Rethinking "Reasonable Efforts" to Protect Trade Secrets in a Digital World

Elizabeth A Rowe, University of Florida

Available at: https://works.bepress.com/elizabeth_rowe/2/
RETHINKING “REASONABLE EFFORTS” TO PROTECT
TRADE SECRETS IN A DIGITAL WORLD

ELIZABETH A. ROWE∗

I.  INTRODUCTION..............................................................................................................2

II. TRADE SECRET LAW OVERVIEW ..................................................................................7
    A. SOURCES OF THE REASONABLE EFFORTS REQUIREMENT ......................................9
    B. INTERPRETATION FROM THE CASE LAW..........................................................10

III. THE DIGITAL WORLD ..................................................................................................15
    A. EASIER STORAGE AND ACCESSIBILITY .............................................................17
    B. EASIER DISSEMINATION .........................................................................................20
        1. E-Mail ................................................................................................................20
        2. The Internet .........................................................................................................23
        3. Cellular Phones ..................................................................................................27
    C. DATA SECURITY PARALLELS ..................................................................................28

IV. SHOULD REASONABILITY BE REDEFINED IN LIGHT OF KNOWN
    TECHNOLOGICAL RISKS? ..........................................................................................30
    1. Introducing Greater Objectivity into the Analysis ..............................................32
    2. Defendant’s Conduct as a Secondary Consideration ........................................37
    3. Support from Tort law Concepts ..........................................................................38

V. CONCLUSION ..................................................................................................................39

∗ Associate Professor of Law, University of Florida, Levin College of Law.  I am grateful to Jeff Childers and Bill Page for their comments on earlier drafts of this work.  I also thank, for their comments, participants at the Feist, Facts, and Fiction Conference at George Washington University Law School where a part of this Article was delivered, and participants at a faculty workshop at Case Western University Reserve Law School sponsored by the Center for Law Technology and the Arts.  For research assistance I am very grateful to Alicia Phillip, Mi Zhou, and Abbey Morrow.
I. INTRODUCTION

Trade secret misappropriation is pervasive, and every trade secret owner is a potential victim. The very technological tools in use today that increase the efficiency with which companies do business create challenges for trade secret protection. They make trade secrets easier to store, easier to access, easier to disseminate, and more portable, thus increasing the risks that trade secrets will be destroyed. According to an FBI report, the mobility of trade secrets makes them “one of the country’s most vulnerable economic assets.” Many well known companies such as Apple Computer, Inc., Caterpillar, Inc., Charles Schwab & Co., Du Pont, Estee Lauder Cosmetics, the Four Seasons Hotels and Hewlett-Packard have all recently been plaintiffs in trade secret misappropriation cases where the alleged misappropriation involved the use of technological tools to transfer the trade secret information.

The facts of *Four Seasons Hotels & Resorts v. Consorcio Barr* provide a vivid illustration of some of the measures one who is determined to discover trade secret information could pursue to penetrate the very technology on which many businesses rely. The story occurs mostly in Caracas, Venezuela where the defendant, Consorcio, is the owner of the building which housed the Four Seasons Hotel Caracas. Consorcio entered into various agreements with Four Seasons Hotels whereby the Four Seasons would manage the operations of the hotel and license its brand name and trademarks to Consorcio in connection with the operation of the hotel. Pursuant to these agreements, while Consorcio could have received from Four Seasons hard copy print-outs of guest histories upon request, it

---


3 Four Seasons Hotels & Resorts v. Consorcio Barr, 267 F. Supp. 2d 1268, 1271-72 (S.D. Fla.).

4 *Id.* at 1272.
was not entitled to any of the proprietary electronic data that Four Seasons considered trade secret, such as detailed guest information in databases and financial management information.\(^5\)

When Four Seasons refused to grant Consorcio access to this information, Consorcio took drastic measures to obtain the information. To begin with,

a group of Consorcio’s personnel, including armed security guards, forcibly entered the Four Seasons’ computer systems room . . . [and] [u]nder the pretext of self-executing a Venezuelan court order . . . downloaded onto back-up tapes all of the guest information and data stored electronically on [one of Four Seasons’ servers] in Caracas, as well as all of the financial information and data stored electronically on [another Four Seasons] server.\(^6\)

Consorcio personnel (more specifically, the former assistant to the Four Seasons’ Manager of Information Technology) then transferred the downloaded information to a laptop, and using the Four Season’s IT Director’s password gained full access to the databases.\(^7\)

Prior to that time, Consorcio had also taken other steps to acquire Four Seasons’ proprietary data by, for instance, intercepting Four Seasons’ e-mail communications\(^8\) and using a program to attempt to crack Four Seasons’ passwords.\(^9\) Consorcio also hired Bencomo, the former Assistant Systems Administrator at the Four Seasons,\(^10\) who came equipped with inside knowledge of the Four Seasons computer networks as well as the administrative and user passwords.\(^11\) A forensic examination of Bencomo’s

---

\(^5\) *Id.* at 1280-81.

\(^6\) *Id.* at 1279-80.

\(^7\) *Id.* at 1281, 1283.

\(^8\) Four Seasons Hotels & Resorts v. Consorcio Barr, 267 F. Supp. 2d 1268, 1289 (S.D. Fla.).

\(^9\) *Id.* at 1292.

\(^10\) *Id.* at 1293.

\(^11\) *Id.* at 1293, 1294-95.
laptop revealed thirty-eight e-mails sent to Consorcio that contained Four Seasons’ data in encrypted spreadsheets.\(^{12}\) Bencomo is also believed to have engaged in “spoofing”\(^{13}\) to access the Four Seasons network.\(^{14}\)

While not all trade secret misappropriation cases are this dramatic, misappropriation through technology occurs regularly and often surreptitiously. The digital world complicates protection of trade secret information and increases the likelihood of destroying trade secret status of misappropriated information. There is a tension between the need to keep information secret and modern technological methods that allow the information to be easily accessed, reproduced, and disseminated. Information breaches occur most commonly through such activities as “unauthorized access to information, loss of laptop and mobile devices, theft of proprietary information, and insider e-mail abuses,” and more than half of these breaches occur as a result of corporate mismanagement of the information or from insiders who abuse their access.\(^{15}\)

Trade secret law protects valuable business information and inventions more easily and inexpensively than patent protection. Modern trade secret law simply requires that the information be of value and that it be kept secret.\(^{16}\) Secrecy is thus the *sine qua non* of trade secret protection,\(^{17}\) but it can be difficult to accomplish. Because the final determination of whether information will be entitled to trade secret protection is not made until the trade secret owner is in litigation, courts

\(^{12}\) *Id.* at 1296.

\(^{13}\) As described in the case, spoofing occurs when a person in attempting to gain access to a network, sets up a fake IP address which is not traceable back to their own IP address. *Four Seasons Hotels & Resorts v. Consorcio Barr*, 267 F. Supp.2d 1268, 1298, 1304 (S.D. Fla.).

\(^{14}\) *Id.* at 1298.


\(^{16}\) *See Unif. Trade Secrets Act § 1(4) (amended 1985), 14 U.L.A. 538 (2005); Restatement (First) of Torts § 757 cmt. b (1939).*

will second-guess whether the owner did enough to keep the information secret.”

At a fundamental level, “the extent of the property right [in a trade secret] is defined by the extent to which the owner of the secret protects his interest from disclosure to others.” The doctrinal lens through which a court evaluates the sufficiency of protection measures is through the “reasonable efforts” requirement. Did the putative trade secret owner take reasonable efforts to protect the trade secret? While absolute secrecy is not required, the trade-secret owner is expected to show that it took efforts reasonable under the circumstances to protect the secret. This standard is very flexible, and intuitively necessitates a fact intensive case by case determination that considers a host of factors in trying to ascertain reasonableness. It is, however, at the heart of every trade secret misappropriation case and often determines the outcome.

This Article explores a question previously unaddressed in the literature: should the greater risks presented to trade secrets in a digital world change the way that courts evaluate reasonable efforts when a trade secret is misappropriated using some form of computer technology? Should reasonableness be pegged to a “should have known” standard such that courts impute an objective expectation that higher safety precautions will be utilized because of the risks that in today’s digital world trade secrets are easier to access and disseminate? Because the reasonable efforts requirement necessitates consideration of what is reasonable under the circumstances, I argue that the changing circumstances that have come about as a result of new technology requires a reexamination of what security measures are reasonable.

