes 15 & 18.
215. See id.
217. See supra text accompanying note 77.
218. See supra note 73.
219. See Zoecon Indus. 713 F.2d at 1178.
220. Id. at 1176, 1178.
221. See supra Part II.A.
acquaintances simply because their names or personal information were stored in an online contact list occasionally used for work purposes. Nevertheless, employers also have a strong interest in protecting the valuable lists they have generated.

Misappropriation may exist in many forms, including misappropriation via improper means or tortious acts as well as via the breach of confidence. Many of the objections to an employer’s owning information found in their employees’ contact lists rests on a belief that there is some inherent, inalienable part of one’s personality expressed in content that they create, such as a social networking profile. Much like the common law restrictions requiring reasonable terms regarding the length and scope of noncompetition and nonsolicitation agreements, there must be limits of reasonableness as to what contact information employers own after they have compiled information from their employees’ online contact lists. Employees should have ownership rights in their own personal profiles and even the most casual acquaintances. Courts must balance employers’ interests in using their employees to promote the business against employees’ rights to establish their own identities outside of the workplace.

IV. CONCLUSION: A BALANCED APPROACH

There are several approaches to trade secret misappropriation—the traditional tort approaches found in the Restatement of Torts and the UTSA, as well as the unfair competition approach found in the Restatement (Third) of Unfair Competition, which includes some of the many contractual restriction approaches. While there are some arguments regarding who actually owns online social networking contact lists, who actually produced the lists, and, in some cases, who actually disclosed the lists, it is important to note that employers are required to take a great number of precautions in order to receive protection from the courts. In order to assert rights over employees’ online contact lists, employers must be especially vigilant in requiring employees to use the privacy features provided by social networking sites and in making clear to them the confidential nature of any privileged information.

While there are many different online social networking sites, ranging from the largely social MySpace to the business-focused

223. See Radin, supra note 192.
224. See supra Part II.A.4.
225. See generally supra Part I.
LinkedIn, one thing that all social networking websites have in common is their ability to easily connect people from all over the world.\(^{226}\) When companies seek to generate business and find new clients, this ability to find new connections among employees’ existing social networks can be invaluable. When information about potential clients is compiled from these networks at an employer’s expense, such lists closely resemble the type of information previously protected under various trade secret rationales—tortious misappropriation, unfair competition, and contract.\(^{227}\)

However, Internet-based contact lists generate some unique dilemmas because an additional party—the social network—is involved.\(^ {228}\) Furthermore, social networks give users the ability to personalize and control their own online identities, even though social networking is also part of working life. The distinction between an employee’s personal use of social networks and his work-related use is often unclear.

The law remains unsettled as to how to resolve trade secret, unfair competition, and wrongful disclosure issues arising from online social networking at work. Because of this ambiguity, courts should strongly consider employers’ interests in protecting the business investment regarding their employees’ connections and in developing compilations of information about their customers that give them an advantage over their competitors. When employers take reasonable precautions to protect such information, an online list or a list compiled from online data should be treated no differently from traditional forms of client lists, including the protections given to both employers and employees.

*Brian Van Wyk*

---

227. See generally *supra* Part I.
228. See *supra* text accompanying notes 184-89.

*J.D. Candidate, Vanderbilt University Law School, 2010; B.A., University of California, Santa Barbara, 2006. The author wishes to thank the editorial staff of the *Vanderbilt Journal of Entertainment and Technology Law*, especially Austin Broussard and Erica Youngstrom, for their suggestions and assistance throughout the composition of this Note. Finally, the author wishes to thank his parents Patricia and Mitchell Van Wyk for their support, and Christina Cosce for her endless patience and support throughout the production process.