Chicago-Kent Law Review

Volume 84
Issue 3 *Symposium: Data Devolution: Corporate Information Security, Consumers, and the Future of Regulation*

Article 4

June 2009

Trade Secrets, Data Security and Employees

Elizabeth Rowe

TRADE SECRETS, DATA SECURITY AND EMPLOYEES

ELIZABETH ROWE*

INTRODUCTION

Data security is critical to trade secret protection because the value of a trade secret lies entirely in its secrecy. Accordingly, to the extent that security is compromised, the trade secret protection itself can be completely lost even without the company knowing or intending it to happen.[1]

Often when we think about data security we envision preserving trade secrets[2] against outsiders, such as hackers who find their way into the pre-

* Elizabeth A. Rowe is an Associate Professor of Law at the University of Florida Levin College of Law. I am very grateful to Andrea Matwyshyn for allowing me the opportunity to participate in this ground breaking conference on data security. These pages memorialize my remarks at the conference. This piece is also related to my book chapter on this topic. See, *Dangers from the Inside: Employees as Threats to Trade Secrets, in* HARBORING DATA; CORPORATIONS, LAW AND INFORMATION SECURITY (A. Matwyshn, ed, 2009). Thank you to Allison Imber, Luke Napodano, and Gary Sobolevskiy for their research assistance.

1. For a discussion of trade secret law, see, for example, Michael Ahrens, *Wisconsin Confidential: The Mystery of the Wisconsin Supreme Court's Decision in* Burbank Grease Services v. Sokolowski *and Its Effect upon the Uniform Trade Secrets Act, Litigation, and Employee Mobility*, 2007 WIS. L. REV. 1271; Katarzyna A. Czapracka, *Antitrust and Trade Secrets: The U.S. and the EU Approach*, 24 SANTA CLARA COMPUTER & HIGH TECH. L.J. 207 (2008); Sarah Gettings, Burbank Grease Services, LLC v. Sokolowski*: Frustrating Uniformity in Trade Secret Law*, 22 BERKELEY TECH. L.J. 423 (2007); Robert Graham Gibbons & Bryan J. Vogel, *The Increasing Importance of Trade Secret Protection in the Biotechnology, Pharmaceutical and Medical Device Fields*, 89 J. PAT. & TRADEMARK OFF. SOC'Y 261 (2007); David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure*, 59 FLA. L. REV. 135 (2007); Marisa Anne Pagnattaro, *Protecting Trade Secrets in China: Update on Employee Disclosures and the Limitations of the Law*, 45 AM. BUS. L.J. 399 (2008); Julie Piper, *I Have A Secret?: Applying the Uniform Trade Secrets Act to Confidential Information That Does Not Rise to the Level of Trade Secret Status*, 12 MARQ. INTELL. PROP. L. REV. 359 (2008); Elizabeth A. Rowe, *Introducing a Takedown for Trade Secrets on the Internet*, 2007 WIS. L. REV. 1041; Elizabeth A. Rowe, *Saving Trade Secret Disclosures On The Internet Through Sequential Preservation*, 42 WAKE FOREST L. REV. 1 (2007); Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777 (2007).

2. For a discussion of preservation of trade secrets and the risks of their disclosure, see, for example, Tait Graves, *Nonpublic Information and California Tort Law: A Proposal for Harmonizing California's Employee Mobility and Intellectual Property Regimes Under the Uniform Trade Secrets Act*, 2006 UCLA J. L. & TECH. 1; R. Mark Halligan, *Recent Developments in Trade Secrets Law*, 6 J. MARSHALL REV. INTELL. PROP. L. 59 (2006); Sahana Murthy, *Public Concern—A "Newsworthy" Exception to the Grant of Preliminary Injunctions in Trade Secret Cases*, 36 GOLDEN GATE U. L. REV. 219 (2006); Tori Praul, Apple Computer, Inc. v. Does*: An Unsatisfying Resolution to the Conflict Between Trade Secret Law, Journalist's Privilege, & Blogging*, 21 BERKELEY TECH. L.J. 471 (2006); Michael L. Rustad, *The Negligent Enablement of Trade Secret Misappropriation*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 455 (2006); Sharon K. Sandeen, *Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law*, 2006 MICH. ST. L. REV. 667; Kurt M. Saunders, *The Law and*

mises or into computers illegally. The reality is that the biggest threat comes not from outsiders,[3] but internally from those who are the most trusted employees. Recent statistics suggest that eighty percent of computer crimes are committed by employees.[4] With that in mind, it is interesting that companies tend to focus on the technological aspects of data protection while neglecting the most critical component and the biggest threat—employees on the inside.[5]

Ethics of Trade Secrets: A Case Study, 42 CAL. W. L. REV. 209 (2006).

