REASONABLE MEASURES TO PROTECT TRADE SECRETS IN A DIGITAL ENVIRONMENT

VICTORIA A. CUNDIFF*

ABSTRACT

The law of trade secrets is long-established: to obtain the court's assistance in enforcing trade secret rights, the trade secret owner must consistently take measures that are reasonable under the circumstances to protect its trade secrets. The increased digitization of trade secrets and the increased availability of digital tools to remove them have made the "circumstances" far more hostile to trade secrets and far less forgiving of errors than ever before. While the law does not require the trade secret owner to build an impenetrable fortress around the secret, the trade secret owner that does not take these new circumstances into account in designing a protection program has not taken reasonable measures. This article discusses practical contractual and litigation measures trade secret owners should consider in protecting their assets and examines the benefits and limitations of various statutory tools.

* Partner and Chair of the Global Trade Secrets Practice Group at Paul, Hastings, Janofsky & Walker LLP; Visiting Lecturer in Law, Yale Law School. Ms. Cundiff's practice focuses on intellectual property, trade secrets and departing-employee issues. She thanks Laura Keller Isenberg (also of Paul, Hastings, Janofsky & Walker LLP) and Robert Walker (a graduate of the University of Detroit Mercy School of Law and the University of Windsor Faculty of Law in the J.D./LL.B. program) for their contributions to this paper.

INTRODUCTION

If a thief wanted to remove a company's laboratory notebooks, research files, test results, manufacturing processes, long- and short-term strategic plans, marketing plans, customer proposals, contract files, credit reports, financial analyses, personnel lists and compensation files, he could back up a tractor-trailer truck to the office in the dead of night and load up several boxes. In this scenario, the thief would have to finish the job undetected by company guards, surveillance cameras and certainly before employees returned to the office the next morning.

There are new ways, however, to perform the same task. They are far more efficient. Today's thief could simply walk out with the information on his digital music player. If he wanted to travel light, he could simply e-mail the information to its intended destination.

Indeed, if he wanted to share confidential company information with the world, he could post it on the Internet, a fate suffered by Microsoft Corporation, Apple Computer, Ford Motor Company and scores of other companies in the motion picture, high technology and other industries.[1] To profit from the theft, he could use the Internet to sell or auction off the information. In addition, if he had functioned as his employer's information technology ("IT") administrator, he might even be able to hijack the company's domain name on renewal by directing the annual renewal notices to be sent to him, rather than his former employer.

The digital world is no friend to trade secrets.

On the other hand, digital media can also capture digital trails (or, as some have dubbed them, "mouse droppings").[2] Forensic analysis can in many cases reveal whether and when information has been accessed, copied, transferred or deleted—trapping or exonerating those suspected of misappropriating trade secrets. Some digital tools, such as encryption, multi-level passwords and intranets, can protect information more securely than non-digital safeguards.

---

1 *See, e.g.*, United States v. Genovese, 409 F. Supp. 2d 253, 255 (S.D.N.Y. 2005) (defendant charged with selling Microsoft source code on the Internet); Ford Motor Co. v. Lane, 67 F. Supp. 2d 745 (E.D. Mich. 1999) (Internet blogger posted various Ford Motor Company internal documents); Hiawatha Bray, *Website to be Closed as Part of Deal with Apple*, BOSTON GLOBE, Dec. 21, 2007, at 4E, *available at* http://www.boston.com/business/globe/articles/2007/12/21/website_to_be_closed_as_part_of_deal_with_apple (discussing Harvard undergraduate's post of confidential Apple information on the Internet).

2 Mouse Droppings, Mondofacto, http://www.mondofacto.com/facts/dictionary?mouse+droppings (last visited Apr. 10, 2009) (attributing the term to a 1996 MacWorld article by Larry Irving).

Digital watermarking embedded in documents distributed in either hard copy or digital format can permit ready identification of the source of any leaked materials.

In addition to these digital tools, a variety of statutes and emerging case law offer legal tools to remedy the digital misappropriation of trade secrets. Furthermore, as discussed in Part II below, emerging case law reinforces earlier rulings stating that if the trade secret owner moves quickly, even the posting of a trade secret on the Internet does not necessarily destroy the status of the information as a trade secret as a matter of law.

This article discusses reasonable measures to protect trade secrets in a digital world. In particular, it focuses on physical and contractual measures to protect trade secrets. It then discusses legislation, including the Economic Espionage Act[3] ("EEA") and the Computer Fraud and Abuse Act[4] ("CFAA"), that can provide new remedies to aggrieved trade secret owners. It discusses how digital tools can provide early warning and evidence of misappropriation. Finally, it examines what a trade secret owner who has followed these reasonable measures can do upon discovering its trade secrets on the Internet.

I. REASONABLE MEASURES TO PROTECT TRADE SECRETS: WHAT'S DIFFERENT IN A DIGITAL WORLD?

A. Back to Basics

A trade secret owner's duty to be vigilant in protecting its secrets is built into the most frequently applied definition of a "trade secret": a trade secret "derives independent economic value, actual or potential, from not being generally known to . . . other persons" and must be "*the subject of efforts that are reasonable under the circumstances to maintain its secrecy*."[5]

---

3 18 U.S.C. § 1831–39 (2006).

4 *Id.* § 1030.

5 UNIFORM TRADE SECRETS ACT § 1(4)(i)–(ii) (1985) (adopted in 46 states and the District of Columbia) (emphasis added); *see* 18 U.S.C. § 1839(3)(A) (providing that trade secrets must be the subject of "reasonable measures" to keep such information secret). The definitions followed in the other states are based on the Restatement, which provides that "[a] trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it." RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939). The Restatement uses the existence of measures to protect the confidentiality of the information as evidence that the information has value and is in fact secret. *Id.*

Courts and commentators suggest a variety of reasons for imposing the requirement to take "reasonable" measures to maintain secrecy on trade secrets owners: to signal to confidantes and third parties what information is claimed by the owner as its secret, to provide evidence that the information is in fact valuable to the owner and to prevent misappropriation from occurring altogether, thus reducing judicial enforcement costs.[6]

While careful efforts to preserve secrecy are required of trade secret owners, the owner is not required to take every *conceivable* measure to maintain secrecy. The law does not require "super-reasonable" measures to maintain secrecy because doing so would require over-investment in protection, potentially reducing innovation and creating inefficiencies, and would dampen the "spirit of inventiveness."[7] As Judge Posner has explained, a balance between vigilance and practicality must be achieved: "[T]he question is whether the additional benefit in security would have exceeded [the] cost" of the contemplated protection.[8] Trade secret owners are not expected to "take extravagant, productivity-impairing measures to maintain their secrecy."[9] It would be overly burdensome, for example, to require an engineering company to forbid any copying of its drawings, which would require a team of engineers to huddle over a single drawing, rendering efficient work impracticable.[10]

The measures used to protect trade secrets do not need to be "super-reasonable" or cost inefficient in the digital world, either. However, the trade secret owner must be vigilant in identifying new threats and in considering the new digital resources available to counter them. The basic steps for protecting trade secrets remain straightforward: (1) control access to the secret; (2) do not disseminate the secret more widely than necessary; (3) do not give access to individuals who fail to hold the information in confidence; and (4) establish,

---

6 *See, e.g.*, Rockwell Graphic Sys. Inc. v. DEV Indus., Inc., 925 F.2d 174, 179 (7th Cir. 1991); Robert Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CAL. L. REV. 241, 245 (1998); Michael Reisch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV. 1, 45–46 (2007).

7 WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 355, 369 (2003); Douglas Lichtman, *How the Law Responds to Self-Help*, 1 J. L. ECON. & POL'Y 215, 232 (2005). The quote is from the notable case, *E.I. du Pont de-Nemours & Co. v. Christopher*, 431 F.2d 1012, 1016 (5th Cir. 1970), where the court stated that "[its] tolerance of the espionage game must cease when the protections required to prevent another's spying cost so much that the spirit of inventiveness is dampened."

8 *Rockwell Graphic Sys.*, 925 F.2d at 180.

9 *Id.*

10 *Id.*

update and follow security guidelines for keeping it safe.[11] New technologies present new reasons—and new ways—to implement these time-honored rules. Trade secret owners who do not make informed decisions to adapt their practices to take new technologies into account have failed to take reasonable measures to protect their secrets.

B. Digital Safeguards in a Digital Environment

1. Controlling Access to Information

Protecting trade secrets begins with making thoughtful decisions about who should be authorized to gain access to them. When contemplating revealing trade secrets to other businesses, such as suppliers or financial partners, the disclosing party should examine the potential disclosee's business reputation and the practices employed to protect its own trade secrets. A company that is lax with its own information can hardly be trusted to safeguard a third party's secrets. A due-diligence questionnaire should inquire about the disclosee's own use of digital security measures and non-disclosure/non-compete agreements ("NDAs").

If a business arrangement is established, disclosing companies should consider negotiating the right to monitor the protection of their data. While the contours of the relationship will suggest appropriate protective measures, the trade secret owner should never simply leave the details of protection up to the third party without confirming that they are robust.[12] After reviewing the value of the secret and the protections that the recipient can provide, disclosing companies may decide that certain confidential information will be most secure if it resides only on the trade secret owner's server and is accessible only on a secure intranet through use of passwords the trade secret owner controls. The trade secret owner may also want to consider requiring each individual who receives

---

[11] *See, e.g.*, N. Atl. Instruments v. Haber, 188 F.3d 38, 45 (2d Cir. 1999); Twin Vision Corp. v. Bellsouth Commc'n Sys., No. 97-55231, 1998 U.S. App. LEXIS 13607, at *7 (9th Cir. 1998); Basic Chems., Inc. v. Benson, 251 N.W.2d 220, 226 (Iowa 1977); Schalk v. Texas, 823 S.W.2d 633, 636 (Tex. Crim. App. 1991); Jerry Cohen & Alan Gutterman, TRADE SECRETS PROTECTION & EXPLOITATION 89–90 (1997); Roger M. Milgrim & Eric E. Bensen, MILGRIM ON TRADE SECRETS § 1.04 (2007); Victoria A. Cundiff, *Maximum Security: How to Prevent Departing Employees from Putting Your Trade Secrets to Work for Your Competitors*, 8 SANTA CLARA COMPUTER & HIGH TECH. L.J. 301, 304–05 (1992).