The next Part provides some relevant background on trade secret law and discusses the “reasonable efforts” requirement. Part III introduces

---

18 See In re Innovative Constr. Sys., Inc., 793 F.2d 875, 883 (7th Cir. 1986) (“An indispensable element of a trade-secrets claim is that the information, for which legal protection is sought, be genuinely secret.”)


20 See, e.g., MBL Corp. v. Diekman, 445 N.E.2d 418, 425-26 (Ill. App. 1983) (reviewing plaintiff’s security measures and finding that such measures were insufficient to demonstrate the existence of a protectible trade secret).

the digital world and the way in which electronic technologies has effected how we store, access, and disseminate trade secrets. In Part IV the Article urges courts to give special consideration to the known technological risks that may or may not have been considered by the trade secret owner, rather than continuing to focus on traditional facilities-based measures. It proposes modified guidelines for the reasonable efforts analysis, including consideration of such factors as: (a) the nature of the industry, (b) the nature of the trade secrets and how they were stored, (c) the nature of the measures taken to protect the secrets, and (d) the known risks from storage and protection choices. Accordingly, the framework proposed here should infuse greater consistency into these kinds of cases, which are likely to constitute the bulk of trade secret misappropriation cases within the next few years. The Article concludes, in Part V, that trade secret protection cannot be an after thought. Rather, in order to be reasonable it requires a more conscious, risk assessment approach that better anticipates and ultimately stems the inappropriate dissemination or disclosure of the secrets.
II. TRADE SECRET LAW OVERVIEW

A trade secret can be any information of value used in one’s business that has been kept secret and provides an economic advantage over competitors.22 The wide range of information that can be entitled to trade secret protection include customer lists, costs, sales records, customer information, marketing strategies, secret contract terms, unpublished pricing information, and chemical formulas.23 Trade secrets encompass approximately 80% of the assets of some companies,24 and prior to obtaining patent protection, virtually all inventions are covered by trade secret protection.25

Trade secret law provides protection for facts, ideas, inventions and information. By definition it protects only economically valuable information.26 Accordingly, the kind of proprietary information and innovative concepts that drive the economy tend to fall within the ambit of trade secret law.27 Trade secrets are important to industry and the economy28 because they protect and encourage innovation.29 Part of the


29 See Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 493 (1974); see also Marina Lao, supra note 27, at 1633-34 (noting that corporations are increasingly relying on trade-secret protection).
appeal of choosing trade secret protection over other kinds of intellectual property protection, is the broad scope of information that is protectable and the relative ease with which a business can claim such protection.\textsuperscript{30} A business can, for example, protect trade secrets without complying with a government registration system.\textsuperscript{31}

United States publicly traded companies own an estimated $5 trillion in trade secret information.\textsuperscript{32} Trade secrets are important to businesses of all sizes, from the smallest mom and pop shops to the largest multi-national entities.\textsuperscript{33} They often form the most valuable of companies’ intangible assets,\textsuperscript{34} and the survival of a company may depend on its ability to protect its trade secrets. In the digital age, securing information can be especially daunting because once a trade secret has been disclosed, even if inadvertently, it ceases to be a trade secret.\textsuperscript{35}


\textsuperscript{31} Copyright protection may attach without registration, but registration is necessary before a plaintiff files suit for infringement. Thus, prior to registration, a copyright owner is in a similar situation as the owner of a trade secret who does not know whether the targeted material will indeed be protectable. Registration of a copyright provides a presumption of validity. \textit{See} Bibbero Sys., Inc. v. Colwell Sys., Inc., 893 F.2d 1104, 1106 (9th Cir. 1990).

\textsuperscript{32} See Hutchins, \textit{supra} note 24, at 292.

\textsuperscript{33} \textit{See generally id.; ROBERT P. MERGES, PETER S. MENELL & MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 34-35} (4th ed. 2006) (discussing the importance of trade secrets to small companies).


\textsuperscript{35} While the risk of loss is one that is inherent in choosing this form of protection, it does not necessarily suggest that a trade secret owner should have instead chosen patent protection. The choice of trade secret protection or patent protection must be based on a very careful assessment of the particular information involved and thorough consideration of business and legal factors involving, for example, the nature of the information, the ease with which it can be reverse engineered, and the feasibility and cost of obtaining patent protection. \textit{See generally Andrew Beckerman-Rodau, The Choice between Patent Protection and Trade Secret Protection: a Legal and Business Decision}, 84 J. PAT. & TRADEMARK OFF. SOC’Y 371 (2002). Accordingly, one who chooses trade-secret protection over patent protection has not necessarily forgone a “better” form of protection, especially since there is a wide range of information that is eligible for trade-secret protection but not patent protection. \textit{See JAMES POOLEY, TRADE SECRETS § 3.01[1] [a]
A. Sources of the Reasonable Efforts Requirement

Trade secret law is governed by state law, and the manner in which the reasonable efforts requirement enters into a trade secret misappropriation analysis will be determined by the source of trade secret law followed by that state. Regardless whether the state follows the Restatement of Torts, the Uniform Trade Secrets Act (“UTSA”), or the Restatement of Unfair Competition, the reasonable efforts requirement is a critical part of the analysis. Indeed, it is the most important factor in determining whether the plaintiff has a protectible trade secret.37

The UTSA includes reasonable efforts as part of the definition of a trade secret.38 Accordingly, in order to qualify for trade secret protection the information must be “the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”39 The Restatement of Torts also includes “the extent of measures taken by [the trade secret owner] to guard the secrecy of the information” as one of six factors to be considered in determining whether information qualifies as a trade secret.40

Finally, unlike the UTSA and the Restatement of Torts, the Restatement of Unfair Competition does not include reasonable efforts in defining a trade secret.41 However, in determining whether the acquisition of a trade secret was improper the Restatement of Unfair Competition calls

---


37 See, e.g., MBL Corp. v. Diekman, 445 N.E.2d 418, 425 (Ill. App. 1983) (“Although many factors should be considered to determine if a trade secret exists, what is of primary importance is ‘whether and how an employer acts to keep the information secret.’”) (quoting Lincoln Towers Ins. Agency v. Farrell, 425 N.E.2d 1034, 1037 (Ill. App. 1981)).


40 Restatement (First) of Torts § 757 cmt. b (1939).

41 RESTATEMENT OF UNFAIR COMPETITION § 39 defines 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.” RESTATEMENT (THIRD) UNFAIR COMPETITION § 39 (1995).
for an evaluation of “the extent to which the acquisition was facilitated by the trade secret owner’s failure to take reasonable precautions against discovery of the secret by the means in question.” It further suggests that the “foreseeability of the conduct through which the secret was acquired” should be relevant to determining reasonableness.

The Economic Espionage Act, the federal criminal trade secret statute, also includes a reasonable efforts requirement. Similar to the UTSA, it is included in the definition of a trade secret requiring that “the owner thereof has taken reasonable measures to keep such information secret.” That provision has withstood a void for vagueness challenge, with a court finding that the term “reasonable measures” is not unconstitutionally vague.

**B. Interpretation from the Case Law**

While the above sources of law provide the underpinning for the reasonable efforts requirement, they do not provide guiding standards to the courts on how to determine whether the requirement has been met. The interpretation of the requirement appears to be similar in all jurisdictions such that for the purposes of this Article no further distinctions are necessary between UTSA and non-UTSA states. Absolute secrecy is not required. Rather, the standard is one of relative secrecy and a trade secret owner needs to take steps that are reasonably necessary under the circumstances to maintain secrecy. The plaintiff must take affirmative steps and show concrete efforts to preserve the confidentiality of the alleged

---


43 Id.


45 § 1839(3)(A).


48 See UNIF. TRADE SECRETS ACT § 1 cmt. (amended 1985), 14 U.L.A. 538 (2005); see, e.g., Sheets v. Yamaha Motors Corp., 849 F.2d 179, 183-84 (5th Cir. 1988).

49 Sheets v. Yamaha Motors Corp., 849 F.2d at 183.
secret information. Some courts note, for example, that in addition to requiring employees to sign confidentiality agreements, “reasonable efforts” can include “advising employees of the existence of a trade secret, limiting access to the information on a need to know basis, and keeping secret documents under lock.” The use of security guards, closed circuit television monitors, access codes for information stored on a computer, and the use of varying security access levels for different areas of the facilities have also proven reasonable. For ease of reference, this Article refers to these efforts as traditional facilities-based measures (vis-à-vis technical measures and processes).