3. For a discussion of outsider threats to trade secrets, see, for example, Robert Bejesky, *Investing in the Dragon: Managing the Patent Versus Trade Secret Protection Decision for the Multinational Corporation in China*, 11 TULSA J. COMP. & INT'L L. 437 (2004); Tait Graves & Alexander Macgillivray, *Combination Trade Secrets and the Logic of Intellectual Property*, 20 SANTA CLARA COMPUTER & HIGH TECH. L.J. 261 (2004); Ted Lee & Leila Ben Debba, *Backdoor Non-Competes in Texas: Trade Secrets*, 36 ST. MARY'S L.J. 483 (2005); Stephen R. Wilson, *Public Disclosure Policies: Can a Company Still Protect Its Trade Secrets?*, 38 NEW ENG. L. REV. 265 (2004); Jonathan D. Carpenter, Note, *Intellectual Property: The Overlap Between Utility Patents, Plant Patents, the PVPA, and Trade Secrets and the Limitations on that Overlap*, 81 N.D. L. REV. 171 (2005); Jermaine S. Grubbs, Comment, *Give the Little Guys Equal Opportunity at Trade Secret Protection: Why the "Reasonable Efforts" Taken by Small Business Should be Analyzed Less Stringently*, 9 LEWIS & CLARK L. REV. 421 (2005); John M. Moye, Recent Development, *The Court of Appeals of North Carolina's Narrow Approach to Trade Secrets Protection in* North Carolina Farm Partnership v. Pig Improvement Company, 83 N.C. L. REV. 1567 (2005).

4. Keith Hearnden, *Computer Criminals are Human, Too*, *in* COMPUTERS IN THE HUMAN CONTEXT: INFORMATION TECHNOLOGY, PRODUCTIVITY, AND PEOPLE 415, 419 (Tom Forester ed., 1989). For further discussion of the sources of threats to trade secrets, see, for example, Clay Calvert & Robert D. Richards, *Journalism Sources as Trade Secrets: Whose Source Is It Anyway?*, 23 WHITTIER L. REV. 985 (2002); Richard A. Epstein, *The Constitutional Protection of Trade Secrets under the Takings Clause*, 71 U. CHI. L. REV. 57 (2004); Yuval Feldman, *Experimental Approach to the Study of Normative Failures: Divulging of Trade Secrets by Silicon Valley Employees*, 2003 U. ILL. J.L. TECH. & POL'Y 105; Gary S. Gaffney & Maria E. Ellison, *A Primer on Florida Trade Secret Law: Unlocking the "Secrets" to "Trade Secret" Litigation*, 11 U. MIAMI BUS. L. REV. 1, (2003); Tait Graves, *Bad Faith and the Public Domain: Requiring a Pre–Lawsuit Investigation of Potential Trade Secret Claims*, 8 VA. J.L. & TECH. 2 (2003); 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 (2003); William L. O'Brien, *Trade Secret Reclamation: An Equitable Approach in a Relative World*, 21 J. MARSHALL J. COMPUTER & INFO. L. 227 (2003); Jeff Danley, Note, Cadence v. Avant: *The UTSA and California Trade Secret Law*, 19 BERKELEY TECH. L.J. 289 (2004); Alex Eaton–Salners, Note, DVD Copy Control Association v. Bunner: *Freedom of Speech and Trade Secrets*, 19 BERKELEY TECH. L.J. 269 (2004).