[12] *See, e.g.*, Carboline Co. v. Lebeck, 990 F. Supp. 762, 767–68 (E.D. Mo. 1997) (holding that the trade secret owner had not taken reasonable measures to maintain secrecy where, among other things, it took no measures to protect the information in the hands of suppliers or customers).

access to the trade secret at the third party to enter into NDAs directly with the trade secret owner. This would emphasize to those who gain access to trade secrets that the information must be handled with care and would also create a direct contractual cause of action if the recipient compromises secrecy. An added precaution is to require disclosees to periodically certify that they are in compliance with the terms of their agreements. Finally, with the passage of time, the trade secret owner should consider whether the purposes of the disclosure are still valid in the context of the overall business relationship. Information that was disclosed to permit the other party to assess whether to enter into a business transaction, for example, should be promptly retrieved once the potential deal is pronounced dead.

The same care needs to go into disclosing trade secrets internally. Corporate culture and organization will influence choices about the extent to which information is distributed internally. In many organizations, for example, a procurement officer is not likely to need access to manufacturing formulas, although she may need access to a list of raw materials. By the same token, in many organizations a salesperson will not likely need access to manufacturing processes. In other, flatter, organizations, however, especially those selling technical products, salespeople may need access to certain product development information. In some innovative organizations, teamwork is a hallmark of the culture and all employees are expected to contribute to product development and marketing strategies. Any of these approaches may make sense in the context of the overall corporate culture but disclosure choices need to be made intentionally, not by default, and these choices need to be considered in establishing appropriate protective measures for the trade secrets that are disclosed.

Trade secret owners should work to ensure that those to whom they do grant access know that particular information is confidential. One way to do so is by explicitly legending highly confidential documents with precautionary language warning that they are not to be used or disclosed except as authorized by the identified owner. Such legends may help reduce improper disclosures. They may also help a victimized trade secret owner establish that an unauthorized third-party recipient of the trade secret had "reason to know" that it was not free to use them, a necessary step to prevail on a claim under the Uniform Trade Secrets Act.[13] Regardless of what policy choices a company makes about who within the company (or which third parties) will be authorized to access trade secrets, digital tools can provide some economical, dependable methods for enforcing those choices and protecting trade secrets. Tools such as electronically programmable access cards, computer firewalls, password protections

[13] Uniform Trade Secrets Act § 1(2) (1985).

(including frequent changes of passwords and, for particularly sensitive information, multiple levels of passwords), digital watermarks and secure intranets can provide relatively inexpensive ways to control and monitor access to information and to detect and document misappropriation.[14]

2. Deciding Whether To Permit the Digitization of Trade Secrets

Some core trade secrets, such as the Coca-Cola® formula, are of such value that they will likely never be digitized and will always, quite literally, remain under physical lock and key.[15] Even so, certain aspects of even the most valuable secrets may need to be referenced in, for example, computer systems used in running the manufacturing process. Time-honored security measures, such as segmenting access to the information and using coded names for secret ingredients will prevent such information from being revealed in an integrated form that could be easily understood, disclosed or used without authorization.

Many valuable trade secrets, however, are created, developed, updated or maintained in a collaborative digital environment. Thus, most trade secret owners will need to focus on computer security as they assess how to protect their trade secrets.

3. Protecting Computer and File Security

No computer system is impenetrable. Indeed, cunning cyber-thieves may be able to hack into networks, use spoofing or phishing[16] to discern pass-

---

14 *See, e.g.*, Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268, 1301 (S.D. Fla. 2003) (finding reasonable precautions where the plaintiff's network included: "a firewall/gateway," "a security device . . . designed to prevent unauthorized access in a variety of dimensions, and to keep track of any attempts at unauthorized access when they occur" and "a variety of different logs that are generated automatically" upon attempts of unauthorized access).

15 The Coca-Cola® formula is known to only two persons within the company, whose very identities are a closely-guarded secret. The only written record of the formula is kept in a bank vault that can only be opened upon the passage of a resolution by the company's Board of Directors. *See* Coca-Cola Bottling Co. of Shreveport, Inc. v. Coca-Cola Co., 107 F.R.D. 288, 289, 294 (D. Del. 1985).

16 Spoofing is "typically done by hiding one's identity or faking the identity of another user on the Internet," while phishing is an "attempt to steal . . . personal information . . . [by] send[ing] out e-mails that appear to come from legitimate websites such as eBay, PayPal, or other banking institutions." TechTerms.com, http://www.techterms.com/definition (click on "S" and "P," respectively and scroll down to locate the applicable terms) (last visited Apr. 23, 2009).

words or even "dust" computers secured by fingerprint-recognition technology to copy the user's prints and thereby gain access to the computer. But as strong security measures become increasingly available as part of mass-market software programs, courts may increasingly require trade secret owners to use such measures as part of their reasonable precautions to protect their trade secrets. Failing to install and consistently use commonplace security measures may be found as failure to take reasonable measures to protect trade secrets. For example, standard software tools now make it possible to readily protect key information by requiring use of a separate password to access individual documents after the initial computer log-on. Tutorials on how to use these simple tools are as accessible as clicking the "help" tool on mass-distributed copies of Microsoft Word and Adobe Acrobat. Courts have thus seen the failure to install this extra layer of security as an indication of failure to take reasonable measures to maintain secrecy.[17]

Where frequent information exchanges are planned with trusted business partners, organizations may be able to control access by creating a secure intranet or password-protected FTP server. This approach lets the trade secret owner control and terminate access to the information and has the benefit of preventing transmission of confidential information over the Internet where it can be more readily misdirected. While this approach may not be cost-justified in every case, it, too, is becoming more widely practical.

Other digital tools to protect trade secrets residing on computers can be more resource intensive. While technology to encrypt highly-sensitive data and to prevent it from being forwarded to unauthorized users has become more widely available and less expensive over the past few years, it can still be costly and time-consuming to use for all but the most sensitive information. For example, encrypting an entire sixty to eighty gigabyte laptop can take up to eight hours.[18] That time commitment may be justifiable for the company's crown-jewel information, since security breaches can be quite costly. In a recent study, 57% of the 116 companies surveyed estimated that even a single security breach would cost their organization over $500,000.[19] Other reports suggest even high-

---

17 *See, e.g.*, Boston Laser, Inc. v. Zu, No. 3:07-CV-0791, 2007 WL 2973663, at *10, *12 (N.D.N.Y. Sept. 21, 2007) (finding that plaintiff had not taken reasonable measures to preserve secrecy where, among other things, "the computer network on which such matters are digitally stored is generally not even password protected beyond the log-in process").

18 Gary Anthes, *Encryption: Do It Today or Pay Tomorrow*, COMPUTERWORLD, May 21, 2007, http://www.computerworld.com (search for "encryption: do it today") (last visited Feb. 13, 2009). Of course, encrypting a single file or group of files will take less time.

19 Steve Norall, *The Growing Importance of Storage Security & Key Management in Large Enterprises*, GLOBAL SECURITY MAG., Sept. 2007, http://www.globalsecuritymag.com/

er potential exposure.[20] In recognition of that fact, the use of encryption to protect data is on the rise among business enterprises, with a recent survey indicating that 74% of the surveyed U.S. companies have some encryption plan and 21% implemented an encryption strategy across the enterprise.[21] However, the use of encryption can also slow communications and must be in use at both ends of the transmission, potentially increasing IT and transaction costs.[22] The case law, while recognizing the use of encryption as evidence of the trade secret owner's efforts to protect trade secrets,[23] has thus not yet reached a point where failing to use such encryption as a matter of course constitutes a *per se* failure to take reasonable measures to preserve secrecy.

What measures are "reasonable" may change over time, however. Given the rapidly evolving availability of lower-cost digital safeguards, the diligent trade secret owner will want to coordinate closely with IT personnel to keep abreast of advances in protective technology and to understand how difficult such advances would be to implement. Indeed, state bar organizations that have opined that attorney-client communications do not currently have to be encrypted to create a reasonable expectation of privacy have cautioned that lawyers "must" stay abreast of evolving technology to assess any changes in the likelihood of interception, as well as the availability of improved technologies that may reduce such risk at reasonable cost.[24] Not keeping up with new safe-

---

article-Special-Reports,20071001,27.html (last visited Feb. 13, 2009).

20 *See generally* PONEMON INST. LLC, 2008 ANNUAL STUDY: U.S. ENTERPRISE ENCRYPTION TRENDS (March 2008).

21 *Id.* at 8.

22 For a discussion of practical complications in using encryption, see Elinor Mills, *To Encrypt or Not, That is the Question*, Oct. 2, 2008, CNET NEWS, http://www.news.cnet.com/8301-1009_3-10055033-83.html?tag=mncol (last visited February 22, 2009). Note that a number of the practical impediments to encryption, such as the need to coordinate with recipients to ensure that encryption is in use by the proposed recipient, are less of an obstacle for communications between organizations than for communications between individuals, since the disseminating organization will need to "pre-qualify" and approve the recipient in any event. Moreover, organizations wishing to exchange trade secrets with each other must consider the valuation of the entire exchange, since the up-front cost of implementing such procedures also reduces the potential risks, and therefore total costs, of collaboration.

23 *See, e.g.*, Aetna, Inc. v. Fluegel, No. CV074033345S, 2008 WL 544504, at *5 (Conn. Super. Ct. Feb. 7, 2008) (commenting on plaintiff's use of encryption for some documents as evidence of its reasonable measures to maintain secrecy).

24 *See* N.J. Supreme Court Ethics Comm., Advisory Comm. on Prof'l Ethics, Opinion No. acp701 (2006) (discussing the electronic storage and access of client files); N.Y. St. Bar Ass'n, Comm. on Prof'l Ethics, Opinion 820 (2008) (discussing the use of an e-mail service provider that scans e-mail for advertising purposes); N.Y. St. Bar Ass'n, Comm. on Prof'l

guards is not reasonable. A decision not to encrypt trade secrets that is reasonable this year may become unreasonable in the future if encrypting documents becomes a commonplace and inexpensive practice.[25]

4. Limiting Use of Digital-Storage Media and Restricting Data Transmission

Digital technology is not only capable of protecting trade secrets; it can also place trade secrets at substantial risk. Because so many individuals regularly carry their own personal devices for generating, recording, storing and transmitting digital data (*i.e.*, cameras in cell phones, USB drives and mp3 players), the trade secret owner should consider whether or not to allow such devices into highly secure areas on company property. Thus, if a prospective business partner is given access to a manufacturing facility, in addition to signing a NDA, the visitor should be expressly prohibited from bringing such devices into the facility and should be restricted from entering the most sensitive locations.[26]

A company may also want to restrict its own employees and consultants from taking their own digital devices into the most highly secure areas of the company. While signing an NDA including such provisions will not prevent all violations, it should heighten sensitivity to security issues. The use of NDAs will also support a trade secret owner's breach of contract or tort claim in the event of misappropriation of a trade secret, and may form a strong foundation for injunctive relief.[27] Finally, NDAs will help rebut a claim in litigation with

---

Ethics, Opinion 709 (1998) (discussing the use of the Internet to advertise and to conduct a trademark-focused law practice, the use of e-mail and the use of trade names).