Efforts to protect secrecy are also tied to the requirement that trade secrets have value and indeed, whether or not a company took adequate steps to protect a secret is evidence of the subjective belief that the information was a trade secret, and thus worthy of protection. Some courts may reason that there is a direct relationship between the value of the information and the extent of measures taken to protect it, such that the more valuable the information to the company the more costly or extensive the measures ought to be to protect it. Where a plaintiff has made a strong showing of reasonable efforts to protect the trade secret information,

---

50 See, e.g., Niemi v. Am. Axle Mfr. & Holding, Inc., No. 269155, 2007 Mich. App. LEXIS 22, * 10-11 (Ct. App. Jan. 4, 2007) (granting summary judgment in favor of defendant, and finding that plaintiff did not take concrete efforts to preserve the confidentiality of designs by, for instance, failing to mark the documents as confidential or requiring confidentiality agreements); see also Dicks v. Jensen, 768 A.2d 1279, 1284 (2001) (granting summary judgment in favor of defendant where there was “no evidence in the record that plaintiff took any measures to indicate that the customer list was confidential.”)


53 See Metallurgical Indus. Inc. v. Fourtek, Inc., 790 F.2d 1195, 1199-1200 (5th Cir. 1986) (reasoning that secrecy measures constitute evidence probative of existence of a trade secret).

a court is also more likely to infer that the defendant used improper means to obtain the information. 55

The courts have made clear that a trade secret owner who itself is lax about taking precautions to prevent the secret from escaping cannot expect to hold others to a higher obligation to preserve the secret. 56 In that sense, a court may use the reasonable efforts requirement to determine whether the plaintiff is entitled to a remedy under the law. 57 As one court aptly noted,

[i]f [plaintiff] expended only paltry resources on preventing its . . . drawings from falling into the hands of competitors . . . why should the law, whose machinery is far from costless, bother to provide [plaintiff] with a remedy? The information contained in the drawings cannot have been worth much if [plaintiff] did not think it worthwhile to make serious efforts to keep the information secret. 58

Indeed, where a trade secret owner fails to adequately follow safeguards that it has instituted, a court could find such conduct vis-à-vis the defendant’s to be unreasonable. 59

55 Id. at 427; see also Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 179 (7th Cir. 1991) ("The greater the precautions that [plaintiff] took to maintain the secrecy of the piece part drawings, the lower the probability that [defendant] obtained them properly and the higher the probability that it obtained them through a wrongful act . . . .")

56 See, e.g., Fisher Stoves, Inc. v. All Nighter Stove Works, Inc., 626 F.2d 193, 196 (1st Cir. 1980) (where plaintiff carelessly left customer data at customer’s store, competitor who accidentally discovered it should not be enjoined); Defiance Button Mach. Co. v. C & C Metal Prods. Corp., 759 F.2d 1053, 1056-57, 1063 (2d Cir. 1985) (finding that defendant’s use of consumer list could not be enjoined when plaintiff left the file in an old computer that was subsequently sold.).

57 See, e.g., Dicks v. Jensen, 768 A.2d 1279, 1284 (2001) ("It would be anomalous for the courts to prohibit the use of information that the rightful owner did not undertake to protect.")

58 Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 179 (7th Cir. 1991).

59 See Gemisys Corp. v. Phoenix Am., Inc., 186 F.R.D. 551, 558 (N.D. Cal. 1999) (granting summary judgment in favor of defendant licensee where plaintiff failed to use confidentiality legends on documents pursuant to the terms of its license agreement).
In practice, the question whether the reasonable efforts requirement has been met varies from case to case. The plaintiff must produce sufficient evidence to prove that the alleged trade secret was the subject of reasonable efforts to protect its secrecy. The language the courts use is not always consistent, but courts often look for use of the following kinds of security factors in assessing reasonableness: (1) confidentiality agreements; (2) exit interviews reminding departing employees of their confidentiality obligations; (3) security badges to enter the premises or secured areas; (4) security guards and closed circuit television cameras, and (5) computer passwords or access codes restricting access to certain personnel. Even where a trade secret owner implements security measures internally with employees, it must also be mindful of external protections and failure to do so could lead to a court denying trade secret protection.

Cases analyzing reasonable precautions where trade secrets were allegedly misappropriated, at least in part, by using electronic means appear to focus on the use of the kinds of traditional security measures discussed above such as non-disclosure agreements, steps to secure the facility, notice to employees about protecting trade secrets and use of passwords. In more recent cases, the courts seem to pay a little more attention to technical


61 Schalk v. Texas, 823 S.W.2d 633, 637-40 (Tex. Crim. App. 1991); Gillis Associated Indus. Inc. v. Cari-All, Inc., 564 N.E.2d 881, 886 (Ill. App. Ct. 1990) (finding that plaintiff failed to take such affirmative measures as using internal or external physical security, confidentiality agreements, confidentiality stamps, or entrance and exit interviews imparting the importance of confidentiality). See also Otis Elevator Co. v. Intelligent Sys., Inc., 17 U.S.P.Q.2d 1773, 1775 (Conn. 1990) (finding that plaintiff employed reasonable measures to protect its trade secrets when plaintiff limited access to premises such as personally escorting visitors while on site, video monitoring of doors and parking lots, requiring photo identification badges).

62 See, e.g., Flotec, Inc. v. S. Research, Inc., 16 F. Supp. 2d 992, 1004 (S.D. Ind. 1998) (noting that plaintiff used safeguards internally with its own employees but failed to do so with prospective supplier); Carbolene Co. v. Lebeck, 990 F. Supp. 762, 767-68 (E.D. Mo. 1997) (noting that plaintiff required employees to sign confidentiality agreements and limited their access to secret data on its computer system, but did not use adequate safeguards in circulating the information to customers.)

protection measures, going beyond the use of traditional measures; and steps not taken could be just as important as steps taken.\footnote{See, e.g., Diamond Power Int’l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1335 (N.D. Ga. 2007).} For instance, where an employee downloaded a file consisting of a 900-page electronic document the plaintiff argued that its efforts to protect the file were reasonable because it

(1) required its employees to sign confidentiality agreements that covered “this sort of information,” (2) it was available only to [plaintiff’s] employees on its to [sic] password- and firewall- protected main network, and (3) because [plaintiff] instituted physical measures to make sure no outsiders could access it.\footnote{Id.}

The court disagreed, however, noting that the plaintiff failed to show that it

(1) labeled the file confidential or otherwise communicated the confidentiality of the . . . file directly to its employees, (2) directed its employees to maintain the secrecy of the file (other than through a general confidentiality agreement which did not expressly mention the . . . file), or (3) tracked or otherwise regulated the use of [the file].\footnote{Id.}

Accordingly, the court held that the plaintiff’s efforts were not reasonable under the circumstances.

Unfortunately, the only thing consistent about the way in which the courts analyze reasonable efforts in these cases is the inconsistency in both the approach and outcomes. In one case the court found that the plaintiff had taken reasonable measures to protect a trade secret that was kept on a computer and protected by a password, because it had used licensing agreements, a password protected website, and generally kept the secrets out of the public display at conventions.\footnote{QSRSoft, Inc. v. Rest. Tech., Inc., 84 U.S.P.Q.2d 1297, 1303 (N.D. Ill. 2006).} In another case, a court found that the use of encrypted e-mail to transmit the alleged trade secret and password protection were insufficient to meet the requirement given the
lack of other security measures. 68 Still, other courts do not address the issue directly, disposing of the cases on other grounds. 69

III. THE DIGITAL WORLD

Computers are present in virtually every workplace. A reported 77 million people use a computer at work. 70 Employees most often use computers to access the Internet or to communicate by e-mail, 71 the very kinds of use that could quickly disseminate trade secrets. The employer’s workplace has also expanded into homes, as approximately 12 million employees work full time from home as telecommuters, a trend that has increased in recent years. 72 Management, professional, and sales employees are especially likely to be using technology in the workplace and also among those most likely to be telecommuting. 74


69 See, e.g., Twin Vision Corp. v. Bellsouth Commc’n Sys., No. 97-55231, 1998 U.S. App. LEXIS 13607, at *8 (“We need not decide whether encryption alone is adequate evidence that [plaintiff] made a reasonable effort to preserve the secrecy of its factory access code because we find that it has not met its burden in regard to misappropriation.”)


71 Id.

72 “More than 12 million Americans are full time telecommuters, and another 33 million do at least part of their job at home according to the nonporifit WorldatWork.” Alison Grant, Taking a Big Risk: Surge in Telecommuters Creates New Twists, Novel Legal Questions and Employer Problems, PLAIN DEALER, Feb. 4, 2007, at G1.

73 Sue Shellenbarger, Some Companies Rethink the Telecommuting Trend, WALL ST. J., Feb. 28, 2008, at D1 (noting that from 2005 to 2007 there was a thirty percent increase in the number of full time employees working from home).