5. *See, e.g.*, Press Release, U.S. Attorney's Office, S.D.N.Y., U.S. Announces Arrests in Case Involving Scheme to Steal AOL Customer List and Sell it to Spammers 1 (June 23, 2004), *available at* http://www.usdoj.gov/usao/nys/pressreleases/June04/aolcomplaintpr.pdf. On June 23, 2004, a former America Online (AOL) employee was arrested for stealing the provider's entire subscriber list of 37 million consumers and over 90 million screen names, credit card information, telephone numbers, and zip codes and selling them to a spammer who leveraged and resold the information. *Id.* at 1–3. The software engineer who stole the data did not have immediate access to it; he was able to obtain the information by impersonating another employee. *Id.* at 2. Although the initial sale price of the list is unknown, the spammer paid $100,000 for a second sale of updated information with 18 million additional screen names. *Id.* The list was then resold to a second spammer for $32,000 and leveraged by the first spammer in his Internet gambling business. *Id.* at 1. The second spammer sent mass marketing e–mails regarding herbal penile enlargement pills to AOL members. Amended Complaint at 7, U.S. v. Smathers, Filed Under Seal, (S.D.N.Y. 2004). Customer lists are considered a corporate asset and sometimes protectable under trade secret law, which varies from state to state in its scope. *See* Robert G. Bagnall, *Privacy*, *in* INVESTMENT COMPANY REGULATION AND COMPLIANCE 209, 217 (2004)

A company's investment in firewalls,[6] encryption,[7] password protections and other security measures can be completely undermined in one instance by a single employee.[8] This means that a company's trade secrets, that which gives the company its competitive advantage, can be destroyed by a single employee with the click of a mouse.[9] Often and unfortunately, the trade secret misappropriation is not discovered until it is too late. Framing the problem in this way demonstrates the importance of security as it relates to trade secrets.[10]

I. EXAMPLES OF EMPLOYEE DISCLOSURES

Some examples illustrate the problem. The first example involves the Kodak Corporation. Kodak had a process designed to enhance the speed

("Although the value of a customer list may be difficult to estimate, it is clear that it may be a substantial asset.").

6. A firewall is a blocking device that keeps certain Internet traffic out, while allowing desired traffic to pass. ZDNet.com, Definition for: Firewall, http://dictionary.zdnet.com/index.php?d=firewall (last visited Dec. 21, 2009).

7. Encryption is a method of reversibly scrambling the content of a message or database to prevent unintended recipients from understanding it. ZDNet.com, Definition for: Encryption, http://dictionary.zdnet.com/index.php?d=encryption (last visited Dec. 21, 2009).

8. For a discussion of employee crimes, see H. Lowell Brown, *Vicarious Criminal Liability of Corporations for the Acts of Their Employees and Agents*, 41 LOY. L. REV. 279 (1995); Monique C. Lillard, *Their Servants' Keepers: Examining Employer Liability for the Crimes and Bad Acts of Employers*, 43 IDAHO L. REV. 709 (2007); Margaret K. Minister, *Federal Facilities and the Deterrence Failure of Environmental Laws: The Case for Criminal Prosecution of Federal Employees*, 18 HARV. ENVTL. L. REV. 137 (1994); Daniel L. Pines, *Are Even Torturers Immune from Suit? How Attorney General Opinions Shield Government Employees from Civil Litigation and Criminal Prosecution*, 43 WAKE FOREST L. REV. 93 (2008); Derek Brown, California Supreme Court Survey, *A Review of Decisions: December 1997–March 1998*, 26 PEPP. L. REV. 447 (1999); Monica Scales, Case Note, *Employer Catch–22: The Paradox Between Employer Liability for Employee Criminal Acts and the Prohibition Against Ex–Convict Discrimination*, 11 GEO. MASON L. REV. 419 (2002); Dermot Sullivan, Note, *Employee Violence, Negligent Hiring, and Criminal Records Checks: New York's Need to Reevaluate Its Priorities to Promote Public Safety*, 72 ST. JOHN'S L. REV. 581 (1998).

9. For a discussion of how the digital world threatens the protection of trade secrets, see Elizabeth A. Rowe, *Contributory Negligence, Technology, and Trade Secrets*, 17 GEO. MASON L. REV. 1, 14–26 (2009).