25 *Cf.* T.J. Hooper v. N. Barge Corp., 60 F.2d 737, 740 (2d Cir. 1932) (holding that "seaworthiness" is a term whose definition is not fixed but evolves with technological advances, and, while a seaworthy vessel of an earlier era would not have incorporated a radio, radios were available to vessels of 1928 and thus should have been used).

26 No protection policy is always effective: witness the recent indictment of two employees of Wyko Tire for allegedly misrepresenting their purpose for visiting a Goodyear Tire manufacturing facility, straying into unauthorized areas, using their cell phone cameras to photograph secret equipment and e-mailing the photos to colleagues outside the United States. United States Dept. of Justice, Criminal Div., Two Indicted for Conspiring to Steal Trade Secrets From Goodyear Tire and Rubber Company (Mar. 6, 2009), http://www.usdoj.gov/opa/pr/2009/March/09-crm-204.html. However, the fact that such precautions are in place and are spelled out to visitors should reduce the risk of a successful defense that the owner failed to take reasonable precautions to maintain secrecy and makes it more likely that the defendants will be found to have acquired the trade secret through unauthorized, and therefore "improper," means.

27 *See, e.g.*, Aware, Inc. v. Centillium Commc'ns, Inc., 2009 WL 782115, at *1 (D. Mass. Mar. 13, 2009) (breach of contract claim related to a product development and license agreement

third parties that the company did not take reasonable measures to protect its secrets.[28]

To protect against external dissemination of trade secrets by employees and consultants, companies can take such precautions as imposing restrictions on the amount of data that employees can transfer using company servers. While this approach may not be practical in document-intensive organizations such as consulting or law firms, it may be particularly appropriate for financial institutions and for research organizations that do not routinely transmit large files. To prevent employees from transferring sensitive digitized information to their home or alternate computers through popular web-based storage areas such as g-mail, AOL or Yahoo!, companies can prevent access to such sites from the company servers. To prevent the use of USB drives and similar devices for the unauthorized transfer of data,[29] companies can work with their IT staff to disable or eliminate USB ports on all but certain designated company computers.

Recognizing the practical reality that at times many key employees will need to perform work for the company off-site, companies must also develop realistic guidelines for how company data can be safely accessed off-site, specify any devices to which it can legitimately be transferred and ensure that once the legitimate purpose has been accomplished, the data is properly deleted from any non-company memory devices.

Regardless of whether companies issue laptop computers or other electronic data storage devices to their employees, requiring employees to provide periodic certifications that identify all digital storage devices to which the employee has transferred company information can keep both the employee and the company focused on where data is being stored and what data needs to be de-

---

including, *inter alia*, confidentiality provisions); MacDermid, Inc. v. Raymond Selle & Cookson Group PLC, 535 F. Supp. 2d 308, 317–18 (D. Conn. 2008) (granting employer a preliminary injunction to prevent violations of non-disclosure and non-compete agreements); Harvard Apparatus, Inc. v. Cowen, 130 F. Supp. 2d 161, 175–76 (D. Mass. 2001) (noting that confidentiality agreements signed by employees supports an inference that the underlying information was confidential).

28 *See, e.g.*, Xantrex Tech. Inc. v. Advance Energy Indus., Inc., 2008 WL 2185882, at *18 (D. Colo. 2008) ("It is undisputed that Xantrex took reasonable measures in protecting against disclosure of the Xantrex trade secrets, having employees sign non-disclosure agreements such as the one [the defendant] signed, as well as housing important documents on a secure, user-access controlled server.").

29 A striking example of the use of USB drives to remove vast amounts of information may be found in *Andarko Petroleum Corp. v. Davis*, No. H-06-2849, 2006 WL 3837518, at *6 (S.D. Tex. Dec. 28, 2006), where an expert testified that by repeatedly loading two USB drives, one defendant was able to download the equivalent of 1.5 million pages of raw data and transport much of it to his computer at his new employer.

leted. Finally, when the employee or consultant and the company end their relationship, it is good practice to require departing employees to certify that the information has been properly deleted from each device the company does not own. Such certifications can be useful reminders to employees and provide grounds for impeachment if litigation ensues.[30]

5. Traveling with Digitized Trade Secrets

Employers would do well to remind employees not to use laptops and other digital storage devices off-site in a manner that permits third parties to see them. A recent survey of 1000 U.S. and British mobile workers confirmed the unsurprising fact that it has become increasingly easy to view sensitive information on others' laptops in public places.[31] One-third of the workers polled admitted to encountering competitively sensitive information while traveling, simply because it was there in the open to be seen or heard. More alarmingly, 10% of those polled admit to having been able to use the information for their own business purposes.[32] Given these findings, it may be cost-effective —a "reasonable measure"—for a company to spend a few dollars per employee on a physical "privacy screen" to shield computer screens from the view of strangers and to remind employees not to discuss sensitive company business where they can be overheard.

As a further security refinement, some companies require employees traveling with company computers to replace their regular "fully loaded" hard drive with a clean hard drive to prevent the risk of exposing information not necessary for the specific business trip or to carry the necessary information with them on an authorized USB drive that they can keep with them at all times. This approach may become more common given a Ninth Circuit ruling that the U.S. Customs Department ("Customs") can seize and search travelers' laptops without probable cause.[33] Indeed, recent reports indicate that Customs has been

---

30 *See, e.g.*, Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1330 (N.D. Ga. 2007) (noting that "[d]espite having recently copied . . . numerous electronic files . . . onto his home computer, Davidson also certified in writing at an exit interview that he did not have in his possession, nor fail to return" any such materials, which was a clear misrepresentation, constituting evidence of misappropriation and breach of contract).

31 Louisa Peacock, *Data Protection: Mobile Working Leaves Secret Company Information Exposed to Snoopers*, PERSONNELTODAY, June 20, 2008, http://www.personneltoday.com/articles/2008/06/20/46410/data-protection-mobile-working-leaves-secret-company-information-exposed-to-Snoopers.html (last visited Feb. 13, 2009).

32 *Id.*

33 United States v. Arnold, 523 F.3d 941, 948 (9th Cir. 2008).

increasingly impounding the laptops of corporate travelers.[34] While the extent of such seizures is not yet known, the possibility of a seizure is an additional reason not to travel with more information than necessary for a particular trip.

Finally, those permitted to carry trade secrets in laptops, PDAs or other digital storage devices should be reminded that the loss or compromise of such devices can now place thousands of files at risk, not just a few pages. Common-sense safeguards—such as not leaving devices unattended and being sure digital devices are not accidentally left behind in public areas—therefore take on a heightened importance. Examples of such missteps are increasingly familiar in news reports. While news accounts have not revealed details of any trade secrets lost in this manner, in one highly publicized case, the Transportation Security Administration ("TSA") lost a computer drive containing names, social security numbers, birth dates, payroll data, financial allotments and bank account routing numbers for roughly 100,000 former and current TSA employees.[35] Because the consequences of losing digitized data are potentially so widereaching, savvy high-tech companies are increasingly evolving and updating corporate security guidelines,[36] as well as imposing reporting requirements so the effects of a breach can be properly contained.[37]

6. Conducting Training Programs to Address Adapting Traditional Security Measures to a Digital Environment

One of the most critical measures to maintain secrecy is also the most reasonably priced: developing a culture of protection. In-house training pro-

---

34 *See* Nanci Clarence & Craig Bessenger, *They Have Ways of Making Your Laptop Talk*, THE RECORDER, July 2, 2008, http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202422695427 (last visited Feb. 13, 2009) (emphasizing the "Justice Department's [recent] expansive view of the government's authority" to perform these searches); Lisa Crosby, *Cross-Border Travel Traps: Protecting Client Confidences at the Frontier* 11–12 (Fall 2007), http://www.abanet.org/intlaw/fall07/materials/CrossBorderTravelTrapsProtectingClientConfidences.pdf (last visited Feb. 13, 2009).

35 Stephen Losey, *TSA is Missing Hard Drive With Employees' Personal Information*, FEDERALTIMES.COM, May 7, 2007, http://www.federaltimes.com/index.php?S=2744540 (last visited Apr. 25, 2009).

36 For example recommendations for traveling with computers, see Tom Bradley, *Top 10 Tips To Secure Laptops For Air Travel*, http://netsecurity.about.com/od/newsandeditorial1/a/laptopairsafety.htm (last visited Apr. 25, 2009).

37 One study suggests that hundreds of thousands of laptops are lost in airports every year and that some employees never report the loss. PONEMON INSTITUTE LLC, AIRPORT INSECURITY: THE CASE OF MISSING & LOST LAPTOPS 3, 14 (2008). Most of the lost laptops contain confidential company information. *Id.* at 14.

grams can help ensure that secrecy precautions do not consist simply of a single policy statement the employee signs when starting a new job. Ongoing training makes the protection of trade secrets a continuous commitment that is constantly refined in light of new technical issues and solutions. Frequent training programs can focus not only on new technological threats but also on the core goals and critical importance of the overall trade secrets protection program. Courts increasingly cite the use of such training programs as evidence that a plaintiff has taken reasonable precautions.[38]

Training programs must reflect modern realities. To offer reasonable protections, the programs of today will necessarily include guidelines to address additional issues than those provided just a few years ago. The company needs to consider its position on such new communication tools as blogs, for example. In some high-tech environments, prohibiting employees from "blogging" will likely lead only to deception or a shrinking pool of qualified applicants. In such environments, rather than simply ignoring blogs, the training program might appropriately acknowledge or even "embrace" the "blogosphere" by establishing and presenting company guidelines for "safe" blogging.[39]

Moreover, in conducting such training programs, trade secret owners must be mindful that sometimes measures to maintain the secrecy of information in the physical world are not effective online. One notorious example was the U.S. military's effort to electronically "black out" portions of a classified document before making it available on its website.[40] The electronic "black out" function could neatly obscure confidential portions of documents intended to be printed out as hard copies.[41] If the same documents were viewed online, however, the "black out" square could be undone by viewers, which would reveal the

---

38 *See* Avery Dennison Corp. v. Finkle, No. CV010757706, 2002 WL 241284, at *3 (Conn. Super. Ct. Feb. 1, 2002) (finding the fact that company provided employees yearly refresher courses in intellectual property and trademarks as evidence that company had used reasonable precautions to maintain the secrecy of its information); *cf.* Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1336 (N.D. Ga. 2007) (finding that employer had not taken reasonable measures where, among other failings, it "provided virtually no guidance to its employees concerning the safe handling of this information").

