WHO OWNS YOUR FRIENDS?: *PHONEDOG v. KRAVITZ* AND BUSINESS CLAIMS OF TRADE SECRET IN SOCIAL MEDIA INFORMATION

Jasmine McNealy, J.D., Ph.D.*

I. INTRODUCTION

In April 2006, PhoneDog, a technology news and review web site, hired Noah Kravitz to review products, create video blogs, and use other social media outlets to connect current and potential PhoneDog customers to the PhoneDog web site.[1] To connect with customers, PhoneDog tasked Kravitz with maintaining and updating the Twitter account @PhoneDog_Noah, from which he would tweet links to newly posted information and reviews.[2] By all accounts, Kravitz was successful in his employment, as "the @PhoneDog_Noah account generated nearly 17,000 Twitter followers,"[3] and Kravitz became a contributor on CNBC's "Street Signs" and "Fox Business Live" representing PhoneDog.[4] In

* S.I. Newhouse School of Public Communication Syracuse University.

1. PhoneDog v. Kravitz, No. C11-03474 MEJ., 2011 U.S. Dist. LEXIS 129229, at *2 (N.D. Cal. Nov. 8, 2011).

2. *Id.* at *2-3.

3. *Id.* at *3.

4. Notice of Motion and Motion to Dismiss Plaintiff PhoneDog, LLC's Second and Third Claims for Relief in the First Amended Complaint Pursuant to Fed. R. Civ. Proc. Rule 12(b)(6); Memorandum Of Points & Authority in Support Thereof

October 2010, Kravitz left PhoneDog, but instead of relinquishing the @PhoneDog_Noah account as PhoneDog requested, he changed the account handle to @noahkravitz, which he continued to use.[5] In December 2010, Kravitz began working for TechnoBuffalo, a PhoneDog competitor,[6] where he writes product reviews, creates video blogs, and connects with customers, much as he did with PhoneDog.[7]

In 2011, PhoneDog initiated a lawsuit against Kravitz claiming that the @PhoneDog_Noah Twitter account, renamed @noahkravitz, along with its 17,000 followers, was a trade secret.[8] PhoneDog argued that Kravitz's continued use of the account to communicate with followers and connect them to a competing service is misappropriation of that trade secret.[9] According to PhoneDog, Kravitz's misappropriation of trade secrets has caused damage to the company's business and a loss of advertising revenue.[10] As such, the company claims it is owed $340,000 for the industry value of the Twitter followers as well as punitive damages for both intentional and negligent interference with prospective economic advantage and conversion.[11] The federal district court in California granted Kravitz's motion to dismiss on the interference

---

at 4, PhoneDog v. Kravitz, No. C-11-03474 MEJ., 2011 U.S. Dist. LEXIS 129229, at *2 (N.D. Cal. Nov. 8, 2011).

5. *PhoneDog,* 2011 U.S. Dist. LEXIS 129229, at *3.

6. Noah Kravitz's Counterclaims and Answers to Plaintiff's First Amended Complaint For Misappropriation of Trade Secrets, Interference with Prospective Economic Advantage and Conversion at 4, PhoneDog v. Kravitz, No. C11-03474 MEJ., 2011 U.S. Dist. LEXIS 129229, at *2 (N.D. Cal. Nov. 8, 2011).

7. Plaintiff PhoneDog, LLC's Opposition to Defendent Noah Kravitz's Motion to Dismiss for Lack of Subject Matter Jurisdiction and Failure to State Claim at 10, PhoneDog v. Kravitz, No. C11-03474 MEJ., 2011 U.S. Dist. LEXIS 129229, at *1 (N.D. Cal. Nov. 8, 2011).

8. *See PhoneDog,* 2011 U.S. Dist. LEXIS 129229, at *1, *3.

9. *Id.* PhoneDog also claimed that the password to the account constituted a trade secret. *Id.* at *16-17.

10. *Id.* at *11-13.

11. First Amended Complaint for Damages and Injunctive Relief; Misappropriation for Trade Secret; Intentional Interference with Prospective Economic Advantage; Negligent Interference with Prospective Economic Advantage; and Conversion at 10-11, PhoneDog v. Kravitz, No. C11-03474 MEJ., 2011 U.S. Dist. LEXIS 129229, at *1 (N.D. Cal. Nov. 8, 2011).

with prospective economic advantage claims.[12] The trade secret and conversion claims will go to trial.[13]

Although yet to be decided, the *PhoneDog* case raises a novel issue with regard to social media and intellectual property. In an era when businesses are attempting to use new media to gain customers, what does it mean for an employee tasked with maintaining and maximizing the company's social media presence? Will every connection that an employee makes belong, as property, to the company, or will some connections be considered to belong to the employee? Also, should companies be able to claim as a trade secret information that is publicly available to anyone browsing a social media site? *PhoneDog* is not the first case to deal with these issues, yet, very few others do.

This article will examine these issues and related questions. First, this article examines social media, how social media is used to make connections, and business use of the new media platforms. Next, section three explores trade secret and the rules surrounding misappropriation of trade secrets and employee mobility. Section three also offers an analysis of claims of social media as trade secret. Section four analyzes the few other cases found in which a company has asserted an ownership right over a former employee's social media information. Finally, this article will analyze the principles that courts should examine in these cases, and concludes with suggestions on how to avoid these kinds of conflicts.

II. SOCIAL MEDIA AND TRADE SECRET

In general, social media allow users to interact, forming networks and otherwise associating with others that they do or do not know. In fact, searching for friends or acquaintances with whom to connect is one of the norms of social networking.[14] In this

12. *PhoneDog*, 2011 U.S. Dist. LEXIS 129229, at *28.

13. *Id.* at *1-3. Kravitz moved to dimiss the second and third claim again, but was denied. *Id.* at *28.