10. Companies can take preemptive measures such as instituting strong data control policies to mitigate losses due to employee data theft and mishandling. One such means is through employee handbooks and employee codes of conduct. For a discussion of employee handbooks and employee codes of conduct, see Michael D. Moberly, *What the* Heck's *Going on Here? Some Unexpected Consequences of Employee Handbook Acknowledgments*, 34 IDAHO L. REV. 283 (1998); Deborah A. Schmedemann & Judi McLean Parks, *Contract Formation and Employee Handbooks: Legal, Psychological, and Empirical Analyses*, 29 WAKE FOREST L. REV. 647 (1994); Brian T. Kohn, Note, *Contracts of Convenience: Preventing Employers from Unilaterally Modifying Promises Made in Employee Handbooks*, 24 CARDOZO L. REV. 799 (2003); Rachel Leiser Levy, Comment, *Judicial Interpretation of Employee Handbooks: The Creation of a Common Law Information–Eliciting Penalty Default Rule*, 72 U. CHI. L. REV. 695 (2005); Gabriel S. Rosenthal, Comment, *Crafting a New Means of Analysis for Wrongful Discharge Claims Based on Promises in Employee Handbooks*, 71 WASH. L. REV. 1157 (1996).

and the quality of film manufacturing, known as the 401 process.[11] It is a process that the company kept secret. Kodak employed protective steps to restrict access to the information. For instance, it compartmentalized the information so that no one employee had access to all of the information, and it restricted the information to only a handful of employees on a need-to-know basis.[12] Harold Worden was one of few employees who had access to all of the information. He used his authority to secretly acquire the important documents in the 401 process.[13] He then left Kodak and tried to offer the information to Kodak competitors. Eventually he was apprehended in an FBI sting operation, but by that time he had successfully transferred Kodak trade secret information to the competitors.[14]

In another example, a researcher with IDEXX, Inc. who was responsible for developing and manufacturing vegetarian diagnostic kits became unhappy with her job and began to think about leaving.[15] In the process, she had e-mail communications with a competitor who tried to lure her with promises of potential employment. In her numerous e-mail exchanges with this competitor, she disclosed proprietary information,[16] and she transferred files containing a variety of the company's trade secrets.[17] Ironically, her activities came to light when she accidentally e-mailed her supervisor one of the messages to the competitor with the attached trade secret information.[18] Her employer's discovery was especially fortuitous because the researcher had resigned from the company the day before she inadvertently sent the incriminating e-mail.[19]

The final example involves another well known company, Avery Dennison Corporation.[20] A research chemist started consulting with a competitor in Taiwan, and he visited the competitor to provide seminars. Over a period of several years he transferred trade secret information about Avery Dennison and its manufacturing processes to the competitor.[21] He also exploited his co-workers in the process. He pressured them into divulging

11. Mike Mills, *Testing the Limits on Trade Secrets: Kodak Lawsuit Is Likely to Have Broad Impact on Use of Confidential Data*, WASH. POST, Dec. 9, 1997, at C1.

12. William Fitzpatrick, *Uncovering Trade Secrets: The Legal and Ethical Conundrum of Creative Competitive Intelligence*, 68 S.A.M. ADVANCED MGMT. J., Summer 2003, at 8.

13. *Id.*

14. Mills, *supra* note 11.

15. United States v. Martin, 228 F.3d 1, 6 (1st Cir. 2000).

16. *Id.* at 8.

17. *Id.*

18. *Id.* at 10.

19. *Id.*

20. United States v. Yang, 281 F.3d 534, 540 (6th Cir. 2002).

21. *Id.*

their passwords and computers IDs, so that he could access information that was outside the scope of his responsibilities. His theft was discovered when he happened to appear on hidden video burglarizing the files of one of his superiors.[22]

Given these examples, one may wonder why employers do not pay as much attention to trade secret security as they should. I suspect it might be because they do not realize the legal ramifications of failing to actively protect the trade secret information. The general rule is that a trade secret, once published or disclosed, loses its status as protectable information.[23] Therefore, it is not simply a matter of recovering one's stolen property when a trade secret has been taken or lost. Rather, as these examples illustrate, the entire company may be at risk when a sensitive piece of information becomes public or when it lands in the wrong hands.