39 *See, e.g.*, IBM, IBM Social Computing Guidelines, http://www.ibm.com/ (search "social computing guidelines") (last visited Apr. 25, 2009). The guidelines are noted to be evolving and emphasize that "it is very much in IBM's interest—and, we believe, in each IBMer's own—to be aware of and participate in this sphere of information, interaction and idea exchange" while, among other things, protecting confidential and proprietary information. *Id.*

40 Munir Kotadia, *U.S. Military Security Defeated by Copy and Paste*, CNET NEWS, May 4, 2005, http://news.cnet.com/U.S.-military-security-defeated-by-copy-and-paste/2100-1002_3-5694982.html (last visited Feb. 13, 2009).

41 *Id.*

hidden text.[42] Parties in litigation have suffered the same problem when e-filing electronically-redacted documents that can then be readily unredacted by all who view the file.[43] The point is not the details of this specific example—methods for protecting redacted information may change over time and the risk to digitized information is not limited to redacted data. The key is to be aware of, *and advise* all relevant personnel concerning new challenges and technological solutions to reducing the risk to digitized data.

While focusing on new high-tech security issues is important, trade secret owners should not ignore commonsense precautions in their training programs. One mundane example of a security breach that employees should be reminded to avoid is e-mailing documents revealing "track changes." A company's thinking, proposed negotiation strategy or commercial weaknesses can be revealed through, for example, the following types of internal notes: "I'd delete this section since we don't have these features on the roadmap and haven't figured out how to code this unless you believe investors won't catch this."[44]

Specialized training programs may be appropriate for some company personnel, including those having responsibility for particular types of confidential information. For example, the company should conduct training programs to acquaint IT personnel with the various state, federal and international privacy statutes prohibiting misuse of personnel data collected through websites and other electronic data collection processes.

Finally, companies should include outside consultants or other third parties who are granted access to company secrets in the core training programs

---

42 *Id.*

43 *See* Declan McCullagh, *AT&T Leaks Sensitive Info in NSA Suit,* CNET NEWS, May 26, 2006, http://news.cnet.com/AT38T-leaks-sensitive-info-in-NSA-Suit/2100-1028_3-6077353.html (last visited Feb. 13, 2009) (describing how obscured text can be copied, pasted and viewed inside some PDF readers). The most effective security device may be an old-fashioned one: use a black felt-tipped marker to black out the information and then make a PDF copy of the redacted document. In addition, some electronic redacting techniques do work. *See* Joris Evers, *Editing Tips from the NSA*, CNET NEWS, Jan. 24, 2006, http://news.cnet.com/Editing-tips-from-the-NSA/2100-1029_3-6030745.html (last visited Feb. 13, 2009) (describing common techniques from Microsoft Word and Adobe Acrobat). The details of the best approach, which can change over time, are not as important as the critical fact that every method for protecting trade secrets must be periodically tested against new technologies.

44 *See* Rick Segal, *The Coolest Business Plan Ever*, The Post Money Value, http://ricksegal.typepad.com/pmv/2008/05/the-coolest-bus.html (May 6, 2008) (last visited Feb. 13, 2009) (commenting on a business plan in which internal, visible comments had been forwarded without first accepting all changes in track changes).

discussing confidentiality safeguards—while being mindful not to use those training sessions themselves as a way of revealing specific secrets to consultants who do not otherwise need to know them in the scope of their assignment.

C. Special Contracting Tips for the Digital World

While in the tangible world it may not always be essential to require parties receiving access to trade secrets to sign a NDA,[45] it is good practice. In the digital world, however, it can be essential. First, NDAs should make clear what information the trade secret owner claims should be protected. Second, NDAs are evidence that the person to whom the secret is properly disclosed has agreed to protect it. This fact can be of vital importance when the trade secret owner is forced to seek injunctive relief to protect the secret. For example, a court may be more likely to order the removal of a trade secret that has been posted on the Internet by a vengeful employee if the employee has signed a NDA, thereby contracting away any First Amendment right with respect to the posting.[46] While the California Supreme Court held in *DVD Copy Control Ass'n v. Bunner*[47] that any such First Amendment right would not necessarily trump the trade secret owner's Fifth Amendment rights in its property,[48] requiring authorized recipients of trade secrets to agree not to post the secrets on the Internet or on other electronic messaging services should help forestall a First Amendment challenge to injunctive relief.

In entering into NDAs, trade secret owners should resist limiting the non-disclosure obligation to a fixed period of time. A trade secret is legally protectable until such time as it has become generally known or others are able to independently develop the information through lawful means.[49] Contractually limiting the obligation to treat the information as a trade secret[50] to a shorter

---

45 *See, e.g.*, Phillips v. Frey, 20 F.3d 623, 632 (5th Cir. 1994) (finding implied duty of confidentiality where information was disclosed at the request of a party who purported to need it in evaluating a business deal it had proposed).

46 *Cf.* Ford Motor Co. v. Lane, 67 F. Supp. 2d 745, 753 (E.D. Mich. 1999) (contrasting showing to be made when a third party posts trade secrets as opposed to a posting made by an employee subject to a NDA; noting that the latter has waived First Amendment rights).

47 74 P.3d 1 (Cal. 2003).

48 *Id.* at 16–17.

49 Uniform Trade Secrets Act § 1(4) (1985).

50 Note that some jurisdictions, most notably Georgia and arguably Wisconsin, require contractually specified finite time limits on non-disclosure obligations relating to *confidential information* that does not qualify as a trade secret. *See, e.g.*, Equifax Servs., Inc. v. Examination Mgmt. Servs., Inc., 453 S.E.2d 488, 491, 495 (Ga. Ct. App. 1995); Williams v. N. Tech. Servs., Inc., No. 95-2809, 1997 WL 330306, at *5 n.6, *8 (Wis. Ct. App. 1997). While there

period of time, however, through provisions stating that the obligation shall be in effect for "two years after first access," for example, may be found to constitute a failure to take reasonable precautions to maintain secrecy for a longer period of time, even if the plaintiff follows other security precautions for a longer period of time.

Thus, in *Silicon Image, Inc. v. Analogix Semiconductor, Inc.*[51] the court found that, notwithstanding the plaintiff's diligent use of other measures to maintain secrecy, the fact that its NDAs required distributors and customers to keep schematic and programming information confidential only for specified periods of two or three years mandated a finding that the plaintiff had not taken reasonable measures to maintain secrecy against third parties once those NDAs had expired.[52] The parties who had signed the NDAs were now contractually free to use or disclose the information at any time. The plaintiff attempted to justify the time limitation on secrecy as "reasonable" because, it claimed, "companies in the Silicon Valley will not sign a non-disclosure agreement that imposes perpetual confidentiality obligations."[53] The court rejected this justification, finding that since the trade secret owner had not taken reasonable contractual measures to protect its trade secrets beyond the contractual period, it must not have thought the secret was worth protecting—even against third parties—for a longer period.[54] The holding is a warning that if a particular business party will not agree to hold the information in secrecy on the trade secret owner's terms, the trade secret owner may have to choose between maintaining long term trade secrecy as against the world and making the disclosure to that particular business party.

Companies should not only contractually require individuals to whom they provide access to trade secrets to agree to return all such secrets at the termination of the relationship (or earlier, as directed), but also require deletion of those secrets from the hard drives of any computers or electronic storage devices used by the individual that are not owned by the company. Conversely, to prevent disgruntled employees from crippling the company upon their departure, employees should also be directed not to delete trade secrets from company computers without express authorization.

---

is room for debate over what information falls into each category, a critical point in distinguishing the two categories of information seems to be whether the information has actual or potential independent economic value.

51 No. C-07-00635, 2008 WL 166950 (N.D. Cal. Jan. 17, 2008).

52 *Id.* at *12.

53 *Id.*

54 *Id.*

Employee agreements should also clearly state that employees are not authorized to use or access company computers for personal economic or business gain.[55]

Finally, trade secret owners should pay close attention to the special risks that departing IT administrators and security staff can pose to trade secrets and confidential information. Such personnel might be directed to sign an addendum to the "standard" company secrecy agreements in which they acknowledge and certify that company domain names are the company's property, that all domain name registrations prepared by the employee are held in trust for the company, and that all user passwords, system and user data, system reports and security analyses are company property which may not be disclosed or used for others. Law firms should be particularly sensitive to this obligation, as Model Rule of Professional Conduct 5.3 requires attorneys to ensure that non-lawyers conduct themselves in accordance with client confidentiality obligations.[56]

D. Federal Statutes: The Economic Espionage Act and the Computer Fraud and Abuse Act

Recognizing that computers increasingly serve as "get-away cars" when trade secrets are misappropriated, trade secret owners have turned for relief to a variety of federal and state statutes that prohibit unauthorized use and access of computer systems. The EEA and the CFAA both provide remedies that may, in particular cases, go beyond those provided under state misappropriation statutes.[57] Moreover, both Acts also offer potential access to the federal courts,

---

55 *See infra* Part 1.D.3.

56 MODEL RULES OF PROF'L CONDUCT R. 5.3 (1983); *see* Joshua Poje, *Model Rule 5.3 and Your Technical/Computer Staff,* ABA LEGAL TECHNOLOGY RESOURCE CENTER, June 23, 2008, http://meetings.abanet.org/ltrc/index.cfm?data=23/06/2008 (last visited Feb. 13, 2009) (reporting a recent survey of 300 senior-IT professionals revealing that one-third of the responders admitted to browsing confidential data and one-half admitted to looking at information that did not directly concern them).

57 Violators of the Economic Espionage Act can be fined up to $500,000 and imprisoned up to 15 years, 18 U.S.C. § 1831(a) (2006), and may be subject to injunctive relief and forfeiture. *Id.* §§ 1834, 1836. The Computer Fraud and Abuse Act subjects perpetrators to a fine and potential imprisonment up to five years and additionally provides civil remedies. *Id.* §§ 1030(c), (g). Remedies under the Uniform Trade Secrets Act include injunctive relief, damages as proven at trial and, potentially, punitive damages and attorneys fees. Uniform Trade Secrets Act §§ 2–4 (1985). Note that use of a computer to transmit trade secrets can constitute misappropriation under state trade secret statutes, regardless of whether it is also a violation of the EEA or the CFAA. *See, e.g.*, Newsouth Commc'ns Corp. v. Universal Tel. Co., No. CIV.A. 02-2722, 2002 WL 31246558, at *21–22 (E.D. La. Oct. 4, 2002) (holding that e-mailing trade secrets out of the company without authorization or for purposes con-

which, absent diversity jurisdiction, would otherwise be denied to a trade secret owner. Each has been used to punish trade secret misappropriation accomplished with the use of computers.[58]

1. Differences Between the Acts

Each of the Acts, however, also poses practical limitations. For example, while the EEA offers the advantage of having been specifically enacted to protect trade secrets,[59] it currently provides no private right of action. A trade secret owner may not be able to interest a prosecutor in a particular dispute or for a variety of reasons may prefer to file a private action.[60]

By contrast, the CFAA does provide a private right of action.[61] However, unlike the EEA, the CFAA was not enacted with trade secret protection in mind, nor is it a private, civil version of the EEA.[62] It is an anti-"hacking" statute.