14. *See* Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship,* 13 J. COMPUTER-MEDIATED COMM. 210, 211 (2008).

way, social media are thought to build social capital through the facilitation of networking, communication, and the creation of trust between users.[15] "What makes social network sites [SNS] unique is not that they allow individuals to meet strangers, but rather that they enable users to articulate and make visible their social networks."[16]

Most social networking websites require users to create profiles and input identifying information as benign as a name or as specific as location information.[17] Users are able to choose the level of detail and precision in the information they provide. Individuals are then able to connect with "friends," "follow" others, send messages, chat, view user-generated media, and otherwise interact using the website as a medium. Those on the network may disclose and exploit information available from other users.[18]

It is not surprising, then, that an increasing number of businesses use these platforms to connect with current and potential customers. All of the big three SNS in the U.S., Facebook, Twitter and LinkedIn, provide businesses with the ability to attract consumers.[19] Facebook, for example, allows users to "like" the pages of celebrities and businesses. LinkedIn, likewise, allows companies to create profile pages with which other site users can

15. Jon M. Garon, *Wiki Authorship, Social Media, and the Curatorial Audience*, 1 HARV. J. SPORTS & ENT. L. 95, 99 (2010). Garon defines social capital as "features of social organization such as networks, norms, and social trust that facilitate coordination and cooperation for mutual benefit." *Id.* at 97 (quoting Anita Blanchard & Tom Horan, *Virtual Communities and Social Capital*, *in* SOCIAL DIMENSIONS OF INFORMATION TECHNOLOGY: ISSUES FOR THE NEW MILLENNIUM, 7 (G. David Garson ed., 2000)).

16. Boyd & Ellison, *supra* note 14, at 211.

17. *See Twitter Privacy Policy,* TWITTER, http://twitter.com/privacy (last visited Jan. 10, 2013).

18. *See* Lee Humphreys, Phillipa Gill & Balachander Krishnamurthy, *How Much is too Much? Privacy Issues on Twitter*, 9 (2010), *available at* http://www.2.research.att.com/~bala/papers/ica10.pdf.

19. *See* Katheryn A. Andresen, *Marketing Through Social Networks: Business Considerations—From Brand to Privacy*, 38 WM. MITCHELL L. REV. 290, 297-99 (2011-2012).

connect. Twitter, as a micro-blogging site,[20] allows companies to speak directly to their consumers. In all cases, businesses are able to take advantage of the SNS platforms to engage current and potential customers directly, and a company is provided with a tally of SNS users with whom it is connected.[21] The company's connections, likes, followers, or friends are visible on the company's profile page.

Unless an SNS user takes steps to protect their profile information, all of their postings and connections are available to public scrutiny.[22] But secrecy is one of the main factors in evaluating the existence of a valid trade secret.[23] A question arises, then, as to whether the use of social media to make connections for business purposes can be the subject of a trade secret.

A. TRADE SECRET LAW

Trade secret protection, in the United States, has its foundations in state common law.[24] Under the classic Restatement approach, trade secret is defined 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."[25] This very broad definition of a trade secret includes almost any information that can be used for a business purpose to acquire a competitive advantage. According to Milgrim, this makes trade secret unlimited as to the "class [or kind] of matter" that is eligible for protection, unlike information that

20. *Microblogging*, HOWTO, http://www.howto.gov/social-media/microblogging (last visited Jan. 10, 2013).

21. *See* Andresen, *supra* note 19, at 298-99 (showing that users' network "addresses" are knowable).

22. *Protecting Your Private Parts on Facebook, LinkedIn, and Twitter,* THE SUITCASE ENTREPRENEUR, http://suitcaseentrepreneur.com/entrepreneurs/protecting-your-private-parts-on-facebook-linkedin-and-twitter/ (last visited Jan. 10, 2013).

23. ROGER M.MILGRIM & ERIC E. BENSEN, MILGRIM ON TRADE SECRETS §1.01 (LexisNexis 2012).

24. *See id.*

25. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995).

would be the subject of copyright or patent protection.[26]

In the mid-1980s, states began adopting the Uniform Trade Secrets Act (UTSA), created by the American Law Institute.[27] Currently 46 states, as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands, have codified the UTSA.[28] The

26. MILGRIM & BENSEN, *supra* note 23.

27. *Id.*

28. *Legislative Fact Sheet – Trade Secrets Act,* UNIF. LAW COMM'N, http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act (last visited Jan. 10, 2013). *See also* ALA. CODE 1975, §§ 8-27-1 to 6 (West, Westlaw through 2012 Reg. and First Spec. Sess.), ALASKA STAT. §§ 45.50.910-945 (West, Westlaw through 2012 2nd Reg. Sess. and Third Spec. Sess), ARIZ. REV. STAT. ANN. §§ 44-401 to 407 (West, Westlaw through Second Reg. Session of the Fiftieth Legis. (2012)), ARK. CODE ANN. §§ 4-75-601 to 607 (West, Westlaw through 2012 Fiscal Sess.), CAL. CIV. CODE §§ 3426-3426.11 (West, Westlaw current with all 2012 Reg. Sess. laws), COLO. REV. STAT. ANN. §§ 7-74-101 to 110 (West, Westlaw through the Second Reg. Sess. and First Extraordinary Sess. of the 68th General Assemb. (2012)), CONN. GEN. STAT. ANN. §§ 35-50 to 58 (2005 & Supp. 2012), DEL. CODE ANN. tit. 6, §§ 2001-09 (West. Westlaw through 78 Laws 2012), D.C. CODE §§ 36-401 to 410 (West, Westlaw through December 11, 2012), FLA. STAT. ANN. §§ 688.001-.009 (West Supp. 2012), GA. CODE ANN. §§ 10-1-760 to 767 (2009 & Supp. 2012), HAW. REV. STAT. ANN. §§ 482B-1 to 9 (West, Westlaw through 2012 Reg. Sess. Act 329), IDAHO CODE ANN. §§ 48-801 to -807 (West, Westlaw through 2012 2nd Reg. Sess. of the 61st Legis.), 765 ILL. COMP. STAT. ANN. 1065/1-9 (West, Westlaw through 2012 Reg. Legis. Sess. P.A. 97-1157 with the exception of 97-1150), IND. CODE ANN. §§ 24-2-3-1 to -8 (West 2006 & Supp. 2011), IOWA CODE ANN. §§ 550.1-.8 (West 2011), KAN. STAT. ANN. §§ 60-3320 to -30 (West 2008 & Supp. 2011), KY. REV. STAT. ANN. §§ 365.880-.900 (LexisNexis 2008 & Supp. 2011), LA. REV. STAT. ANN. §§ 51:1431-39 (2012), ME. REV. STAT. ANN. tit.10 §§ 1541-48 (West 2009 & Supp. 2011), MD. CODE ANN., COM. LAW, §§ 11-1201 to -1209 (LexisNexis 2005 & Supp. 2011), MICH. COMP. LAWS SERV. §§ 445.1901 to .1910 (LexisNexis 2006), MINN. STAT. ANN. §§ 325C.01- 325C.08, (West 2011 & Supp. 2012), MISS. CODE §§ 75-26-1 to -19 (West, Westlaw through 2012 Legis. Sess.), V.A.M.S. §§ 417.450-417.467 (West, Westlaw through 2012 Second Sess.), MONT. CODE ANN. §§ 30-14-401 to -409 (West, Westlaw current with 2011 laws), NEB. REV. STAT. §§ 87-501 to -507 (West, Westlaw through 102nd Legis. Second Reg. Sess. (2012)), N.R.S. 600A.010-600A.100 (West, Westlaw through the 2011 76th Reg. Sess.), N.H. REV. STAT. ANN. §§ 350-B:1-B:9 (West, Westlaw through 2013 Reg. Sess.), NMSA 1978 §§ 57-3A-1 to -7 (West, Westlaw through Second Reg. Sess. Of the 50th Legis. (2012)), NDCC 47-25.1-01 to -08 (West, Westlaw through 2011 Reg. and Spec. Sess. of 62nd Legis. Assemb.), OHIO R.C. §§ 1333.61-1333.69 (LexisNexis 2006 & Supp. 2011), 78 OKL. ST. ANN. §§ 85-94 (West2002 & Supp. 2011)), OR. REV. STAT. §§ 646.461-646.475 (West 2011 & Supp. 2011), 12 PA.CON. .STAT. §§ 5301-5308 (West Supp. 2012), RHODE ISLAND GEN. LAWS