II. THE THIRD PARTY PROBLEM

The employer has some recourse through civil misappropriation claims[24] and criminal penalties[25] against an employee who steals its secrets. However, these remedies suffer from limitations. For example, most employees who misappropriate trade secrets may not be caught or even if they are discovered do not have deep pockets, so, any kind of financial restitution for the misappropriation is very limited. More problematic from a legal perspective is that when the information gets into the hands of a third party, such as a competitor or the press, the trade secret owner may have no recourse against that third party, and indeed may not be able to prevent the third party from using the information.[26]

A series of cases involving the Church of Scientology illustrate this problem.[27] You may be aware that the Church conducts very strict patrols

22. Lorin L. Reisner, *Transforming Trade Secret Theft Violations into Federal Crimes: The Economic Espionage Act*, 15 TOURO L. REV. 139, 145 (1998).

23. *See* Rowe, *Saving*, *supra* note 1 at 5.

24. For a discussion of trade secret misappropriation claims, see, for example, Rustad, *supra* note 2.

25. For a discussion of criminal trade secret penalties, see, for example, Mark D. Seltzer & Angela A. Burns, *Criminal Consequences of Trade Secret Misappropriation: Does the Economic Espionage Act Insulate Trade Secrets from Theft and Render Civil Remedies Obsolete?*, 1999 B.C. INTELL. PROP. & TECH. F. 52501 (1999).

26. *See id.* at 5.

27. For a discussion of the Church of Scientology, see Michael Browne, Comment, *Should Germany Stop Worrying and Love the Octopus? Freedom of Religion and the Church of Scientology in Germany and the United States*, 9 IND. INT'L & COMP. L. REV. 155 (1998); Emily A. Moseley, Note, *Defining Religious Tolerance: German Policy Toward the Church of Scientology*, 30 VAND. J. TRANSNAT'L L. 1129 (1997); James Walsh, Survey, *Tax Treatment of the Church of Scientology in the United States and the United Kingdom*, 19 SUFFOLK TRANSNAT'L L. REV. 331 (1995).

of Web sites, and any postings related to the Church. What follows may provide a renewed understanding and appreciation for the Church's vigilance.

In 1991 the Church of Scientology filed a lawsuit against a disgruntled former Church member.[28] In response to the suit, the member filed an affidavit containing sixty-nine pages of documents that the Church considered trade secret information.[29] The Church filed a motion with the court to seal the affidavit,[30] which the court denied.[31] The information therefore remained in the court files, and it was publicly available.[32] Determined to protect the secrecy of the information in the affidavit, the Church undertook extraordinary efforts to keep the information private: it sent a Church member to the courthouse every single day to check out the court file, keep it for the entire day, and return it at the end of the day.[33]

Unfortunately, another disgruntled Church member obtained the affidavit and posted it on the Internet.[34] The Church discovered the sixty-nine page affidavit on the Internet ten days after it was posted, obtained a temporary restraining order from the court, and had it removed.[35] That, however, was not the end of the story as the Church member had already sent a copy of the affidavit to the Washington Post.[36] The Church contacted the Post and requested that the allegedly secret documents be returned.[37] The Post complied.[38] Nevertheless, a reporter from the Post then contacted the clerk's office and requested a copy of the affidavit from the court file.[39] Since the file had never been sealed, the Post received the copy from the court file. The Church then returned to the court, renewed its motion to seal the file, and it was granted.[40]

The Church's success in finally sealing the court file proved to be an empty victory. The Post ran its story using the information that it had received legally from the clerk's office. In response, the Church filed a mi-

28. Religious Tech. Center v. Lerma, 908 F. Supp. 1362, 1364 (E.D. Va. 1995).
29. *Id.*
30. *Id.*
31. *Id.*
32. *Id.* at 1364–65.
33. *Id.* at 1365, 1368.
34. *Id.* at 1364.
35. *Id.*
36. *Id.*
37. *Id.*
38. *Id.*
39. *Id.* at 1365.
40. *Id.*

sappropriation claim against the Post.[41] In the end, the court held that the Post had not misappropriated any trade secrets of the Church because the materials used by the Post had, in fact, not been secret.[42] It had been available on the Internet for ten days, making it public. Accordingly, there was no claim against the Post for trade secret misappropriation.[43] Despite the extraordinary and best efforts of the Church to protect their secrets, they were lost.[44]