The EEA focuses on the nature of the *information* that the defendant has allegedly misappropriated and, among other things, expressly prohibits the unauthorized transmittal, downloading or uploading of a trade secret using com-

---

trary to those of the trade secret owner can constitute trade secret misappropriation under the Louisiana Uniform Trade Secrets Act).

58 *See* B & B Microscopes v. Armogida, 532 F. Supp. 2d 744, 758 (W.D. Pa. 2007) (holding that an employee violated the CFAA when he destroyed company computer files containing trade secrets that he had developed for the company); United States v. Genovese, 409 F. Supp. 2d 253, 254 (S.D.N.Y. 2005) (indicting an individual under the EEA for selling, over the Internet, "jacked" computer source code). The Economic Espionage Act is not limited to misappropriation involving the use of computers. For examples of criminal prosecutions under the two statutes, see the website of the Computer Crime and Intellectual Property Section of the Department of Justice, http://www.usdoj.gov/ criminal/cybercrime/ index.html (last visited Apr. 25, 2009).

59 18 U.S.C. §§ 1831–1832.

60 *See, e.g.*, Joseph N. Hosteny, *The Economic Espionage Act: A Very Mixed Blessing*, INTELL. PROP. TODAY, Feb. 1998, at 8 (placing emphasis on reflections by a former prosecutor who described some of the reasons that prosecutors may decline to prosecute violations of the EEA).

61 Under the CFAA, any individual who has suffered damage or loss by a violation of the Act may "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

62 Some trade secret misappropriations involving the use of computers do not fall within the terms of the CFAA. *See, e.g.*, Am. Family Mut. Ins. Co. v. Rickman, 554 F. Supp. 2d 766, 772 (N.D. Ohio 2008) ("[C]omputer access alone does not make the conduct subject to the CFAA.").

puters.[63] Remedies for violation include, in addition to fines and imprisonment, criminal forfeiture of property constituting, or derived from, any proceeds obtained as a result of the misappropriation.[64] Significantly, the Department of Justice takes the position that the Mandatory Victims Restitution Act of 1996[65] ("MVRA") applies to violations of the EEA.[66] The MVRA provides for restitution to the victim of the full amount of the victim's losses caused by defendant's acts.[67]

The CFAA, by contrast, focuses on intrusions to the *computer system* housing the information. The CFAA was initially designed to protect against unauthorized access to classified information, financial records and credit information on governmental and financial institution computers.[68] Its protections were later extended to information present on any computers in interstate commerce, with some limitations.[69] The CFAA punishes anyone who "intentionally accesses a computer or system without authorization or "exceeds authorized access, and thereby obtains . . . information from any protected computer," where a "protected computer" includes any computer that "is used in or affect[s] interstate or foreign commerce or communication."[70] The CFAA defines "exceeds authorized access" as "access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser

---

63 18 U.S.C. § 1831(a)(2). In a recent guilty plea under the Act, a former IBM employee admitted violating the EEA by duplicating, downloading and e-mailing a highly confidential IBM Memo—"marked 'IBM Confidential' on each page"—to a Hewlett-Packard Senior Vice President with the subject line "For Your Eyes Only." United States v. Malhotra, No. CR 08-00423, at 2–3 (N.D. Cal. filed June 27, 2008), *available at* http://blog.wired.com/27bstroke6/files/malhotrachargingdoc.pdf. Hewlett-Packard immediately reported the event to the Department of Justice. Defendant Atul Malhotra's Memorandum Re Sentencing; Exhibits at 2, United States v. Atul Malhotra, No. CR 08-00423-JF (N.D. Cal. filed Oct. 21, 2008).

64 18 U.S.C. §§ 1834, 1836.

65 Mandatory Restitution Act of 1996 § 204, 18 U.S.C. § 3663A (2006).

66 U.S. DEP'T OF JUSTICE, COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., PROSECUTING INTELLECTUAL PROPERTY CRIMES MANUAL 174–75 (3d ed. 2006), *available at* http://www.usdoj.gov/criminal/cybercrime/ipmanual/ipma2006.pdf.

67 18 U.S.C. §§ 3663A(c)(1)(B), 3664(f)(1)(A).

68 S. REP. NO. 99-432, at 3 (1986).

69 18 U.S.C. § 1030(a)(7).

70 *Id.* §§ 1030(a)(2), e(2). The Act also prohibits the unauthorized access of computers to defraud and the access of computers without authorization causing damage. *Id.* §§ 1030(a)(4)–(5), (e)(6), (e)(8) (defining the violations described). It has been held not to apply to failed attempts to access protected computers. Scory LLC v. Maroney, No. 51064(U), slip op. at 3–4 (N.Y. Sup. Ct. May 22, 2007).

is not entitled . . . to obtain or alter."[71] It does not, however, define "without authorization." That omission has been the focus of considerable judicial discussion where the violation is alleged to have been committed by employees or other "insiders" to whom the trade secret owner had at some point granted authorization to access the protected computer in furtherance of legitimate activities for the owner.[72]

Further, while recovery under the CFAA can include compensation for "*any reasonable cost* to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service,"[73] "reasonable cost" has been held not to include revenue lost by reason of trade secret misappropriation.[74]

---

71 18 U.S.C. § 1030(e)(6).

72 *See infra* Part I.D.3.

73 18 U.S.C. § 1030(e)(11) (emphasis added); *see* Modis, Inc. v. Bardelli, 531 F. Supp. 2d 314, 320 (D. Conn. 2008) (stating in dicta that "'the costs of responding to the offense' are recoverable regardless of whether there is an interruption in service, and federal courts have sustained actions based on allegations of costs to investigate and take remedial steps in response to a defendant's misappropriation of data"). Furthermore, in *In re Doubleclick Inc. Privacy Litigation*, the court looked to a Senate Report and stated:

> [I]ntruders often alter existing log-on programs so that user passwords are copied to a file which the hackers can retrieve later. After retrieving the newly created password file, the intruder restores the altered log-on file to its original condition. Arguably, in such a situation, neither the computer nor its information is damaged. Nonetheless, this conduct allows the intruder to accumulate valid user passwords to the system, requires all system users to change their passwords, and requires the system administrator to devote resources to resecuring the system. Thus, although there is arguably no 'damage,' the victim does suffer 'loss.' If the loss to the victim meets the required monetary threshold, the conduct should be criminal, and the victim should be entitled to relief.
>
> . . . Under the bill, damages recoverable in civil actions by victims of computer abuse would be limited to economic losses for violations causing losses of $5,000 or more during any 1-year period. *S. Rep. No. 104-357 seems to make clear that Congress intended the term "loss" to target remedial expenses borne by victims that could not properly be considered direct damage caused by a computer hacker.*

154 F. Supp. 2d 497, 521 (S.D.N.Y. 2001) (quoting S. REP. NO. 104-357, at 11 (1996)) (emphasis added in last sentence) (emphasis in original removed).

74 *See* Andritz, Inc. v. S. Maint. Contractor, LLC, No. 3:08-CV-44 (CDL), 2009 WL 48187, at *3 (M.D. Ga. Jan. 7, 2009) (dismissing CFAA claim where plaintiff did not allege that it had lost revenue or incurred costs because of an interruption of service but only that it was dam-

Thus, while the CFAA is increasingly invoked as a way of pursuing those who have used computers to access and disseminate trade secrets, it is not well-suited to address every trade secret misappropriation involving computers, particularly those coming at the hands of people who had once been trusted "insiders," and it does not remedy all injuries that may have been caused by the use of computers to steal trade secrets.

2. Uses of the CFAA Against Outsiders

In appropriate cases, however, the CFAA has proved to be an important tool in fighting trade secret misappropriation involving the use of a computer. For example, in *Creative Computing v. Getloaded.com LLC*,[75] the CFAA was used to punish unauthorized use of another's password to access a restricted website. To prevent competitors from taking advantage of the information posted on its website, Creative, the trade secret owner, restricted access to certain key portions of its logistics website solely to subscribers.[76] In response, Getloaded, a potential competitor, "used the login name and password of a . . . subscriber, in effect impersonating the trucking company, to sneak into [Creative's website]."[77] Getloaded also hired a Creative employee who, before his resignation, had downloaded confidential information, permitting him to access Creative's server from home and obtain information "regarding several thousand of Creative's customers."[78] The court concluded that "[t]hese tricks enabled [Getloaded] to see all of the information available to Creative's bona fide customers" and that Getloaded had exploited an unpatched security hole to gain access

---

aged because defendants copied proprietary information and used it to steal customers from plaintiff); Condux Int'l, Inc. v. Haugum, No. 08-4824 ADM/JSM, 2008 WL 5244818, at *8 (D. Minn. Dec. 15, 2008) (noting that defendant's activity may well have diminished the confidentiality, exclusivity or secrecy of the proprietary information, but holding that to cause damage under the CFAA the action "must have had an effect on the binary coding used to create, store, and access computerized representations of information"); Am. Family Mut. Ins. Co. v. Rickman, 554 F. Supp. 2d 766, 772 (N.D. Ohio 2008) ("[T]he underlying premise of [the CFAA] is directed toward computer piracy, and the loss of revenue must be related to the misuse of the computer—something more than misuse of information obtained from the computer through authorized access."); L-3 Commc'ns Westwood Corp. v. Robicharux, No. 06-0279, 2007 WL 756528, at *4 (E.D. La. Mar. 8, 2007) (same); Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 478 (S.D.N.Y. 2004) (same).

75 386 F.3d 930 (9th Cir. 2004).

76 *Id.* at 932.