minority of states that have not yet adopted the UTSA maintain the common law approach to trade secret as expressed in the Restatement of Unfair Competition.[29] The purpose of the UTSA was to allow business to protect "commercially valuable" information without having to disclose that information through the patent application process.[30] The UTSA also sought to codify and standardize the basic principles of the common law trade secret, and draws from the principles in the Restatement.[31]

Under the UTSA, a trade secret is any information 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.[32]

Such information can be in the form of a formula, pattern,

1956, §§ 6-41-1 to -11 (2001 & Supp. 2005), S. C. CODE 1976, §§ 39-8-10 to -130 (Supp. 2010), SDCL §§ 37-29-1 to -11 (West, Westlaw through 2012 Reg. Sess.), T.C.A. §§ 47-25-1701 to -1709 (West, Westlaw through 2012 Second Reg. Sess.), UTAH CODE ANN. §§ 13-24-1 to -9 (West, Westlaw through 2012 Fourth Spec. Sess.), VT. STAT. ANN. tit. 9, §§ 4601-4609 (2006), VT. STAT. ANN. tit. 12 § 523 (2006), V.I. CODE ANN. tit. 11 §§ 1001-1010 (West, Westlaw through 2012 Reg. Sess.), VA. CODE 1950, §§ 59.1-336 to -343 (West, Westlaw through 2012 Reg. Sess.), RCWA 19.108.010-19.108.940 (1999), W. VA. CODE, §§ 47-22-1 to -10 (West, Westlaw through 2012 First Extraordinary Sess.), WIS. STAT. ANN. § 134.90 (West, Westlaw through 2011 Act 286), WYO. STAT. ANN. §§ 40-24-101 to -110 (West, Westlaw through 2012 Budget Sess.).

29. *See* N.J. STAT. ANN. 2C § 20-1 (West 2011), TEX. PENAL CODE ANN. § 31.05 (West 2011). New York follows the common law. *See* Michael J. Hutter, *The Case for Adoption of a Uniform Trade Secrets Act in New York*, 10 ALB. L.J. SCI. & TECH. 1, 1-64 (1999-2000) (describing New York's current common law system regarding trade secrets and advocating that it adopt a uniform trade secret law). Massachusetts introduced UTSA legislation 2012. Brian P. Bialas, *Will Massachusetts Adopt the Uniform Trade Secrets Act?*, FOLEY HOAG LLP (Apr. 5, 2012), http://www.massachusettsnoncompetelaw.com/2012/04/articles/trade-secrets/will-massachusetts-adopt-the-uniform-trade-secrets-act/.

30. UNIF. TRADE SECRETS ACT, Prefatory Note (1985).

31. *Id.*

32. *Id.* at § 1.4.

process, etc.[33] Courts have examined six factors enumerated in the 1939 Restatement of Torts when considering whether certain information qualifies for trade secret protection under the UTSA:

> (1) the extent to which the information is known outside of the claimant's business;
>
> (2) the extent to which it is known by employees and others involved in the business;
>
> (3) the extent of measures taken by the claimant to guard the secrecy of the information;
>
> (4) the value of the information to the business and its competitors;
>
> (5) the amount of effort or money expended by the business in developing the information;
>
> (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.[34]

No one factor is more dispositive of trade secret protection than the others, and some courts do not examine all of these factors when deciding whether information is subject to trade secret protection.[35] Nevertheless, one of the essential issues for a plaintiff claiming trade secret protection is secrecy.[36]

1. SECRECY

The consistent aspect of both the Restatement and UTSA approaches to trade secret subject matter is the requirement that a

33. *Id.*

34. RESTATEMENT OF TORTS (FIRST) § 757 cmt. b (1939).

35. *See, e.g.*, Hollingsworth Solderless Terminal Co. v. Turley, 622 F.2d 1324, 1329-35 (9th Cir. 1980); Dicks v. Jensen, 768 A.2d 1279, 1284 (Vt. 2001); Jet Spray Cooler, Inc. v. Crampton, 282 N.E.2d 921, 925 (Mass. 1972); Frantz v. Johnson, 999 P.2d 351, 358-59 (Nv. 2000); Fred Siegel Co., L.P.A. v. Arter & Hadden, 707 N.E.2d 853, 862 (Ohio 1999).

36. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995).

business' competitors not know the information.[37] Information considered general industry knowledge does not qualify for protection.[38]

Every part of the subject matter of a trade secret does not, however, have to be secret to qualify for protection. In *Metallurgical Industries Inc. v. Fourtek, Inc.*, for instance, the Fifth Circuit ruled that a company's claim of trade secret was not vitiated because the scientific principles used were generally known.[39] *Metallurgical Industries* involved the creation of a process and the modification of furnaces that would allow for more efficient reclamation of Tungsten carbide and the recovery of zinc.[40] Metallurgical Industries (M.I.) entered into a contract with Therm-O-Vac Engineering & Manufacturing Company (Therm-O-Vac), a manufacturer, to design and construct two zinc recovery furnaces.[41] M.I. was unsatisfied with the resulting creation and made extensive modifications, which proved successful in making the furnaces useful for commercial operation.[42] A year later, M.I. contacted and shared its design with another manufacturer in hopes of obtaining additional furnaces.[43] When that manufacturer refused to create the furnace as instructed, M.I. returned to Therm-O-Vac for a new furnace.[44]

Therm-O-Vac went bankrupt, and four of its former employees formed Fourtek, another manufacturing operation.[45] When Fourtek was tasked to make a furnace for another company, they did so using the modifications learned from M.I.[46]

At trial for misappropriation of trade secret, Fourtek argued that the basic zinc recovery process used by M.I. was industry

37. *Id.*; UNIF. TRADE SECRETS ACT § 1.
38. Wissman v. Boucher, 240 S.W.2d 278, 280 (Tex. 1951).
39. Metallurgical Indus., Inc. v. Fourtek, Inc., 790 F. 2d 1195, 1199 (5th Cir. 1986).
40. *Id.* at 1197-98.
41. *Id.*
42. *Id.* at 1197.
43. *Id.*
44. *Id.*
45. *Id.* at 1198.
46. *Id.*

knowledge, and that M.I. lost any trade secret protection it would have had by disclosing the information to the companies with which it attempted to contract.[47] The Fifth Circuit found Fourtek's arguments unpersuasive because M.I. had taken measures to ensure the secrecy of its furnace modifications, which included hiding the furnaces from view, restricting access, and requiring those authorized to see the furnaces to sign a non-disclosure agreement.[48] The "subjective belief of a secret's existence suggests that the secret exists."[49] M.I.'s disclosure of the modifications to potential business partners did not vitiate trade secret protection.[50]

Metallurgical Industries provides two important policy reasons for not requiring absolute secrecy with respect to obtaining trade secret protection. First, businesses should be able to disclose information to potential and current business partners.[51] These disclosures were not public announcements, but disclosures of information to entities with whom it wished to collaborate.[52] Second, and related to the first, trade secret law should allow for disclosures for economic purposes.[53] M.I., for example, disclosed the trade secret information to the manufacturers to inquire if they could construct the furnace to M.I. specifications.[54] Disclosures as part of business transactions should not terminate trade secret protection.[55] Confidentiality is only one factor to be considered when examining whether trade secret information should be protected.[56]

2. THE CUSTOMER LIST CONUNDRUM

47. *Id.* at 1199-1200.
48. *Id.* at 1199.
49. *Id.*
50. *Id.* at 1200.
51. *Id.*
52. *Id.*
53. *Id.*
54. *Id.*
55. *Id.*
56. *See id.* (A holder may divulge information to a limited extent without destroying its status as a trade secret).

The secrecy of customer lists, according to some, is one of the most frequently litigated trade secret claims.[57] The Restatement recognizes trade secret protection for customer lists so long as the list is sufficiently secret and economically valuable to the person who created it.[58] Protection for customer lists under the UTSA is similar, and can be discerned from the law's definition of a trade secret. That is, the information must derive economic value from not being generally known, and cannot be readily ascertainable.[59] According to Hillman, although few UTSA states have expressly applied the Act to customer lists, the case law establishes how courts will apply trade secret principles in these cases.[60]

The UTSA definition of trade secret requires a very fact specific inquiry of whether a customer list qualifies for trade secret protection.[61] A determination of whether information is "readily ascertainable" requires that the court examine many factors including, the ease in replication of the list.[62] As a list becomes longer and more complex, the difficulty in independently recreating it increases.[63] Therefore, a list of only the names and contact information of the clients of a business would not be protectable

57. Henry J. Silberberg & Eric G. Lardiere, *Eroding Protection of Customer Lists and Customer Information Under the Uniform Trade Secrets Act*, 42 BUS. L. 487, 487 (1986).

58. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 42 cmt. f (1995).

59. UNIF. TRADE SECRETS ACT § 1(4)(i).

60. Robert W. Hillman, *The Property Wars of Law Firms: Of Client Lists, Trade Secrets and the Fiduciary Duties of Law Partners,* 30 FLA. ST. U. L. REV. 767, 772 (2002).

61. *See generally* Silberberg and Lardiere, *supra* note 57; Morlife, Inc. v. Perry, 56 Cal. App. 4th 1514 (Cal. Dist. Ct. App. 1997), Lillge v. Verity, No. C 07-2748 MHP, 2007 U.S. Dist. LEXIS 73543, at *10 (N.D. Cal. Oct. 2, 2007), ATC Distrib. Group, Inc. v. Whatever It Takes Transmissions & Parts, Inc., 402 F.3d 700, 714 (6th Cir. 2005), JPMorgan Chase Bank, N.A. v. Kohler, No. 3:09CV-677-H, 2009 U.S. Dist. LEXIS 81387, at *3-5 (W.D. Ky. Sep. 8, 2009), Brown v. Rollet Bros. Trucking Co., 291 S.W.3d 766 (Mo. Ct. App. 2009), Fisher BioServices, Inc. v. Bilcare, Inc., No. 06-567, 2006 U.S. Dist. LEXIS 34841, at *52 (E.D. Pa. May 31, 2006), Burbank Grease Serv., LLC v. Sokolowski, 693 N.W.2d 89, 94-97 (Wis. Ct. App. 2005).