The digital world increases the likelihood of destroying trade secret status, because information in digital form can be stored and processed in so many ways, that it becomes very difficult to track and control. Unlike the traditional options of file cabinets or boxes, laptops, PDAs, cell phones, USB flash drives, portable hard drives, iPods and MP3 players are among the many possible locations where one might download and store electronic information. As even Congress has observed, “[c]omputer technology enables rapid and surreptitious duplication of information. Hundreds of pages of information can be loaded onto a small computer diskette, placed into a coat pocket, and taken from the legal owner.”

There is a tension between the need to keep information secret and modern technological methods that allow the information to be easily accessed, reproduced, and disseminated. Information breaches occur most commonly through such activities as “unauthorized access to information, loss of laptop and mobile devices, theft of proprietary information, and insider e-mail abuses” and more than half of these breaches occur as a result of corporate mismanagement of the information or from insiders who abuse their access. A recent report of data breaches that occurred to date in 2008 revealed that most were the result of lost or stolen laptops, hard drives or thumb drives, and the posting of sensitive data on web sites or distribution through e-mail.

While this Article focuses on trade secret misappropriation, there may be other causes of action available where a computer has been used inappropriately to transmit or intercept information. For instance, the Computer Fraud and Abuse Act ("CFAA") prohibits accessing a computer without authorization to obtain information. It may therefore be

---


76 See Robert P. Green & Glenn Dickinson, supra note 75, at 19.


78 Robert P. Green & Glenn Dickinson, supra note 75, at 19.

79 Brian Krebs, Data Breaches Hit 8.3 Million Records in First Quarter, THE WASH. POST, Apr. 3, 2008, at D03.

80 18 U.S.C. § 1030 (2006). The phrase “without authorization” is not defined in the Act and it is questionable whether it would cover an employee who at the time of accessing the information was permitted to access the computers, even if the later use of the information were unauthorized. See Diamond Power Int’l, Inc. v. Davidson, 540 F. Supp. 2d 1322, at 1342-44 (N.D. Ga. 2007) (recognizing a split among the courts on the interpretation of “without authorization” but holding that “a violation does not depend upon
applicable where employees use the employer’s computer to send “unauthorized” e-mail with confidential information to others, including, prospective new employers. The CFAA provides both criminal and civil remedies, including a private right of action against a person who intentionally causes damage to a protected computer. In addition, use of e-mail to encourage an employee to reveal trade secrets can be prosecuted as wire fraud, in so far as it comprises a scheme to defraud the employer. The Electronic Communications Privacy Act (“ECPA”) may also apply where one intercepts, or endeavors to intercept, any electronic communication.

The rest of this Part discusses the ways in which trade secrets have become more vulnerable because of the use of technological tools in the workplace. It examines some of the tools that augment the ease with which they can be stored, accessed, and disseminated. The challenge of protecting trade secret information is also placed in the larger context of data security and the lessons that might be learned from that parallel struggle.

A. Easier Storage and Accessibility

Where it might have required several drawers of file cabinets filled with paper to store sensitive business information, today that information can be stored in a single spreadsheet or document, or stored on a computer’s hard drive. It can then be downloaded onto a USB thumb drive, which is


82 18 U.S.C. § 1030 (g). 

83 18 U.S. C. § 1030 (a)(5)(A). A “protected computer” is a computer “which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.” 18 U.S. C. § 1030(e)(2)(B). 


86 This abbreviation is short for Universal Serial Bus drive. Universal Serial Bus drive is a type of serial bus that allows peripheral devices such as disks, modems, printers, digitizers, data gloves to be easily connected to a computer. BRITANNICA CONCISE ENCYCLOPEDIA 2008 (Encyclopædia Britannica Online June 15, 2008), available at http://search.eb.com/ebc/article-9381643 (last visited June 19, 2008).
literally about the size of one’s thumb, and connected to another computer anywhere to read the information. This means that for someone intending to steal the information, instead of having to photo copy hundreds of pages of documents, and load them into boxes or folders to leave the building, it is a simple matter to either download the information, within seconds, onto a thumb size storage device which fits easily into a pocket, or attach the information to an e-mail sent to an outside account where it can later be easily retrieved.

The risk of misappropriation involving these new storage devices is already evident in trade secret misappropriation cases. For example, in one case an employee misappropriated his employer’s trade secrets by downloading the equivalent of 1.5 million pages of raw text onto two USB drives. The employee attached a thumb drive to his desktop computer several times before his departure to copy files which he then transferred to the desktop computer at his new employer and also onto the new employer’s servers.

In another, a departing employee transferred, among other things, a sensitive five-hundred-page document to his home computer while working for the plaintiff, but after he had already accepted employment from the plaintiff’s principal competitor. He did it by downloading the files from his employer’s computer system to a zip drive and then later transferred the information from the zip drive to his home computer. In yet another case an employee provided confidential customer lists on a USB drive to a competitor. Thus, the very ease with which large amounts of information can now be stored rapidly, transported quickly and later accessed in the original format provides greater incentive and opportunity for it to be removed.

The use of servers to consolidate, store and publish information can also pose risks to trade secrets. Information which previously might have been locked away in dusty file cabinets scattered across many offices or even the globe can now be accessed immediately by every employee in the


88 Id. at *18.


90 Id. at 1330.

Employees can then download a wide range of information onto personal laptops or miniaturized storage devices. Wireless networks are popular because of the lower cost and greater convenience that they offer relative to wired connections. Unfortunately, they are much more vulnerable to intrusion than hard-wired networks and pose high security risks if left unprotected.

Finally, laptop computers epitomize information portability. They enable employees to take valuable data to any location. When an employee connects her corporate laptop to wireless networks such as public Wi-Fi connections or “hot spots,” information stored on the laptop is susceptible to hackers. In addition, the theft of a laptop can expose a company’s most sensitive information, posing challenges to data security and trade secret protection. For instance, the personal data of about 26 million veterans and military troops was recently exposed when a burglar stole a laptop from the home of an employee of the Department of Veterans Affairs. If this kind of theft led to a large scale exposure of trade secrets, it could be devastating to a company, as the trade secret protection in all of the now public data would be lost.

Companies should therefore pay closer attention to laptop security and to policies governing employees’ use of laptops. Boeing Co., for instance, “requires employees to access most sensitive information through company servers instead of downloading the data to a laptop . . . [and] employees working with payroll data must use a cable lock to physically

---

92 See, e.g., Four Seasons Hotels and Resorts v. Consorcio Barr, 267 F.Supp. 2d 1268, 1283 (S. D. Fl. 2003) (“The Lotus Notes server was connected to all of the servers for all Four Seasons’ worldwide to allow e-mail communication. Aside from that, it also provided access to Four Seasons’ corporate databases which provided other information.”)


95 Id.


97 Pamela Yip, Firms Ready to Put Leash on Laptops: Companies Expect Employees to ‘Guard Them Like a Wallet’ to Prevent Theft and Protect Sensitive Data, THE DALLAS MORNING NEWS, July 16, 2006, at 1D.
secure their laptops to a desk at all times . . . .”

ING America requires the installation of encryption software on all laptops before they can leave the premises. For both of these companies, their policies are in reaction to having suffered recent laptop thefts; with trade secrets there are no second chances at protection once the secrets have been exposed.

B. Easier Dissemination

Trade secret law only protects secret information. With the click of a mouse or the push of a button e-mail, the Internet, and even cell phones can expose trade secrets to potentially millions of people within seconds. Once the trade secret becomes public, the trade secret owner may be rendered powerless to stop third parties, including competitors, from using it, and the trade secret owner also faces the complete loss of trade secret status. Accordingly, the grave risks posed by these technologies cannot be left unaddressed.

1. E-Mail

One need not even attach a physical device to a work computer to transfer information. E-mail can accomplish most transfers of files and other data with little effort, and of course, even without attachments,

---

98 Id.

99 Id.

100 The Boeing thefts, which occurred in November 2005 and April 2006, exposed thousands of current and former employees’ social security numbers and addresses. The ING laptop stolen in June 2006 contained retirement plan information on 13,000 employees. Id.