77 *Id.*

78 *Id.*

to the code "Creative used to operate its website."[79] The court therefore upheld the jury's finding that Getloaded had violated both the Idaho Trade Secrets Act and the CFAA.[80]

The trial court had entered a temporary injunction against, among other things, destroying evidence.[81] Getloaded destroyed evidence in violation of the temporary injunction, leading the trial court to grant a more expansive permanent injunction[82] which enjoined Getloaded from "accessing any portion, *public or not*, of [Creative's] website."[83] The Ninth Circuit affirmed the award of damages and attorney's fees and the trial court's entry of the broad permanent injunction, concluding that "the past egregious conduct of Getloaded, its owners and employees, . . . justif[y] the extraordinarily broad prohibition imposed."[84] The court reasoned that "Getloaded [was] in a position analogous to one who has repeatedly shoplifted from a particular store, so the judge prohibits him from entering it again, saving the store's security guards from the burden of having to follow him around whenever he is there."[85]

3. Uses of the CFAA Against Former Insiders

A more common scenario in which a trade secret owner may attempt to invoke the CFAA involves actions by former "insiders," such as when an employee, while authorized to access the company's network for purposes of her work, decides to accept another job and, before departing, copies, transmits or destroys important confidential electronic information to better compete with the former employer in her new job. A new *employer* is potentially liable for violating the CFAA if it directs the employee to access and transmit or destroy electronic data from the computer of another employer, since the new employer was never authorized to use the computer.[86]

---

79 *Id.*

80 *Id.* at 938.

81 *Id.* at 932–33.

82 *Id.* at 933.

83 *Id.* at 935–37 (emphasis added).

84 *Id.* at 937.

85 *Id.* at 937–38.

86 *See, e.g.*, Contract Assocs. Office Interiors, Inc. v. Ruiter, No. CIV. S-07-0334, 2008 WL 2225702, at *2 (E.D. Cal. May 29, 2008) (denying new employer's motion for summary judgment against prior employer's CFAA claim against it in light of genuine issues of material fact as to whether "[new employer] was aware that its new [employee]—fresh from the employ of a competing company that had worked on similar . . . projects—had immediately arrived with considerable outside work product substantiating several lucrative . . . projects,"

The courts have differed, however, in their conclusion of whether the *employee* is also liable under the CFAA. The dispute centers on whether the CFAA applies to an employee who at some point had been authorized by the original employer to access the computer. In *Modis, Inc. v. Bardelli*,[87] the District Court of Connecticut noted the differing views of courts on what constitutes unauthorized access:

> At present, courts are split as to what circumstances give rise to access without authorization or access that exceeds authorization. Some courts . . . have ruled that an accesser who has obtained and used proprietary information in violation of a duty of loyalty violates [the] CFAA.
>
> . . . [Others] confine: (1) a CFAA violation for accessing without authorization to instances involving an outsider or user who does not have permission to access the computer; and (2) a CFAA violation for access in excess of authorization to instances involving a user whose authorization is limited to certain information.[88]

A number of courts have held that the employee's authorization to access information ceases or is "exceeded" when the employee uses her lawful access to engage in conduct intended to benefit a new employer. For example, in *International Airport Centers, L.L.C. v. Citrin*,[89] the Seventh Circuit held that the employee's authorization to access his company-owned laptop terminated the instant "he resolved to destroy files that incriminated himself and other files that were also the property of his employer."[90] Similarly, in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*,[91] the court concluded that once the employee acted on interests adverse to those of his employer by disseminating

---

thus triggering a duty to disaffirm employee's acts or be held liable for violating the CFAA under agency principles); Binary Semantics Ltd. v. Minitab, Inc., No. 4:07-CV-1750, 2008 WL 763575, at *5 (M.D. Pa. Mar. 20, 2008) (concluding that the "[new employer] may be held liable for the CFAA violation" because the complaint sufficiently alleged that the "[employee] was acting at the direction of [the new employer] when she allegedly accessed plaintiff's protected computer and stole plaintiff's trade secrets"); *cf.* Role Models Am., Inc. v. Jones, 305 F. Supp. 2d 564, 567–68 (D. Md. 2004) (holding that simply receiving an unsolicited e-mail from an individual employed by a competitor does not by itself subject the e-mail recipient to liability under the CFAA action unless recipient exerted some control).

87 531 F. Supp. 2d 314 (D. Conn. 2008).

88 *Id.* at 319 (citations omitted).

89 440 F.3d 418 (7th Cir. 2006).

90 *Id.* at 420.

91 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

trade secret information via e-mail, he acted "without authorization" and could therefore be held liable under the CFAA.[92]

In *Lockheed Martin Corp. v. Speed*,[93] however, a Florida federal district court declined to construe "with authorization" as transient permission that the employee lost upon switching allegiance to a new master.[94] Instead, and in explicit disagreement with *Citrin* and *Shurgard*,[95] the court held that, because the defendants were authorized by the plaintiff-company "to access the precise information at issue," they could not be found liable under the CFAA.[96] Thus, the court granted the defendant's motion to dismiss because the "access was neither 'without authorization' nor 'exceeding authorization' as those terms are contemplated by the [CFAA]."[97] Additionally, the court concluded that ambiguous terms of the CFAA must be narrowly construed in view of the rule of lenity, because the Act was originally conceived as a criminal statute.[98]

The narrower view as set forth in *Lockheed* has increasingly been adopted by other courts as being "better reasoned" on the theory that the CFAA was enacted as an anti-hacker statute to prevent only "the unauthorized pro-

---

92 *Id.* at 1125; *see* Mintel Int'l Group, Ltd. v. Neergheen, No. 08 c 3939, 2008 WL 5246682, at *2–3 (N.D. Ill. Dec. 16, 2008) (finding probable success on merits of CFAA claim where employee e-mailed confidential company documents including customer lists to his personal e-mail account and used computer to print out confidential company documents for personal use); *see also* Sam's Wines & Liquors, Inc. v. Hartig, No. 08 C 570, 2008 WL 4394962, *3 (N.D. Ill. Sept. 24, 2008) (finding on motion to dismiss that plaintiff properly pled that employee who accessed company computer for purpose of downloading documents to send to future employee had exceeded authorized access under the CFAA, but further holding that complaint did not satisfy damages requirements under the CFAA as document was only copied, not altered or otherwise impaired); Int'l Sec. Mgmt. Group, Inc. v. Sawyer, No. 3:06CV0456, 2006 WL 1638537, at *20–21 (M.D. Tenn. June 6, 2006) (holding that the plaintiff "established a likelihood of success" on a claim that the defendants had violated the CFAA when the defendant-employee emailed confidential documents to another company); Nilfisk-Advance, Inc. v. Mitchell, No. 05-5179, 2006 U.S. Dist. LEXIS 21993, at *7–8 (W.D. Ark. Mar. 28, 2006) (denying motion to dismiss CFAA claims where employee was alleged to have exceeded authorization by e-mailing confidential files to home computer).

93 81 U.S.P.Q.2d (BNA) 1669 (M.D. Fla. 2006).

94 *Id.* at 1674.

95 *Id.* at 1673–74 ("To the extent *Citrin*[, following *Shurgard*,] holds that an employee accesses 'without authorization' at the moment the employee acquires a subjectively adverse interest to the employer, the Court respectfully disagrees.").

96 *Id.* at 1672, 1676.

97 *Id.* at 1676.

98 *Id.*; *see* Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 966–67 (D. Ariz. 2008) ("[P]rinciples of statutory construction persuade the Court to adopt a narrower view of the CFAA.").

curement or alteration of information, not its misuse or misappropriation" and that its prohibitions should therefore not be read broadly.[99]

Accordingly, a trade secret owner considering using the CFAA where the misappropriation has involved the use of a computer to which the owner had granted the potential defendant some access must carefully review the current case law in the relevant jurisdictions to see whether it is entitled to assert such a claim.

4. Contracting to Secure the Benefits of the CFAA

In view of the *Lockheed* line of cases, *Hewlett-Packard Co. v. Byd:Sign, Inc.*[100] provides guidance as to how an employer can draft contracts with its employees to maximize the chance that the CFAA will be held to apply to any pre-resignation access or transmission of trade secrets for the benefit of a future employer.[101] There, Hewlett-Packard ("HP") alleged the individual defendants, now former employees, had "conspired to use their positions of trust and confidence at HP to obtain trade secrets and other proprietary information from HP and then illegally funneled those secrets and HP's corporate opportunities to an enterprise founded by several of the [defendants]."[102] All of the former em-

---

99 *See Shamrock*, 535 F. Supp. 2d at 965–67 (quoting Brett Senior & Assocs. v. Fitzgerald, No. 06-1412, 2007 WL 2043377, at *3 (E.D. Pa. July 13, 2007)); Condux Int'l, Inc. v. Haugum, No. 08-4824, 2008 WL 5244818, at *5–6 (D. Minn. Dec. 15, 2008); *see also* Bridal Expo, Inc. v. Van Florestein, No. 4:08-cv-03777, 2009 WL 255862, at *10–11 (S.D. Tex. Feb. 3, 2009); Andritz, Inc. v. S. Maint. Contractor, LLC, No. 3:08-CV-44, 2009 WL 48187, at *3 (M.D. Ga. Jan. 7, 2009); Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929, 935 (W.D. Tenn. 2008); Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1342–43 (N.D. Ga. 2007) (stating that the view in *Lockheed* is better reasoned than in *Citrin* and *Shurgard*); B & B Microscopes v. Armogida, 532 F. Supp. 2d 744, 758 (W.D. Pa. 2007) (same); *cf.* Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 483, 500 (D. Md. 2005) (holding no violation of the CFAA where a union official used authorized access to visit a secure website and view membership information, which the official then used for the benefit of a competing union despite having signed an agreement "stipulating 'not to use the information . . . for any purpose . . . contrary to the policies'" of the union). The *Werner-Masuda* court concluded that "the gravamen . . . is not so much that [she] improperly accessed the information . . . but rather what she did with the information once she obtained it. The . . . CFAA, however [does] not prohibit the unauthorized disclosure or use of information, but rather unauthorized access." 390 F. Supp. 2d at 499.

The approach followed by the cases in this footnote has been criticized by some commentators as overly narrow. *See, e.g.*, 1 RAYMOND T. NIMMER & HOLLY K. TOWLE, THE LAW OF ELECTRONIC COMMERCIAL TRANSACTIONS ¶ 3.05[2] (rev. ed. 2008).

100 No. 6:05-CV-456, 2007 WL 275476 (E.D. Tex. Jan. 25, 2007).

101 *Id.* at *11–13.