62. Hillman, *supra* note 60, at 774.

63. *Id.*

under trade secret law because that information would be ascertainable from public sources without much effort.

When a list includes information that is extensive, i.e. including specialized business information, courts have concluded that the additional information creates a trade secret.[64] In *Lillge v. Verity*, for instance, a federal district court in California ruled that in order for a customer list to qualify as a trade secret, the list must constitute more than just the names of clients.[65] Lists including information about customer preferences and characteristics provide the possessor with a competitive edge. Such information would, therefore, qualify as trade secret, assuming the business took steps to maintain its secrecy.[66]

Furthermore, the creation of a client list requires a business to expend time and other resources cultivating a relationship with each client. According to Hillman, this relationship is what distinguishes a business from other businesses with whom the customer may interact.[67] "The relationship is of value not only to the firm but also to any of its members whom clients may identify as forming part of that relationship."[68] Employees leaving a business may find such relationships valuable for soliciting customers to their new business.

3. THE CASE OF DEPARTING EMPLOYEES

A recent study of trade secret cases in the United States found that in 93% of state trade secret cases, the accused misappropriator was either an employee or business partner; that number was 90%

64. *See* Lillge v. Verity, No. C 07-2748 MHP, 2007 U.S. Dist. LEXIS 73543, at *11 (N.D. Cal. Oct. 1, 2007).

65. *Id.* (granting an injunction against former employee's use of customer list information).

66. *Id.* (citing Western Electro-Plating Co. v. Henness, 180 Cal. App. 2d 442, 445 (Cal. Rptr. 2d 1960)).

67. Hillman, *supra* note 60, at 774.

68. *Id.*

in federal trade secret cases.[69] Elizabeth Rowe states that a business' failure to guard itself against possible employee disloyalty is risky; "it would not be prudent to overestimate employee loyalty and trustworthiness."[70] Indeed employees and business partners are in a unique position with respect to trade secrets, specifically customer lists. Employees and business partners may have daily access to such lists or may have been heavily involved in their creation and development.

The participation of former employees and business partners in the creation and development of client lists poses problems when business plaintiffs sue former employees or business partners for misappropriation of a trade secret. Under the UTSA, there are two possible ways to misappropriate a trade secret; only one definition applies with respect to former employees or business partners.[71] A plaintiff may prove misappropriation of a trade secret by a former employee or business partner if they can prove that the:

> (ii) [D]isclosure or use of a trade secret of another without express or implied consent by a person who;
>
> (A) used improper means to acquire knowledge of the trade secret; or
>
> (B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was;
>
> (I) derived from or through a person who had utilized improper means to acquire it;
>
> (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or

69. David. S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45:2 GONZ. L. REV. 291, 291–334 (2010).

70. Elizabeth A. Rowe, *Information Security and Trade Secrets, in* HARBORING DATA: INFORMATION SECURITY, LAW, AND THE CORPORATION 92, 98 (Andrea M. Matwyshyn ed., 2009).

71. UNIF. TRADE SECRETS ACT § 1(2).

> (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
>
> (C) before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.[72]

Courts have ruled that departing employees have a duty to protect their employer's trade secret, even in the absence of an express contract.[73] When the employee has signed an employment contract, courts impute public policy limitations into the scope and duration of the agreement. In many cases, an employee will have had access to the information at issue in the scope of their job, which brings into question the sufficiency of the steps taken (or not taken) by the employer to ensure the information's secrecy vis a vis staff. In *Fred Siegel Co. v. Arter & Hadden*, the Ohio Supreme Court ruled that there was a triable issue of fact as to whether a firm had taken sufficient steps to protect the secrecy of its client list.[74] In *Fred Siegel*, a law firm maintained its client list on a password-protected computer and kept all hardcopies of the list in lockable cabinets.[75] Additionally, employees were "probably" told that the information was confidential and that they were not allowed to retain copies of the list.[76]

In contrast, when an employee is allowed to retain client list information, courts have not found that the employee misappropriated a trade secret when using such information to contact clients for new employers.[77] In *Robert S. Weiss & Assocs.,*

72. UNIF. TRADE SECRETS ACT § 1(2)(ii).

73. Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 318 (2008-2009) (discussing how when the employee has signed an employment contract, courts impute public policy limitations into the scope and duration of the agreement).

74. Fred Siegel Co., L.P.A. v. Arter & Hadden, 707 N.E.2d 853, 862 (1999).

75. *Id.*

76. I*d.*

77. *E.g.* Robert S. Weiss & Assocs., Inc. v. Wiederlight, 546 A.2d. 525, 539 (Conn. 1988).

Inc. v. Wiederlight, the Connecticut Supreme Court ruled that the former employee of an insurance company did not misappropriate the firm's client list.[78] The former employee having personally developed and serviced the clients on the list was significant in determining whether the trade secret existed.[79] The court found that it was the employee's personal relationship with the customers on the list that allowed him to meet their particular needs; the employee was the only agent with whom customers interacted at the firm.[80]

Wiederlight demonstrates that although a court may consider a customer list to be a trade secret, a former employee will not be said to have misappropriated that secret if he or she was in charge of cultivating the information.[81] This is important to remember for cases like *PhoneDog*, in which a company sues a former employee for misappropriating a social media customer list.[82]

The important questions for the courts in these cases will be (1) whether it was the business or the employee that was responsible for the creation and development of the list, and (2) with whom the customers share a relationship.

III. TURNING SOCIAL MEDIA INFORMATION INTO PROPERTY

To obtain a clearer picture of how the federal district court in California may rule in *PhoneDog*, it is perhaps necessary to examine similar cases. To date, the courts have decided on two reported cases dealing with social media contact information and trade secrets, both in federal district court.[83] In both cases, a business organization sued a former employee or business partner.[84]

78. *Id.*
79. *Id.*
80. *Id.*
81. *Id.*
82. *PhoneDog*, 2011 U.S. Dist. LEXIS 129229, at *1.
83. *See* cases *infra* Part III.
84. *See* cases *infra* Part III.