101 As of the writing of this article I am not aware of any trade secret losses as a result of stolen laptops. However, this may be explained by the fact that such instances would not be reported. Companies have no incentives to report this kind of trade secret theft since it could cause embarrassment to the company and might lead to other kinds of losses as well, such as for instance, a drop in stock prices. Unlike the privacy laws and state breach notification laws that require disclosures when companies suffer data security breaches, see, e.g., CAL. CIV. CODE § 1798.29 (2008), N.Y. GEN. BUS. LAW § 899-aa (2008), DEL. CODE ANN. tit. 6, § 12B-102 (2008), ARK. CODE ANN. § 4-110-105 (2008), no such mandatory disclosures are currently in place for trade secret losses.

102 See Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984) (“Information that is public knowledge or that is generally known in an industry cannot be a trade secret.”); Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475 (1974) (“The subject of a trade secret must be secret, and must not be of public knowledge or of a general knowledge in the trade or business.”).
information can also be exchanged in the text of the message. Many trade secret cases involve employees transmitting files containing trade secret information through e-mails. In a case prosecuted under the Economic Espionage Act, a product development manager gained access to secret product information belonging to a customer of his former employer. As he later accepted new employment from a competitor of that customer, he downloaded the secret information and e-mailed them to his new employer. In another case, an engineer who had knowledge of secret software source codes was terminated from work. In resentment, he sent e-mail messages to several competitors of his former employer, offering the secret software source codes for sale. All messages were sent from an alias e-mail account at a public library so that it would be difficult to uncover the true identity of the sender. To his surprise, the competitor brought those messages to the attention of his former employer. His identity was eventually revealed when the FBI’s Computer Hacking and Intellectual Property Squad detected accesses to the alias e-mail account through his home internet connection.

Trade secret information can also be transmitted by employees from their corporate email account to their private e-mail accounts and to competitors. In a case that made headlines recently, seven former Citibank employees were accused of emailing secret client data from work to their personal e-mail addresses before leaving to join a competitor. As

105 Id.
107 Id.
108 Id.
109 Id.
110 Id.
a result of these bankers’ use of Citibank’s trade secret information to lure away clients, Citibank is alleged to have lost about $50 million of business.\textsuperscript{113}

In another example, a researcher who was responsible for developing and manufacturing veterinary diagnostic kits for IDEXX became dissatisfied with her job and began to consider leaving the company.\textsuperscript{114} As part of her plan to find new employment, she exchanged e-mails with a competitor who tried to lure her with promises of potential employment opportunities.\textsuperscript{115} During her e-mail exchanges with the competitor she disclosed proprietary company information, and transmitted software and computer files containing a variety of IDEXX trade secrets.\textsuperscript{116} Ironically, her activities were only discovered after she accidentally sent her supervisor one of the e-mails -- addressed to the competitor -- that contained the company’s trade secret files.\textsuperscript{117} Her employer’s discovery was especially fortuitous because she had resigned from the company the day before she inadvertently sent the e-mail to her supervisor.\textsuperscript{118} Absent her mistake, it is very unlikely that she would have been caught.

Instant messaging is on the rise in the workplace, providing what e-mail does not: real-time conversations and an indication of which contacts are available at a given time.\textsuperscript{119} Messaging poses the same kinds of security risks as e-mail, and it is estimated that about one-third of employees in the U.S. use instant messaging, often without the knowledge of their employers.\textsuperscript{120}

\begin{itemize}
\item \textsuperscript{113} Id.\textsuperscript{113}
\item \textsuperscript{114} U.S. v. Martin, 228 F.3d 1, 6 (1st. Cir. 2000).\textsuperscript{114}
\item \textsuperscript{115} Id. at 7.\textsuperscript{115}
\item \textsuperscript{116} U.S. v. Martin, 228 F.3d 1, 8 (1st. Cir. 2000).\textsuperscript{116}
\item \textsuperscript{117} Id. at 10.\textsuperscript{117}
\item \textsuperscript{118} Id.\textsuperscript{118}
\item \textsuperscript{119} See Carola Mamberto, \textit{Instant Messaging Invades the Office}, \textsc{The Wall St. J.}, July 24, 2007, at B1.\textsuperscript{119}
\item \textsuperscript{120} Id.\textsuperscript{120}
\end{itemize}
2. The Internet

Approximately 1.4 billion people use the Internet, and it is undoubtedly a powerful communication tool.\footnote{See Global Internet Freedom, CONG. TESTIMONY, May 20, 2008, available at 2008 WLNR 9511892.} It has changed the way in which the world does business, and many companies today rely on computers and the Internet to survive and exist.\footnote{See generally Andrea M. Matwyshyn, Symposium, Personal Jurisdiction in the Internet Age of Nodes and Power Laws: A Network Theory Approach to Internet Jurisdiction through Data Privacy, 98 NW. U. L. REV. 493, 499 (2004) (discussing trends in the Internet economy).} Many employees access the Internet not only from their workplaces, but from home as well, as over fifty percent of all households are connected to the Internet.\footnote{See Daniel W. Park, Trade Secrets, the First Amendment, and Patent Law: A Collision on the Information Superhighway, 10 STAN. J. L. BUS. & FIN. 46, 47 (2004).}

The Internet is a dangerous place for trade secrets. Many courts assume that a trade secret posted on the Internet has become generally known and consequently lost its trade secret status.\footnote{See Religious Tech. Ctr. v. Netcom On-Line Commc’n Servs., Inc., No. C-95-20091 RMW, 1997 U.S. Dist. LEXIS 23572, at *40-41 (N.D. Cal. Jan. 3, 1997); Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1368 (E.D. Va. 1995); DVD Copy Control Ass’n v. Bunner, 10 Cal. Rptr. 3d 185, 192-93 (Ct. App. 2004). But see DVD Copy Control Ass’n, 10 Cal. Rptr. 3d at 190 (finding that the mere posting of information on the Internet does not destroy a trade secret).} Even when a party posting\footnote{Posting “consists of directly placing material on or in a Web site, bulletin board, discussion group, newsgroup, or similar Internet site or ‘forum,’ where it will appear automatically and more or less immediately to be seen by anyone with access to that forum.” O’Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 91 (Ct. App. 2006). It therefore allows direct self-publication of information, or one may also send information to a site, the owners or moderators of which make decisions about what to post. See id. at 91.} trade secret information may not have intended to cause harm to the trade secret owner, the nature of the Internet is such that the secret nonetheless could be destroyed.\footnote{See, e.g., Jerome Stevens Pharm., Inc. v. Food & Drug Admin., 402 F.3d 1249, 1250, 1254 (D.C. Cir 2005) (reversing district court dismissal, holding that FDA could be liable for misappropriation of trade secrets where it posted plaintiff’s trade secrets on its website for five months, and remanding).} Unlike other mass media, the Internet has no editors who scrutinize submissions and decide what materials will be
published. Any person sitting at a computer can post information onto the Internet, resulting in immediate and irreparable harm. One judge captured the problem in these words:

The court is troubled by the notion that any Internet user . . . can destroy valuable intellectual property rights by posting them over the Internet, especially given the fact that there is little opportunity to screen postings before they are made. Nonetheless, one of the Internet’s virtues that it gives even the poorest individuals the power to publish to millions of readers can also be a detriment to the value of intellectual property rights. The anonymous (or judgment proof) defendant can permanently destroy valuable trade secrets, leaving no one to hold liable for the misappropriation.  

The nature of the Internet is such as the trade secret owner may never know the identity of the person making the disclosure, and the person posting the information may very well be far removed from the person who originally misappropriated the secret.

Because the value of a trade secret lies in its secrecy, most misappropriators who have acquired another’s trade secrets and plan to use them for their own competitive advantage, have no incentive to publicize the secret. The culture of the Internet, however, has led to a higher likelihood that those in possession of other’s trade secrets will make them public, rather than continuing to keep them secret for personal gain. The great ease with which virtually anyone can post information on the Internet coupled with its “disinhibiting effect” and a general decline in employee loyalty in the workplace, have allowed disgruntled employees to achieve the ultimate revenge against their former employers by destroying trade secrets.

---


128 See, e.g., DVD Copy Control Ass’n v. Bunner, 10 Cal. Rptr. 3d 185, 195 (Ct. App. 2004) (noting that a defendant in a trade secret case typically “has as much interest as the plaintiff has in keeping the secret away from good faith competitors and out of the public domain.”)


One court articulated this phenomenon in the following words: “With the Internet, significant leverage is gained by the gadfly, who has no editor looking over his shoulder and no professional ethics to constrain him. Technology blurs the traditional identities of David and Goliath.” Accordingly, Internet disclosures are likely to become a greater problem than they have been in the past, and the few cases highlighted below illustrate that a trade secret owner generally has no satisfactory recourse when trade secrets have been published on the Internet.