102 *Id.* at *1.

ployees had signed agreements not to disclose any of HP's "intellectual property, trade secrets, technical secrets, or confidential information to unauthorized persons"[103] and to "*refrain from sending or accessing messages on HP's computer systems for personal gain*."[104] Relying on *Lockheed*, the individual defendants challenged whether HP had stated a claim under the CFAA, arguing that HP "failed to allege that the [d]efendants had accessed HP computers . . . 'without authorization.'"[105] The court disagreed. It distinguished *Lockheed* on the basis that, unlike the Lockheed employees, the HP employees had expressly agreed that they were not authorized to send or access messages using their employer's computers for personal gain.[106] Accordingly, the court denied the motion to dismiss HP's claims that the employees had accessed the computer system without authorization.[107]

Hewlett-Packard suggests a relatively costless way for employers to bring many acts involving use of company computers to misappropriate trade secrets under the protections of the CFAA: include language similar to that used by HP in their confidentiality contracts. Doing so not only contractually revokes the employee's authorization to access the computer once his or her purpose in doing so is for personal gain, but also arms the employer with both a breach of contract and a statutory claim against the disloyal employee for access other than as agreed. Employers may want to consider going further than HP did by defining "personal gain" to include both "personal economic and non-economic purposes." Additionally, in light of the continuing debate over the meaning of "authorization" under the CFAA, the employer may want to consider including express language in the NDA or employment agreement drawn from Section 112 of the Restatement (Second) of Agency to limit the employee's authorization to use the computer system, rather than simply expecting the court to conclude that authorization to access the computer terminates once the agent's interests diverge from the principal's.[108] *Hewlett-Packard* ultimately informs employers that employee agreements can play a vital role in the war to maintain the integrity of confidential company information.

---

103 *Id.* at *12 (internal quotation marks omitted).

104 *Id.* at *13 (emphasis added).

105 *Id.* at *11.

106 *Id.* at *13.

107 *Id.*

108 RESTATEMENT (SECOND) OF AGENCY § 112 (1958) ("Unless otherwise agreed, the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal.").

The CFAA, of course, applies not just when new employees join a company, but also when the company's own employees leave to work elsewhere. Accordingly, a prudent employer should also seek acknowledgments from new hires that they have not transmitted or transferred confidential information belonging to third parties to the company or to its computer system. Such an acknowledgement warns the new employees of the new company's expectations and will help shield the hiring company against potential liability under the CFAA arising out of the new hires' conduct which it has disapproved and of which it is not aware.

5. Further Points to Note in Asserting CFAA Claims

A CFAA claim is not a substitute for a breach of contract or misappropriation claim. Parties seeking a remedy under the Act must comply with the pleading requirements under the specific provisions of the Act claimed to have been violated or risk dismissal. Courts have held that a party asserting certain CFAA claims must establish both *damage* to a protected computer and *loss from that damage* "aggregating at least $5,000 in value."[109] It should be noted that the CFAA has recently been amended to eliminate the loss requirement for certain provisions of the Act,[110] so determining which section of the Act is claimed to have been violated becomes even more critical than in the past.

"Damage," as defined in the CFAA, means "any impairment to the integrity or availability of data, a program, a system, or information"[111] and has been held to cover the deletion, overwriting or destruction of computer files.[112] Notably, however, the mere accessing of files or the use of computers to send e-mails in furtherance of the alleged misappropriation generally does not constitute

---

109 18 U.S.C. § 1030(c)(4)(A)(i)(I) (2006); Garrelli Wong & Assocs. v. Nichols, 551 F. Supp. 2d 704, 708 (N.D. Ill. 2008) ("A thorough reading of the [CFAA] shows that it is necessary for a plaintiff to plead *both damage and loss* in order to properly allege a civil CFAA violation." (emphasis added)). *Contra* 18 U.S.C. § 1030(g) ("Any person who suffers *damage or loss* by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." (emphasis added)).

110 Effective September 26, 2008, 18 U.S.C. § 1030 was amended by the Identity Theft Enforcement and Restitution Act, Pub. L. No. 110-326, 122 Stat. 3560 (2008). Among other things, the law eliminated the requirement in 18 U.S.C. § 1030(a)(5) that the defendant's action must result in a loss exceeding $5,000. *Id.*

111 18 U.S.C. § 1030(e)(8).

112 *See, e.g.*, Patrick Patterson Custom Homes, Inc. v. Bach, 586 F. Supp. 2d 1026, 1035 (N.D. Ill. 2008).

"damage" as contemplated by the CFAA.[113] Trade secret owners who assert claims under the CFAA should be aware that "loss" includes "the costs of responding to the offense" but does not include damages from the *misuse* of the information that was improperly accessed or transmitted.[114]

One tactical consideration that may lead trade secret owners to consider asserting a CFAA claim as well as a state law claim for trade secret misappropriation is that the CFAA affords a basis for filing in federal court under federal question jurisdiction.[115] In a given dispute, this possibility may be advantageous for a variety of reasons. Plaintiffs should not assume, however, that filing a federal claim will necessarily make the case proceed swiftly or lead to litigation of all claims relating to the events surrounding the misappropriation in one forum.

First, as discussed above, there is significant variation among the federal courts on the question of whether the CFAA has been violated when a person who is at some point authorized to access a computer, such as an employee, uses that computer to transfer trade secrets.[116] In jurisdictions holding that such conduct does not constitute "unauthorized access" or "exceeding authorized access," the statute does not apply and there will be no basis for federal question jurisdiction. The same is true if a plaintiff cannot establish the requisite "damage" under the Act.[117] As one federal court explained in dismissing a CFAA claim:

> What this complaint boils down to are allegations of breach of employment covenants and the usual torts that attend such employment disputes. Such

---

113 *See, e.g.*, Chas. S. Winner, Inc. v. Polistina, No. 06-4865, 2007 WL 1652292, at *2 (D.N.J. June 4, 2007). In dismissing plaintiff's CFAA claim, the court stated:

> It is important to note that with one exception, the only factual allegations in the complaint that concern the use or misuse of a computer are *allegations that the individual defendants sent internal and external e-mails to further the interests of their prospective employer and in a manner disloyal to their former employer*. Nowhere in the complaint is it alleged that the individual defendants damaged any computers, caused any other harm to computers, or exceeded their authorized access to files or other stored data.

Id. (emphasis added) (footnote omitted).

114 *See* Sam's Wine & Liquors, Inc. v. Hartig, No. 08 C 570, 2008 WL 4394962, at *3–4 (N.D. Ill. Sept. 24, 2008); *Garelli Wong & Assocs.*, 551 F. Supp. 2d at 710; *see also* sources cited *supra* note 74. *But see* Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1195 (E.D. Wash. 2003).

115 28 U.S.C. § 1331 (2006).

116 *Cf. supra* notes 89–91 and accompanying text.

117 *See Sam's Wine*, 2008 WL 4394962, at *2–3. *But see* Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1195 (E.D. Wash. 2003).

> disputes existed long before e-mails and the routine use of computers to communicate business information. Absent diversity jurisdiction, a case of this kind sounds in state statutory and common law and is heard in state court.[118]

Second, even if there is a cognizable claim under the CFAA, the court has supplemental jurisdiction only "over all other claims that are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution."[119] If the state law claims substantially predominate over the claim over which the federal court has original jurisdiction or raise novel or complex issues of state law, the federal court can decline to exercise supplemental jurisdiction.[120] When a trade secret owner asserts a CFAA claim along with a host of state law claims[121] or when the CFAA claim is asserted against some but not all defendants, a challenge to supplemental jurisdiction may be likely on the theory that "permitting litigation of all claims in the district court [is] . . . allowing a federal tail to wag what is in substance a state dog."[122] If supplemental jurisdiction is

---

118 *Polistina*, 2007 WL 1652292, at *2.

119 28 U.S.C. § 1367(a) (2006).

120 *Id.* §§ 1367(c)(1)–(3) ("The district courts may decline to exercise supplemental jurisdiction over a claim under subsection (a) if—(1) the claim raises a novel or complex issue of State law, (2) the claim substantially predominates over the claim or claims over which the district court has original jurisdiction, (3) the district court has dismissed all claims over which it has original jurisdiction . . . ."); s*ee* Andritz, Inc. v. S. Maint. Contractor, LLC, No. 3:08-cv-44, 2009 WL 48187, at *3 (M.D. Ga. Jan. 7, 2009) (dismissing CFAA claim for failure to properly allege damages caused by access of computer without authorization and refusing to exercise supplemental jurisdiction over state claims); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 968 (D. Ariz. 2008) (dismissing the state law claims for lack of subject matter jurisdiction because the court declined to exercise supplemental jurisdiction over the state law claims after dismissing the CFAA claims); Civic Ctr. Motors, Ltd. v. Mason St. Imp. Cars, Ltd., 387 F. Supp. 2d 378, 382 (S.D.N.Y. 2005) (dismissing CFAA claim for failure to allege compensable loss and therefore dismissing state law claims after refusing to exercise supplemental jurisdiction); *see also* Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d 667, 684 (E.D. Tex. 2001) (granting defendant's motion for summary judgment against plaintiff's CFAA claim and declining to exercise supplemental jurisdiction over plaintiff's state law claims); *cf.* Liebert Corp. v. Mazur, No. 05 C 2069, 2005 WL 1563202 (N.D. Ill. June 6, 2005) (remanding CFAA case to state court based on *Colorado River* abstention principles).

121 Examples of such claims include breach of contract, breach of fiduciary duty, breach of state computer laws, inevitable or threatened misappropriation, breach of fiduciary duty, tortious interference and breach of state computer laws.

122 Rocky Mountain Twist v. Brackey, No. CV07-119, 2008 WL 744149, at *6 (D. Mont. Mar. 13, 2008) (quoting Borough of West Mifflin v. Lancaster, 45 F.3d 780, 789 (3d Cir. 1995)).

declined, injunctive relief on the non-CFAA claims could be delayed.[123] If a plaintiff wishes to avoid this possible result, it can assert the CFAA claims in state court.

E. Other Statutes That Can Protect Digitized Secrets

Other state and federal statutes also help to prevent the misappropriation of digitized secrets. The Electronic Communications Privacy Act, for example, prohibits the intentional, unauthorized interception of e-mails *in transmission.*[124] The Stored Communications Act prohibits the intentional, unauthorized access of a wire or electronic communication while it is in electronic *storage.*[125] As wired communications technology evolves and becomes wireless, the applicability of specific statutes to a particular intrusion may also evolve. To prevent dismissal of claims on the basis that they were brought under the wrong statute, it will be essential to focus on the technical details of what was accessed—for example, stored data or data in the act of being transmitted, and how it was accessed. At least one court has held the Stored Communications Act to apply to the retrieval of stored voicemail,[126] although that conclusion depends on the nature of the voicemail system and whether it is integrated into a computer system. How the data was accessed will also prove to be crucially important.

Disputes involving both state law claims and claims arising under one of these two federal acts also pose the same supplemental jurisdictional issues addressed above regarding CFAA claims.[127]

A growing number of states have also passed legislation to protect against theft of trade secrets or against unauthorized access to, destruction or transmission of computerized data.[128] Some of these statutes provide private

---

123 *See, e.g.*, *id.* at *10–11 (denying injunctive relief on state law claims "assuming the [c]ourt declines supplemental jurisdiction over those claims").