A. EAGLE V. MORGAN[85]

Eagle v. Morgan is a convoluted case full of counterclaims and crossclaims.[86] For the most part, the subject matter of trade secret claims in this case includes the connections to a LinkedIn account, as well as a cellular telephone number.[87] Linda Eagle, and two other partners, founded Edcomm, Inc., a financial services training business, in 1987.[88] Eagle created a LinkedIn account in 2008, which she used to promote Edcomm and connect with family, colleagues, and "build social and professional relationships."[89] Eagle received assistance in maintaining her account from another Edcomm employee.[90]

In 2010, Eagle and her partners allowed another company to purchase all of the outstanding common shares of Edcomm.[91] In June 2011, Eagle and her partners were terminated from the company.[92] After her termination, Eagle was unable to access her LinkedIn account as the Edcomm owners had changed her password and her account profile to display the new Interim CEO's name and photograph.[93] The remaining information on the profile — the recommendations, awards, and connections — were those of Eagle.[94] Edcomm initiated a suit against Eagle making various common law and statutory claims; Eagle filed suit in a different federal court, making 11 claims against Edcomm.[95] Edcomm countersued, claiming, among other things, misappropriation of a trade secret.[96]

85. Eagle v. Morgan, No. 11-4303, 2011 U.S. Dist. LEXIS 147247, at *1 (E.D.Pa. Dec. 22, 2011).
86. *See id.*
87. *Id.* at *2-8.
88. *Id.* at *1-2.
89. *Id.* at *2-3.
90. *Id.* at *3.
91. *Id.*
92. *Id.*
93. *Id.* at *3-4.
94. *Id.* at *5.
95. *Id.* at *5-6.
96. *Id.* at *9.

As a preliminary issue, the federal district court in Pennsylvania had to apply Pennsylvania state law in deciding whether Edcomm truly had a valid trade secret.[97] Pennsylvania is a UTSA state, and uses the UTSA definition of trade secret, with the express addition of customer lists as protectable information.[98] The court noted that Pennsylvania courts used the six factors from the Restatement in determining whether information qualified as a trade secret.[99] According to the court, neither the LinkedIn account connections, nor the cellular phone number constituted trade secrets.[100] Many of the LinkedIn connections were to Edcomm customers.[101] Edcomm, however, "disclose[d] the identity of more than 1,000 [of its] clients" on the Edcomm website.[102] Further, other LinkedIn connections, those to Edcomm instructors, had similar contact information available on their LinkedIn profiles.[103]

This information, then, was not a trade secret because it was readily ascertainable by the business community and publically known.[104] The court found the cellular phone number was also publicly available, and therefore not a trade secret.[105] Because no trade secret existed, Edcomm's misappropriation of trade secret claim was dismissed.[106]

B. CHRISTOU V. BEATPORT, LLC.

97. *Id.* at *27.
98. 12 PA. CONS. STAT. § 5302 (2004).
99. *Eagle*, 2011 U.S. Dist. LEXIS 147247, at *28-29.
100. *Id.* at *37.
101. *Id.* at *38.
102. *Id.* at *30.
103. *Id.*
104. *Id.* at *37.
105. *Id.*
106. *Id.* It is interesting to note that the court denied Eagle's motion to dismiss Edcomm's misappropriation of an idea claim, stating that there was an issue of fact as to whether Edcomm's employees actually created and maintained the LinkedIn accounts. *Id.* at *38.

The social media trade secret dispute in *Christou v. Beatport* centers on MySpace profile and friends list information.[107] In 1998, Regas Christou, the owner of several nightclubs in the Denver area, hired Bradley Roulier as a talent buyer and booking assistant.[108] After several years, and while still employed by Christou, Roulier and partners founded Beatport, an online music marketplace, for which Christou co-signed a loan in exchange for later partial ownership in the company.[109] Roulier never transferred ownership in the company.[110] Beatport became commercially successful by 2005.[111]

While still employed by Christou, Roulier opened a competing nightclub in 2008.[112] Christou alleged that Roulier used his ownership of Beatport to coerce music acts into refusing to perform at his clubs.[113] As a result, Christou was unable to compete in the nightclub market. Christou filed suit against Beatport claiming, among other things, theft of trade secrets.[114] The federal district court in Colorado denied Beatport's motion to dismiss this claim.[115]

Like Pennsylvania, Colorado is a UTSA state.[116] The Colorado statute specifically includes "listing[s] of names, addresses, or telephone numbers, or other information relating to any business or profession which is secret and of value" as qualifying for trade secret protection.[117] Beatport argued, however, that neither Christou's MySpace profile, nor his MySpace friends list were trade secrets as both were publicly available information.[118] In deciding the merits of Beatport's motion to dismiss, the court

107. Christou v. Beatport, LLC, 849 F. Supp. 2d 1055, 1074 (D. Colo. 2012).
108. *Id.* at 1062.
109. *Id.*
110. *Id.* at 1063.
111. *Id.*
112. *Id.*
113. *Id.*
114. *Id.* at 1063-64.
115. *Id.* at 1077.
116. *See supra* note 28.
117. COLO. REV. STAT. ANN. § 7-74-102(4) (West 2006).
118. *Christou*, 849 F.Supp.2d at 1075.

applied an eight-factor test from the Tenth Circuit.[119] The court noted that Christou attempted to safeguard the profiles through passwords and logins, and restricted that information to his employees.[120]

According to the court, with regard to businesses, the friends list is more than just a list of friends, since it allows access to personal and contact information.[121] It was unlikely, then, that Beatport and Roulier knew the contact information of all of contacts on the list from general experience, even assuming Beatport knew all of their names.[122] Also, given the nature of SNS, Christou's MySpace friends were probably friends with other neighboring nightclubs.[123]

The court weighed the fifth and sixth factors in this case most heavily in terms of determining whether the MySpace information was a trade secret.[124] These factors require the court to examine whether Beatport could have obtained the friend information from a source other than Christou.[125] According to the court, the important aspect was not the names of the friends, but the contact information connected to those names, and that the information was not readily available from outside sources.[126] This favored recognizing the list as a trade secret.[127] The court also considered whether Christou expended significant cost and effort to develop

119. *Id.* at 1074-75 ("(1) whether proper and reasonable steps were taken by the owner to protect the secrecy of the information; (2) whether access to the information was restricted; (3) whether employees knew customers' names from general experience; (4) whether customers commonly dealt with more than one supplier; (5) whether customer information could be readily obtained from public directories; (6) whether customer information is readily ascertainable from sources outside the owner's business; (7) whether the owner of the customer list expended great cost and effort over a considerable period of time to develop the files; and (8) whether it would be difficult for a competitor to duplicate the information.").