In Religious Technology Center v. Lerma, a disgruntled former member of the Church of Scientology, published documents taken from a court record on the Internet. The Church considered these documents to be trade secrets and sued the former employee, Lerma, to enjoin him from disseminating the alleged trade secrets. The court refused to issue the injunction, though, because by the time the Church sought the injunction, the documents no longer qualified as trade secrets. The court explicitly stated that “[o]nce a trade secret is posted on the Internet, it is effectively part of the public domain, impossible to retrieve.”

In another Scientology case, the Church sought an injunction against another disgruntled former member who posted Church writings on several USENET groups. Despite being “troubled by the notion that any Internet user . . . can destroy valuable intellectual property rights by posting them

---


134 Id. at 1364.


137 Id.

138 Id.

over the Internet,” the court held that since the writings were posted on the Internet, they were generally available to the relevant public and there were no trade secret rights available to support an injunction.140

In *Ford Motor Co. v. Lane*,141 the defendant operated a website that contained news about Ford and its products.142 Lane published some documents on his website relating to the quality of Ford’s products.143 He did so despite knowing that the documents were confidential.144 Ford sought a restraining order to prevent publication of the documents, claiming that the documents were trade secrets.145 Ultimately, however, Lane’s First Amendment defense prevailed, with the court reasoning that an injunction to prevent Lane from publishing trade secrets would be an unconstitutional prior restraint on speech.146

The advent of blogging also poses risks, as employees and others discuss a myriad of company related issues in public online, not all of which may be suitable for disclosure. Even though some employees have been fired for blogging about work, business blogs are on the rise.147 A new blog is created every second,148 and an estimated eighty-nine percent of corporations are either blogging now or intend to set up blogs.149 Some blogs may even focus on breaking stories about their competitors, as for instance, when a blog sponsored by Miller Brewing Co. revealed that

---

140 Id. at 1256-57.
142 Id. at 747.
143 Id.
144 Id. at 748.
145 Id.
competitor Anheuser-Busch was preparing a new kind of brew.\textsuperscript{150} This blogging culture, generally unrestricted by editors and gatekeepers, sets the stage for easy dissemination of trade secret information, even if inadvertent. In one case, Apple Inc. sued and settled with a website for publishing trade secrets and allegedly soliciting Apple employees to reveal secrets about a new miniature Apple computer.\textsuperscript{151}

3. Cellular Phones

Another potential source for dissemination of trade secrets is cell phones. About eighty-four percent of those living in the United States today use a cell phone,\textsuperscript{152} an increase of about sixty-four percent from just five years ago.\textsuperscript{153} Today’s phones combine camera, e-mail, and Internet capability in one small device, and have become ubiquitous.\textsuperscript{154} As a result, they can serve as a great tool for stealing and transmitting company secrets. These increased risks have led security conscious organizations, and even countries, to ban or limit the use of cell phones. Saudi Arabia and North Korea have apparently banned camera phones in an effort to protect government secrets.\textsuperscript{155} The United States Air Force has also banned camera phones from all areas that contain classified information.\textsuperscript{156} Companies like General Motors and Texas Instruments have instituted policies limiting the


\textsuperscript{151} See Hiawatha Bray, \textit{Website to be Closed as Part of Deal with Apple}, \textit{Boston Globe}, Dec. 21, 2007, at 4E.

\textsuperscript{152} This is according to 2007 figures compiled by the International Association for the Wireless Telecommunications Industry. See http://ctia.org/advocacy/research/index.cfm/AID/10323 (last visited June 1, 2008).


\textsuperscript{156} Id.
use of camera phones by visitors and employees on company premises. Samsung Electronics, DaimlerChrysler and BMW also prohibit camera phones at some manufacturing sites. In addition to the risks that cell phones may be used to capture trade secrets, smart phones (which have many of the same functions as a desktop computer) are also at risk of being infected with viruses and other malicious software.

C. Data Security Parallels

The challenge of protecting trade secrets should be reviewed as part of the larger issue of data security generally, where preventing the loss of sensitive data is of critical importance. “The basic tasks of identifying sensitive data, monitoring where it goes, auditing who has access to it, and restricting that access” are common to both data loss prevention and the protection of trade secrets. Accordingly, lessons from that field can be instructive, and a recent report on data security may provide some insights that could be helpful to trade secret protection.

CIO Magazine, CSO Magazine, and PricewaterhouseCoopers, recently conducted a worldwide survey titled The Global State of Information Security. The report produced from the survey revealed several interesting points that are relevant to the discussion about the larger issues surrounding trade secret protection and technology. First, a majority of the companies surveyed conducted enterprise risk assessments of their security strategy. This suggests that all companies ought to include trade secrets as part of their security risk assessments. Trade secrets are a subset of the sensitive commercial data that must be protected, in addition to the private consumer information, and thus should not be left out of risk assessments.

157 Id.

158 See McAleavy, supra note 154, at E01.


160 Jordan Wiens, Take a Stand against Data Loss, INFORMATIONWEEK, Nov. 19, 2007, at S1.


162 Id. at 3.
Second, the use of technological tools such as firewalls, user monitoring, and encryption are now more widely used to protect data. Having these tools already in place and available in the workplace means that they could be implemented in a program to secure trade secrets without too much difficulty. However, reliance on the tools alone is not optimal, as technological tools tend to be reactive, and are not capable of the intelligence and risk assessments that could avoid inappropriate access to trade secrets in the first instance.

Third, the report notes an interesting trend in how companies have come to view information security over the last few years: there has been a shift from ignorance of serious flaws in computer security to awareness of those flaws, but the final stage of using the awareness to fix the flaws has not yet been achieved. To the extent that trends in trade secret protection may be similar to those in information security, knowledge about the importance of trade secret protection probably lags behind information security. As such, the level of knowledge for trade secrets might best be classified in the phase of “ignorance moving towards awareness.” Indeed, part of the impetus for this Article is the hope that it will increase awareness of the enhanced risks that technology poses to trade secrets, and that a more stringent application of the reasonable efforts standard by the courts will eventually, in conjunction with other measures, cause trade secret owners to fix the flaws that currently exist in their trade secret protection strategies.

Fourth, the results from the survey confirmed that the most likely culprit in a “security incident,” by an almost two to one margin, is not a hacker, but an employee. This finding provides strong support for this Article’s premise that reasonable efforts to protect trade secrets requires a comprehensive approach that takes into consideration a trade secret owner’s measures to protect its secrets against outside threats as well as the often overlooked inside threats from employees. It also bolsters the contention that use of the traditional security measures that are generally facilities-based approaches are insufficient. It makes little sense to build taller fences when the most likely thieves are already inside.

---

163 Id. The large increase in the use of encryption was noteworthy, with seventy-two percent reporting using some form of encryption compared to forty-eight percent the previous year.

164 See id. at 5.

165 Id. at 4.

IV. SHOULD REASONABLENESS BE REDEFINED IN LIGHT OF KNOWN TECHNOLOGICAL RISKS?

As the earlier discussions in this Article illustrate, the widespread use of technology in the workplace enhances the risks of trade misappropriation through electronic means. These risks are foreseeable to a trade secret owner, and it seems intuitive that a court in determining reasonableness would deem it relevant to consider what specific security precautions were utilized to protect a secret in light of those risks. The Restatement of Unfair Competition also provides that the “foreseeability of the conduct through which the secret was acquired” should be relevant to determining reasonableness.¹⁶⁷

To be clear, this Article does not advocate changing the reasonable efforts requirement. Rather, because the requirement requires consideration of what is reasonable under the circumstances, the argument is that the changing circumstances that have come about as a result of new technology requires a reexamination of what security measures are reasonable. Further, because trade secret law and the definition of trade secret itself (even more than the other areas of intellectual property) is based on “evolving concepts and ideas”¹⁶⁸ a reexamination of what are reasonable measures to protect information based on current business norms is not only logical but is consistent with trade secret law.

This Article proposes modified guidelines for the reasonable efforts determination. Courts should pay greater attention to the technical measures and processes that companies use to protect their trade secrets, rather than merely focusing on the traditional facilities-based measures. In light of the foreseeability of the greater dangers posed by technology, reasonableness requires evidence of a risk analysis and steps to address those risks. Trade secret owners must avoid after the fact justifications and explanations, and instead show affirmative measures generated from conscious recognition and assessment of the need to protect putative trade secrets. Companies, in adopting new technological tools in the workplace, assume the risks associated with them. As such, where they have not taken adequate steps to protect their alleged trade secret information in light of those risks, they may be denied trade secret protection.¹⁶⁹ In the end, the

¹⁶⁷ Id.