A final example of trade secrets getting into the hands of a third party involved the Ford Motor Company.[45] A young man, Mr. Lane, operated a website about Ford.[46] He was a Ford fanatic and published everything having to do with Ford and Ford automobiles.[47] He received Ford documents from an anonymous source, an employee, containing very sensitive internal Ford information that Ford considered to constitute a trade secret.[48] He had discussions with Ford, and informed the company that he was in possession of these materials.[49] They threatened to obtain a temporary restraining order if he published the information.[50] Lane, in turn, became angry, and posted forty of the documents online, including materials that were highly sensitive.[51] Ford sued and obtained a restraining order to prevent the publication of the documents and also to have the site taken down.[52] On appeal, the order was reversed on First Amendment grounds. The court held that Ford could not obtain an injunction because it would be a prior restraint[53]

41. *Id.*

42. *Id.* at 1369.

43. *Id.*

44. For a discussion of the Church of Scientology's litigation strategy in these trade secret cases, see Elizabeth A. Rowe, *Trade Secret Litigation and Free Speech: Is It Time to Restrain the Plaintiffs?*, 50 B.C. L. REV. 1425, 1452–54 (2009).

45. Ford Motor Co. v. Lane, 67 F. Supp. 2d 745 (E.D. Mich. 1999).

46. *Id.* at 747.

47. *Id.*

48. *Id.*

49. *Id.*

50. *Id.*

51. *Id.*

52. *Id.* at 748–49.

53. For a discussion of prior restraint, see Edward L. Carter & Brad Clark, *Death of Procedural Safeguards: Prior Restraint, Due Process and the Elusive First Amendment Value of Content Neutrality*, 11 COMM. L. & POL'Y 225 (2006); D. H. Kaye, *The Propriety of "Facial Challenges" to Prior Restraints on the Use of the Internet for Scientific Speech*, 40 JURIMETRICS J. 445 (2000); Michael I. Meyerson, *Rewriting* Near v. Minnesota: *Creating a Complete Definition of Prior Restraint*, 52 MERCER L. REV. 1087 (2001); Jennifer L. Monk & Robert H. Tyler, *The Application of Prior Restraint: An Alternative Doctrine for Religious Land Use Cases*, 37 U. TOL. L. REV. 747 (2006); Michael D. Seplow & Paul L. Hoffman, *Punishing Pundits:* People v. Dyleski *and the Gag Order as Prior Restraint in High-Profile Cases*, 39 LOY. L.A. L. REV. 1197 (2006); David P. Weber, United States v. Lara*—Federal Powers Couched in Terms of Sovereignty and a Relaxation of Prior Restraints*, 83 N.D.

against the publication of the information and Ford's commercial interests were not enough to justify that kind of prior restraint.[54]

CONCLUSION

The lesson for trade secret owners from these case stories is that they must be vigilant and proactive in maintaining and protecting their trade secrets. It is an ongoing, never-ending process that requires comprehensive security measures, including more than protection against outsiders. Companies must also address the internal threats, which are usually the weakest links in corporate security programs. It is the very trusted employees on the inside that companies should fear.

L. REV. 735 (2007); Richard Favata, Note, *Filling the Void in First Amendment Jurisprudence: Is There a Solution for Replacing the Impotent System of Prior Restraints?*, 72 FORDHAM L. REV. 169 (2003); Irina V. Nirshberg, Note, *Prior Restraint on Speech and Workplace Discrimination: The Clashing of Two Fundamental Rights*, 34 SUFFOLK U. L. REV. 577 (2001); Marla Brooke Tusk, Note, *No–Citation Rules as a Prior Restraint on Attorney Speech*, 103 COLUM. L. REV. 1202 (2003).

54. *Lane*, 67 F. Supp. 2d at 750, 753.