120. *Id.* at 1075.

121. *Id.* at 1076.

122. *Id.*

123. *Id.* at 1075 ("It is possible if not probable that plaintiffs' MySpace 'friends' were friends with other Denver clubs.").

124. *Id.*

125. *Id.*

126. *Id.* at 1076.

127. *Id.*

the list, and found that creating SNS information requires expending time, money and resources.[128] As a final consideration, the court examined whether Christou's competitors would be able to duplicate the information.[129] Although acknowledging that Roulier and Beatport could reproduce a complete or almost complete list, the court noted that this would require the exhaustion of a significant amount of time and resources, which would make the new list less useful.[130] Christou, therefore, could maintain a valid claim of trade secret in the MySpace information.[131]

IV. PARSING TRADE SECRETS AND SOCIAL MEDIA

Though small in number, and reaching divergent results, the previously discussed cases should prove useful for courts, like that of *PhoneDog*, with respect to what issues are important in deciding whether trade secret protects social media information. The courts in both *Eagle* and *Christou* used the six Restatement factors to come to their decisions.[132] It may be useful then, to use these same factors to consider the facts in *PhoneDog*, and attempt to predict how the federal district court in California will decide this case.

The first Restatement factor asks the extent the information at issue is known outside of the plaintiff's business.[133] PhoneDog claims that both the Twitter account, and the followers list connected to the account, were the subject of the trade secret.[134] As an initial matter, the password to the Twitter account would not be known outside of PhoneDog's business.[135] Factor two asks the extent to which the information at issue was known by the plaintiff's employees and others involved in the business.[136] The

128. *Id.*
129. *Id.*
130. *Id.*
131. *Id.*
132. *See supra* Part III.
133. RESTATEMENT (FIRST) OF TORTS § 757 cmt b. (1939).
134. *PhoneDog*, 2011 U.S. Dist. LEXIS 129229, at *2.
135. *Id.*
136. *Id.* at *2.

court will also examine PhoneDog's secrecy measures with respect to the Twitter password and followers. These may be the most important factors the court will analyze.

The *Eagle* court ruled that the customer and instructor list information contained in Eagle's LinkedIn connections was not the subject of trade secret protection because Edcomm listed many of those same customers and instructors on its website.[137] In contrast, the *Christou* court found that the business list of MySpace friends could be the subject of trade secret because it also contained contact information.[138] The divergent rulings can be explained if the *Christou* ruling is taken as a fundamental misunderstanding of how social media works. The purpose of social media is to share and consume information.[139] Connections are public, and meant to be so.[140] A business using an SNS platform to generate customers does not change the fact that anyone with an Internet connection can view the business's list of friends or followers.

The *Christou* ruling is problematic with respect to the implications for privacy regarding online social media. For the most part, the courts have ruled that SNS users do not have an expectation of privacy or confidentiality in information that they publicly post on an SNS platform.[141] If one views trade secret as a type of organizational privacy, then the lessons from personal privacy cases may prove useful for comparison. *Moreno v. Hanford Sentinel, Inc*. arose after the principal of a local high school obtained a copy of a teenager's negative commentary about her hometown made on her MySpace page and sent it to the local newspaper.[142] Cynthia Moreno's "An Ode to Coalinga," was published in the letters to the editor section along with Moreno's

137. *Eagle*, 2011 U.S. Dist. LEXIS 147247, at *37.

138. *Christou*, 849 F. Supp. 2d at 1075-76.

139. *See supra* Section II.

140. *See* Boyd & Ellison, *supra* note 14 and accompanying text.

141. *See e.g*., Ledbetter v. Walmart Stores, No. 06-cv-01958-WYD-MJW, 2009 U.S. Dist. LEXIS 126859 (D. Colo. Apr. 21, 2009); Dexter v. Dexter, No. 2006-P-0051, 2007 Ohio App. LEXIS 2388 (Ohio Ct. App. May 25, 2007); McMillen v. Hummingbird Speedway, No. 113-2010 CD, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270 (Pa. Ct. C.P. Sept. 9, 2010).

142. Moreno v. Hanford Sentinel, Inc., 172 Cal. App. 4th 1125, 1128 (2009).

full name.[143] After the publication, Moreno and her family received death threats and were forced to move and close their business.[144]

The California appellate court ruled that Moreno could not prove invasion of privacy because in posting the poem online she made "an affirmative act [that] made her article available to any person with a computer and thus opened it to the public eye."[145] Moreno's use of a non password-protected Internet site removed any limited expectation of privacy she may have had.[146]

Although *Moreno* is not completely analogous to the claim in *Christou* or *PhoneDog*, the principles used in the case are important. An SNS user does not have an expectation of privacy in information posted publicly on the Internet. Christou's alleged customer list was the list of friends publicly connected to his business's MySpace profile. The nature of MySpace removes secrecy as a possibility for Christou's friends list. Of course, if Christou had password protected the profile, and removed it from public view, those facts would weigh in favor of a finding that he had taken measures to protect the secrecy of the list. The MySpace profile was used, however, as a marketing tool. Christou wanted, and perhaps encouraged, the public to view the profile touting the clubs. This should have weighed heavily in favor of a finding that there was no secrecy attached to the list.

The *PhoneDog* court will have to consider whether the Twitter followers list was adequately secret enough to warrant trade secret protection. Like MySpace, the Twitter followers list is publicly displayed on the user's account page. Of course, if PhoneDog had required that Kravitz restrict access to the Twitter page, that would bolster its claim that the information was secret. The Twitter account was used as a marketing tool, inviting the public to follow its tweets. This weighs in favor of the information being ruled readily ascertainable.