¹⁶⁹ See RTE Corp. v. Coatings, Inc., 267 N.W. 2d 226, 233 (Wis. 1978) (“Where the owner of the secret disregards caution and fails to take steps to safeguard against disclosure, the courts will, at times, deny him any relief whatever, principally on the theory
reasonableness of the trade secret owner’s efforts serve to further the policies underlying trade secret law, ensuring that protection is granted only to information that meets the secrecy requirement.

Whether a trade secret owner has utilized appropriate safeguards sufficient to meet the reasonable efforts requirement is a question of fact, based on the particular circumstances. These decisions necessitate a balancing between using sufficient precautions to protect the secret on the one hand, while not imposing too many precautions that would impair the functioning of its business. The inquiry will necessarily call for a cost-benefit analysis which will vary in each case based on the costs of the protective measures relative to the attendant benefits of protecting the information. The costs to the trade secret owner will not only include direct financial costs, but indirect costs such as the ability to make appropriate use of the information in the business by sharing it with employees and others who need to use it.

Further, companies ought to view security measures with a certain level of fluidity such that measures that may be reasonable at one point in time based on the circumstances may no longer be reasonable when those circumstances change. As the foreseeable threats to the trade secrets increase, so should the security measures. Accordingly, the known risks posed by technology today (which may not have existed years before) should lead to a reexamination of reasonable efforts not only in practical terms for companies, but for courts as well.

that he courted his own disaster.”) (quoting CALLMAN ON UNFAIR COMPETITION, TRADEMARKS AND MONOPOLIES § 55.1, at 451-53 (3d ed. 1968)).

170 See Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 178 (7th Cir. 1991).

171 See id. at 178-180.

172 See Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 179 (7th Cir. 1991).

173 Id. at 180.


175 Id. at 23.

176 This is not an entirely foreign concept to intellectual property law, where intellectual property owners have had to make adjustments to the way in which they protect their intellectual property rights in light of modern circumstances. For instance, trademark owners who fail to police their marks may be deemed to have abandoned the marks, or those marks are more likely become generic or otherwise lose their distinctiveness. See 3
1. Introducing Greater Objectivity into the Analysis

This Article recommends that courts introduce a more transparent, objective layer into the reasonable efforts analysis. As it currently stands, a trade secret owner impliedly makes a subjective judgment as to the reasonableness of its safety precautions in deciding which safety measures to implement, and which to reject. This determination probably entails, among other things, a cost-benefit analysis, where the owner weighs the costs of protection relative to the value of the secret.\(^{177}\)

However, it is the court who ultimately decides whether those steps were reasonable enough under the circumstances, injecting an objective standard that trumps the trade secret owner’s subjective belief about the sufficiency of its security measures. Ultimately, the fact finder must determine whether additional measures were necessary to protect the putative trade secrets in light of the particular circumstances. On the surface, this bears some resemblance to the “reasonable expectation of privacy” analysis in criminal procedure,\(^{178}\) where the reasonableness of the defendant’s expectation of privacy must be one “that society is prepared to recognize as ‘reasonable.’”\(^{179}\)

\(^{177}\) See Posner, supra note 47, at 473.

\(^{178}\) While there may be parallels between the Fourth Amendment’s reasonable expectation of privacy standard and trade secrecy’s reasonable efforts requirement, ultimately I do not think it appropriate to adopt these Fourth Amendment principles in wholesale fashion into the reasonable efforts analysis. See Posner, supra note 47, at 465-72 (explaining the shortcomings in applying the Fourth Amendment analogy to trade secret law).

\(^{179}\) Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). It is worth noting that in direct parallel to the reasonable efforts requirement discussed in this Article, failure to take steps to protect one’s privacy in the Fourth Amendment context may mean that one does not receive Fourth Amendment protection. See generally Christopher Slobogin, Technologically-Assisted Physical Surveillance: The American Bar Association’s Tentative Draft Standards, 10 HARV. J. L. & TECH. 383, 392 (1997).
Thus, in determining reasonableness the court ought to consider not only the cost-benefit analysis that the plaintiff trade secret owner might have considered, but also the nature of the risks involved, with special consideration to the known technological risks that may or may not have been considered by the trade secret owner. Factors that could aid in that determination include: (a) the nature of the industry, (b) the nature of the trade secrets and how they were stored, (c) the nature of the measures taken to protect the secrets, and (d) the known risks from storage and protection choices. While some of these are interrelated, the benefit of having each considered separately is that it allows a more comprehensive and consistent analysis of the reasonable efforts requirement in each case.

a. Nature of the business and the industry

The nature of the plaintiff’s business including its size (both in terms of personnel and financial strength), the type of services or products offered by the business, the manner in which the business operates, as well as the related question of the nature of the trade secrets are all relevant considerations. In highly competitive industries, or industries that rely heavily on technology to not only generate but store trade secret information, greater efforts ought to be required to meet the reasonableness requirement. This is because the “circumstances” would suggest that these trade secrets are particularly vulnerable. It is noteworthy, for instance, that a majority of the cases that have been prosecuted under the Economic Espionage Act for trade secret theft have involved high technology companies as the victims. Moreover, among the data at highest risk of theft are research and development data, customer lists, financial data, and strategic plans and roadmaps.


b. Nature of the trade secrets and how they were stored

Trade secrets vary tremendously and can be virtually any kind of business information. Accordingly, there can be no one size fits all approach. Rather, storage and protection measures must be carefully tailored to fit the particular situation. Thus, it may make a difference whether the purported trade secret consists of technical specifications and source code or formula. As this Article has made clear, trade secrets that are stored on a computer must be given special protection, and attention must be paid to the accessibility and portability of that kind of information.\(^\text{183}\)

In today’s business environment, it is likely that at least some if not all trade secrets will be stored electronically. As such, the traditional facilities-based measures may be insufficient. Sometimes, however, the very persons trusted with keeping information secure, can betray the trade secret owner. For instance, in *Four Seasons Hotels and Resorts v. Consorcio Barr*, a member of the Information Technology Department, with responsibility for network security, and with total access to the system information and files was inappropriately printing and diverting information for the benefit of the defendant company.\(^\text{184}\) In a case such as this, there was practically no way to avoid the misappropriation, unless perhaps there were checks in place to protect against rogue information technology staffers. While this may certainly be advisable, a court may not, in the context of other precautions taken by the company, consider the failure to protect against internal network security personnel unreasonable.

c. Nature of the measures taken to store and protect the secrets

While the reasonableness of security precautions requires a contextual analysis based on the particular circumstances of the trade secret owner’s business, this section will briefly highlight some of the kinds of measures (beyond confidentiality agreements and passwords) that have been utilized to address the disclosure risks from computer technology.\(^\text{185}\)

\(^{183}\) See Maxine S. Lans, *Can You Keep the Lid on your Trade Secrets?*, MARKETING NEWS, Aug. 29, 1994, at 9 (discussing practical suggestions to protect trade secrets, including computer related trade secrets).

\(^{184}\) *Four Seasons Hotels & Resorts v. Consorcio Barr*, 267 F. Supp. 2d 1268, 1283, 1290 (S.D. Fla.).

\(^{185}\) For an example of traditional (i.e. non-technological) preventive measures, see Randy Kay, *Guide to Trade Secret Protection – Maintaining Secrecy*, SAN DIEGO BUS. J., June 5, 2000, at 31.
Effective protection of trade secret information in this digital era requires both legal and technical approaches. The goal is not necessarily perfect security, since the fact that the information must be kept safe while in use, presents special challenges. Thus, “perfect security is not optimum security.” Rather, the trade secret owner needs to have an infrastructure in place to protect its secrets; one that includes specific processes and technological measures, in addition to the traditional facilities-based security precautions.

Agreements that go beyond a general confidentiality agreement and provide employees with specific notice or instructions can be helpful. At a minimum, companies should give careful deliberation to policies regarding remote access to company computer networks and systems, telecommuting, e-mail and Internet usage, and access rights to sensitive information. Some companies may even choose to ban camera-phones or other recording devices, where such devices could easily expose certain secrets.

Among the available options, a trade secret owner must select those measures that are the best fit given the preceding factors; i.e. nature of its business, the industry, and the particular secrets at issue. In one case, a company required employees to sign a “Computer Security and Non-Disclosure Agreement,” agreeing to maintain usernames and passwords in confidence. Other companies provide each employee with an ID that has to be validated with a password, and that ID is tied to a specific level of access depending on the employee’s role in the company. Still others add

---

186 See generally Antony J. McShane & Sarah E. Smith, Implement an Effective Trade Secret Protection Plan – Before It’s Too Late, INTELL. PROP. TODAY, July 2003, at 16 (outlining strategies for developing a trade secret protection program); Victoria A. Cundiff, Digital Defense: Protecting Trade Secrets Against New Threats (manuscript at 3-14, on file with author) (discussing practical steps to protect trade secrets in a digital environment).