143. *Id.*
144. *Id.* at 1129.
145. *Id.* at 1130.
146. *See id.*

At this point it may be prudent to examine what would generally be the final factor considered under the Restatement: the ease or difficulty in reproducing PhoneDog's password and followers list. At the time of Kravitz's departure from PhoneDog, the Twitter account was reported to have 17,000 followers. A customer list of 17,000 individuals, offline, would require significant effort to duplicate. A list of this length would almost certainly be impossible for Kravitz to memorize and reproduce. The nature of social media, however, allows Kravitz to cultivate a list of just as many, if not more, Twitter followers.

The fourth factor examines the value of the Twitter followers attached to that account, and the fifth factor requires that the court analyze how much effort or money PhoneDog spent in developing the Twitter account followers. PhoneDog argued that the value of the 17,000 followers equates to $340,000, based on industry figures.[147] Kravitz, in response, argued that there is no evidence that a Twitter account has monetary value, but that any value related to the account stems from his efforts in tweeting and people's interest in following him.[148] Whatever the case, the court should use an extensive examination of the facts, similar to that used in *Wiederlight*.[149] In that case, the fact that the former employee was the only agent that had a relationship with the clients on the customer list, that the employee was the sole individual responsible for developing and servicing the list, and that the employee was allowed to retain the list, were all factors that weighed in favor of the list not being protected as a trade secret.[150] Therefore, if the *PhoneDog* court finds that Kravitz was the only person responsible for tweeting using the account, and that he alone cultivated a relationship with the Twitter account followers, this should weigh in favor of a finding that the Twitter account followers was not a protectable trade secret.

147. *PhoneDog*, 2011 U.S. Dist. LEXIS 129229, at *3.

148. *Id.* at *9-10.

149. *See supra* text accompanying notes 53-55.

150. Robert S. Weiss & Assocs., Inc. v. Wiederlight, 208 Conn. 525, 539 (1988).

Whatever the result in *PhoneDog*, the federal district court will be required to initiate an extensive culling of facts related to whether this particular kind of social media should be considered protectable under trade secret law. This will be a case of first impression with implications for future cases involving business ownership of social media information. The ruling may prove either advantageous to businesses in that more may now claim that the connections made through SNS are trade secret, or advantageous to those former employees and business partners who may then be able to use this information to initiate competition.

V. ON PROTECTING SOCIAL MEDIA TRADE SECRETS

Cases like *PhoneDog*, *Eagle*, and *Christou*, though novel with respect to the subject matter being claimed as trade secret, demonstrate the continuing conflict between departing employees and business expectations. Although these are cases of first impression, the businesses in the respective cases could have taken measures to protect themselves. These measures are the same as those used by businesses offline, but should prove useful for new media related issues.

- *Non-disclosure agreements*: A non-disclosure agreement is a binding contract between an employer and employee specifying that the employee is not to disclose certain information learned during the course of their employment.[151] Certainly trade secrets could be protected under such agreements. According to Almeling, et al, these agreements, and those with third parties, are the most important kind of measures businesses use to maintain secrecy.[152] Almeling found that non-disclosure

151. *See* BLACK'S LAW DICTIONARY 1152 (9th ed. 2009) (defining as "a contract or contractual provision containing a person's promise not to disclose any information shared by or discovered from a trade-secret holder, including all information about trade secrets, procedures, or other internal or propriety matters").

152. David S. Almeling et al., *supra* note 69, at 322.

agreements were one of the measures demonstrating that a business took reasonable efforts to maintain secrecy.[153] Non-disclosure agreements do four things: establish that the employee will be exposed to trade secrets, identify the subject of the trade secret, prohibit unauthorized use or disclosure, and require the return of all trade secret related information at the termination of employment.[154]

- *Assignments of rights*: Like other kinds of intellectual property, trade secrets are assignable. Assignments of rights provide that all inventions or work-product the employee creates during the scope of his employment belong to the company.[155]
- *Keep'em separated*:[156] Imagine if in *PhoneDog* and *Eagle*, the employees were required to keep separate personal and business social media accounts. The business social media account would have been specifically maintained for business use. When the employee left the organization, the organization would have been able retain control over the separate business profile, and immediately disabled the former employee's access to the information.

All three of these suggestions, and other measures used in the analog world to protect intellectual property, will prove useful for businesses using social media platforms. The use of these measures, both alone and in concert, may help companies avoid the conflict over who owns the rights to social media information.

153. *Id.*

154. Ron S. Brand, *Implementing a Trade Secrets Protection Program,* NON-COMPETE AND TRADE SECRETS (Aug. 16, 2010, 3:23 PM), http://www.noncompetenews.com/post/2010/08/16/Implementing-a-Trade-Secrets-Protection-Program.aspx.

155. *See generally* PFS Distribution Co. v. Raduechel, 332 F. Supp. 2d 1236 (2004).

156. THE Offspring, *Come Out and Play*, on SMASH (Track Record 1994).

Author's addendum: In December 2012 it was reported that Noah Kravitz had agreed to an out of court settlement with his former employer Phonedog.[157] The terms of the settlement were not disclosed.[158] Although we may never know how a court would decide this case, it is still illustrative of the emerging issue of businesses claiming ownership of social media information created or cultivated by their employees. As of February 2013, the @phonedog_noah account had no followers; @noahkravitz had 23,187.[159]

157. Daniel Terdiman, *Curious Case of Lawsuit Over Value of Twitter is Settled*, CNET (Dec. 3. 2012, 4:23PM), http://news.cnet.com/8301-1023_3-57556918-93/curious-case-of-lawsuit-over-value-of-twitter-followers-is-settled/.

158. *Id.*

159. Noah Kravitz's Phonedog Twitter Account, @phonedog_noah, https://twitter.com/phonedog_noah (last visited Feb. 7, 2013); Noah Kravitz's Twitter Account, @noahkravitz, https://twitter.com/noahkravitz (last visited Feb. 7, 2013).