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

188 See Antony J. McShane & Sarah E. Smith, Implement an Effective Trade Secret Protection Plan – Before It’s Too Late, INTELL. PROP. TODAY, July 2003, at 16.

189 See, e.g., Dan Gillmor, Picture This, Institutions Are Losing the Ability to Control the Creation and Distribution of Images – and Camera-phones are Just the Beginning, CIO INSIGHT.COM, Apr. 6, 2006, available at 2006 WLNR 14748715 (discussing Samsung Electronics ban on camera-phones inside its facilities).

190 Diamond Power Int’l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1327 (N.D. Ga. 2007). The policy, however, did not restrict employees from transferring information to their personal computers, and a departing employee did just that. Id. at 1329.

191 See, e.g., Four Seasons Hotels & Resorts v. Consorcio Barr, 267 F. Supp. 2d 1268,
proprietary legends to their computer screens and mechanisms that lockout unauthorized users.\textsuperscript{192}

Allowing employees to use sensitive company information, particularly where the information is transferred electronically and among various people, without the information being encrypted represents weak protection.\textsuperscript{193} Employers should be especially mindful of employees taking unencrypted information off site such as on their laptops or to their offices at home.\textsuperscript{194} The use of laptops generally should be carefully considered since they present many risks for data loss, including the risk that the laptops themselves might be lost, stolen by a third party or even sold to competitors.\textsuperscript{195}

d. Known risks from protection choices

As with information security generally,\textsuperscript{196} trade secret owners should conduct risk assessments to assure that an effective strategy or infrastructure is in place to protect allegedly valuable trade secrets. Conducting a risk analysis of potential threats to the company’s trade secrets should be comprehensive, paying attention to people, processes, and technology. Reliance on technological measures alone will not be sufficient. Such an approach has limitations in that it tends to be more reactive than proactive.\textsuperscript{197} For instance, the mere use of a password in itself


\textsuperscript{193}Jordan Wiens, \textit{Take a Stand against Data Loss}, INFORMATIONWEEK, Nov. 19, 2007, at S1.

\textsuperscript{194}Id.

\textsuperscript{195}See notes and discussion supra at notes 96 and 97; see also indictment in United States v. Sun available at United States Dep’t of Justice, Intellectual Property Cases: Chicago, Illinois Man Pleads Guilty to Theft of Trade Secrets, Offered to Sell Online Interpreter’s Information, http://www.usdoj.gov/criminal/cybercrime/sunPlea.htm (last visited July 14, 2008) (describing case where employee sold a laptop containing stolen trade secrets to a competitor for $3 million).

\textsuperscript{196}See discussion supra at Section III(C).

\textsuperscript{197}See Berinato, supra note 161, at 5 (noting that information security has been too skewed toward technology rather than proactive intelligence gathering and risk analysis).
may prove too risky. Many employees choose passwords that are too simple and that can be easily decrypted using free software.\textsuperscript{198} Recall, for instance, that the passwords were cracked in the \textit{Four Seasons} case, allowing access to sensitive data.\textsuperscript{199}

A decision to implement certain security measures, done in a rational manner, suggests that certain additional measures were considered and rejected. Often it might be that the costs of additional measures relative to their perceived benefits were prohibitive. Or that some measures would be too disruptive to the company’s productivity. The court should consider the degree to which additional measures might have decreased the risk of disclosure, in light of the known risks posed by the measures that were utilized.

2. Defendant’s Conduct as a Secondary Consideration

The defendant’s conduct in obtaining the trade secret information is not a proposed factor in the reasonable efforts determination mainly because under the \textit{UTSA} and the \textit{Restatement of Torts} the defendant’s conduct is relevant to the misappropriation issue, instead of the threshold issue of whether the information qualifies as a trade secret. While the defendant’s utilization of improper means could be relevant in assessing the strength of protective measures taken by the trade secret owner to protect the secret, it muddies the analysis to give it too much weight, and is perhaps best considered as a secondary factor. It is interesting that the \textit{Restatement of Unfair Competition}, which does include the reasonable efforts requirement as part of the misappropriation analysis, calls for an evaluation of “the extent to which the acquisition was facilitated by the trade secret owner’s failure to take reasonable precautions against discovery of the secret by the means in question.”\textsuperscript{200} It further suggests that the “foreseeability of the conduct through which the secret was acquired” should be relevant to determining reasonableness.\textsuperscript{201} Thus, under that framework, the foreseeability of the defendant’s conduct plays a role in the ultimate determination of whether actionable misappropriation occurred.

\textsuperscript{198} See Ben Worthen, \textit{Hacker Camps Train Network Defenders}, \textit{The Wall St. J.}, Apr. 1, 2008, at B6 (noting that “the best way to mitigate password risk is to put in additional authentication systems, such as biometric readers that scan fingerprints, or smartcards that workers have to swipe before they’re granted access to a system.”).

\textsuperscript{199} See supra text accompanying note 9.

\textsuperscript{200} Restatement (Third) of Unfair Competition § 43 cmt. c (1995).

\textsuperscript{201} \textit{Id}. 
Accordingly, assume a trade secret owner decides to protect sensitive data stored on a company network by requiring that high level employees sign general confidentiality agreements, and not requiring special passwords to access the data. If a low level employee, who did not sign the confidentiality agreement, accesses the trade secret on the computer and e-mails it to a competitor, a court could find such efforts not reasonable and that the data does not deserve trade secret protection. This would reflect the judgment that given the known risks to electronically stored data, the trade secret owner should have taken additional steps such as requiring passwords keyed to various levels of access, encrypting the data, and requiring that all employees sign confidentiality agreements.

3. Support from Tort law Concepts

Further support for holding trade secret owners to a higher duty of care when the risk from use of technology is foreseeable may be found in tort law concepts that consider the plaintiff’s conduct relative to the defendant’s in apportioning liability.\(^\text{202}\) Contributory negligence principles preclude a plaintiff from recovery if it contributed to the injury with its own negligence.\(^\text{203}\) Where, as here, the plaintiff is in a better position than the defendant to decide whether to risk being injured or at least the extent of that risk, based on the precautions it selects, then it seems sensible to allocate the burden of that choice to the plaintiff.\(^\text{204}\) This does not justify much of a leap because trade secret doctrine as it currently exists requires that trade secret owners take reasonable precautions to protect their trade secrets as a prerequisite for proving that a defendant (regardless of his conduct) misappropriated the trade secret.\(^\text{205}\) This is especially powerful where such reasonable efforts are necessary for determining whether a trade secret exists in the first instance, and because modern trade secret law derived, at least in part, from tort law principles. This argument, however, tying contributory negligence and assumption of risk to trade secret principles, appears to be novel and certainly could benefit from more

\(^{\text{202}}\) See RTE Corp. v. Coatings, Inc., 267 N.W.2d 226, 233 (Wis. 1978) (“Where the owner of the secret disregards caution and fails to take steps to safeguard against disclosure, the courts will, at times, deny him any relief whatever, principally on the theory that he courted his own disaster.”)

\(^{\text{203}}\) See Kenneth S. Abraham, The Forms and Functions of Tort Law 144-45 (3d ed. 2007).

\(^{\text{204}}\) See id. at 165 (discussing conscious reasonable risk-taking).

\(^{\text{205}}\) See supra text accompanying text note 38-40.
vigorous analysis. For the purposes of this Article, however, it is offered in the limited capacity of supporting a different take on the reasonable efforts analysis.

V. CONCLUSION

What might have been a “reasonable” precaution ten years ago to protect a trade secret is not necessarily reasonable today in light of the changed circumstances created by technology. These changes increase the risk of trade secret misappropriation, and trade secret owners must be mindful to have adequate security measures, both technical and process based, to deal with these enhanced risks. The approach presented in this Article addresses the problem from two angles. First, it aims to guide, in a more consistent fashion, the way in which courts analyze these cases where trade secrets that have been stored electronically are misappropriated. Second, it aims to encourage greater awareness and vigilance by trade secret owners before the misappropriation occurs. Trade secret protection cannot be an after thought. Rather, in order to be reasonable, it requires a more conscious, risk assessment approach that better anticipates and ultimately stems the inappropriate dissemination or disclosure of the secrets.