124 18 U.S.C. §§ 3121–3127 (2006).

125 *Id.* §§ 2701(a)–(b). A useful discussion of the Stored Communications Act may be found in Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004). Note that in at least one case the Stored Communications Act has been held to prevent a trade secret owner from obtaining information from an Internet Service Provider regarding the contents of stored communications that pertained to alleged misappropriators of trade secrets. O'Grady v. Apple Computer, Inc., 44 Cal. Rptr. 3d 72, 84 (Cal. Ct. App. 2006).

126 United States v. Smith, 155 F.3d 1051, 1059 (9th Cir. 1998).

127 *See supra* notes 119–123 and accompanying text.

128 *See, e.g.*, CAL. PENAL CODE § 449c (2008) (prohibiting theft, taking and use of trade secrets without authorization); CONN. GEN. STAT. § 53-451(b) (1958) (prohibiting "[u]nauthorized use of a computer or computer network"); *id.* § 53a-251(e) (prohibiting "[m]isuse of comput-

rights of action and potentially afford trade secret owners additional remedies, such as attorney's fees.[129] Moreover, traditional tort claims, such as conversion, may apply to removal of digitized trade secrets if the claims depend on "extra elements" that are not pre-empted by the trade secret law, such as where the conversion claim alleges that the wrongful removal entirely deprived the trade secret owner of its right to use the secrets.[130]

F. Using Forensic Analysis to Detect and Demonstrate Misuse or Disclosure of Trade Secrets

Regardless of the legal basis for the claim, properly preserved forensic data can point to and help establish evidence of misappropriation.[131] When practical, it often makes sense for a company to electronically image the hard drive of company-owned computers used by departing employees who had access to key company secrets before placing the computer back into use. Where imaging seems prohibitively expensive, a second-best alternative may be to have a company IT professional copy and carefully review and inventory the computer's contents. The introduction of such forensic evidence in misappropriation actions is becoming more common as computer imaging becomes more routine, particularly if emergency relief is sought by the plaintiff.

---

er system information"); N.J. STAT. ANN. § 2A:38A-1 to -6 (2008) (New Jersey Computer Related Offense Act); N.Y. PENAL LAW § 156.30 (2008) (prohibiting "[u]nlawful duplication of computer related material"); S.C. CODE ANN. § 39-8-90 (1976) (Persons Guilty of Stealing Trade Secrets; Criminal Penalties); VA. CODE ANN. § 18.2-152.3 (2008) (Virginia Computer Crimes Act). For a listing of state computer statutes, see Nat'l Ass'n of Attorneys Gen., Computer Crime Statutes: Index by Crime, http://www.ncsl.org/programs/lis/CIP/compcrime-subs.htm (last visited Apr. 21, 2009).

129 *See* A & G Research, Inc. v. GC Metrics, Inc., No. 51016(U), slip op. at 19 (N.Y. Sup. Ct. May 21, 2008).

130 *See* Thyroff v. Nationwide Mut. Ins. Co., 864 N.E.2d 1272, 1278 (N.Y. 2007). Note that state statutes concerning conversion vary widely. Some claims for conversion are pre-empted by the Uniform Trade Secrets Act because they do not add an extra element beyond misappropriation of trade secrets. *See* MicroStrategy Inc. v. Bus. Objects, S.A., 429 F.3d 1344, 1363 (Fed. Cir. 2005).

131 *See* Universal Engraving, Inc. v. Duarte, 519 F. Supp. 2d 1140, 1155–56 (D. Kan. 2007) (granting employer's motion for preliminary injunction against former employee, because forensic evidence showed that someone accessed the employee's password-protected computer the Sunday night before the employee's resignation; that the employee had been to work on that Sunday and that the employee's passcard had not been used to enter the facility on a Sunday for an entire year prior to that Sunday; and that a flash drive was placed on the employee's computer and information was uploaded on it).

Computer forensic analysis can show, among other things, that information has been deleted, transferred or altered.[132] If damage to the computer or data within it is detected, the costs of investigating and remedying the loss may be recoverable under the CFAA, so careful records of such expenses should be maintained.[133]

Forensic examination can also provide circumstantial evidence of misappropriation or improper conduct.[134] Thus, for example, forensic review may establish how long an employee has been negotiating for a new job, when she accepted the job, whether she has recruited others to join her and whether the new job is likely to place company secrets at risk.

Sophisticated monitoring techniques and forensic analysis are not always essential in detecting misappropriation. In *United States v. Martin*,[135] for example, an e-mail detailing the contents of a package containing confidential information was inadvertently sent from one co-conspirator to her employer's

---

132 *See* United States v. Becht, 267 F.3d 767, 769 (8th Cir. 2001) ("[Computer forensic] analysis . . . revealed 'transfer logs,' records of files transferred to or from [defendant's] computer."); Mintel Int'l Group, Ltd. v. Neergheen, No. 08-CV-3939, 2008 WL 2782818, at *1 (N.D. Ill. July 16 , 2008) (forensic examination revealed that on employee's next to last day of work he had copied, printed and e-mailed to his personal account client lists, vendor lists and "strategic documents"); B & B Microscopes v. Armogida, 532 F. Supp. 2d 744, 753 (W.D. Pa. 2007) (examining defendant's employer-owned computer forensically "revealed that [defendant] had deleted or overwritten every file relating to the KPICS System . . . [and] deleted or overwritten many files/folders which did not relate to the KPICS System, but which pertained to other B & B business"); Andarko Petroleum Corp. v. Davis, No. H-06-2849, 2006 WL 3837518, at *6 (S.D. Tex. 2006) (forensic expert testified that defendant downloaded 7.21 gigabytes, equivalent to 1.5 million pages of raw text); Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268, 1294, 1299–1300, 1326 (S.D. Fla. 2003) (forensic expert testified that examination revealed, among other things, that the defendant had used the examined computer to penetrate plaintiff's intranet and transfer files), *aff'd in part and rev'd in part*, 138 F. App'x 297 (11th Cir. 2005) (unpublished table decision); Liebert Corp. v. Mazur, 827 N.E.2d 909, 918–19 (Ill. App. Ct. 2005) (forensic examination of former employee's hard drive revealed evidence that someone had downloaded files, zipped them to a single file and "more likely than not" burned the zipped file to a CD); LeJeune v. Coin Acceptors, Inc., 849 A.2d 451, 456, 466 (Md. 2004) (forensic expert contradicted defecting employee's claim that he inadvertently copied trade secrets to a CD along with personal files; forensic evidence also showed that information had been erased from examined computer in an effort to conceal downloads); *see also* Sharon Gaudin, *The Ultimate Insider: FBI Analyst Steals National Secrets*, INFORMATIONWEEK, May 10, 2007, http://www.informationweek.com/show/Article.jhtml?articleID=199500751 (describing an FBI intelligence analyst's theft of digitized secrets and the use of computer forensic work to build the criminal case against him).

133 18 U.S.C. §§ 1030(e), (g) (2006).

134 *See* cases cited *supra* note 132.

135 228 F.3d 1 (1st Cir. 2000).

global marketing manager rather than to her confederate, thereby alerting the employer that its trade secrets were being compromised.[136] This "slip" led to conviction of the confederate under the Economic Espionage Act.[137] Such "slips" should be taken seriously and investigated promptly.

Sometimes it may only be possible to piece together evidence of misappropriation after the trade secret owner obtains an order permitting the imaging of the computers that the suspected misappropriator has used outside of the company's premises. While such orders are by no means routinely granted, some courts that have focused on e-discovery issues have ordered the creation of an optical image of relevant hard drives—on a showing of reasonable cause to suspect misappropriation—to *preserve* evidence and directed *production* of particular information from that optical image at a later date.[138] If such an order is contemplated, it is critical to move quickly before key evidence is overwritten or destroyed. An example of information that may be requested from the forensically-preserved evidence might include "all copies of confidential and proprietary information[, as defined in the Order,] that [the individual] wrote, copied, printed or downloaded onto disks or recreated before [or after the individual] left [the company]."[139]

Parties subject to preservation orders must either successfully challenge the order, narrow the order or comply scrupulously; otherwise, they may face sanctions up to and including the striking of their pleadings.[140]

As the law progresses and new situations arise, trade secret owners have been required to become increasingly mindful of the risks associated with digitizing information. The courts have similarly evolved by taking into consideration the fact that employees sometimes e-mail company information to their homes simply to do their work, and may retain digital information on their home

---

136 *Id.* at 10.

137 *Id.* at 10, 19.

138 *See, e.g.*, Verigy US, Inc. v. Mayder, No. C07-04330, 2007 WL 2429652, at *1–4 (N.D. Cal. Aug. 24, 2007) (granting detailed preservation order based on preliminary showing of improper dissemination and retention of trade secrets).

139 *See, e.g.*, Jordana Mishory, *Lexis Noncompete Contracts Lead to Defection Duel in Federal Court*, LAW.COM, June 28, 2007, http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=900005555983 (last visited Apr. 25, 2009).

140 *See, e.g.*, Ameriwood Indus., Inc. v. Liberman, No. 4:06CV524, 2007 WL 5110313, at *1 (E.D. Mo. July 3, 2007) ("Because defendants' intentional actions evidence a serious disregard for the judicial process and prejudice plaintiff, the Court will grant plaintiff's motions for sanctions, *enter default judgment in favor of plaintiff*, and shift to defendants plaintiff's costs, attorney's fees, and computer expert's fees relating to the motions for sanctions and the forensic imaging and recovery of defendants' hard drives." (emphasis added)).

computers after resignation through inadvertence rather than malice. In the early days of forensic examination of computers, a showing that an ex-employee had transferred company trade secrets to a home computer might, without more, have led to at least a temporary injunction forbidding the use or disclosure of the secrets and to an inference that misappropriation was intended. Today, however, courts are more likely to require further evidence addressing, for example, what specific trade secrets were transferred and why the transfer appears to have been out of the ordinary before granting injunctive relief. Detailed forensic examination can often provide such evidence—or refute it.[141]

Finally, trade secret owners should use online resources to keep an eye on whether their own secrets have made their way onto the Internet or whether competitors' websites or announcements have placed trade secrets at risk.[142] Companies should conduct periodic searches to see what is being said about the company in chat rooms and on financial, social networking or other websites throughout the Internet or sign up for monitoring services such as eWatch, CyberCheck and Cyveillance. These online resources reveal what is being reported or discussed about companies or their competitors.

In evaluating postings, the trade secret owner should be careful, however, to distinguish between constitutionally protected exchanges of opinion and unlawful public disclosures of confidential information. The fact that some

---

[141] There are many cases where copying of computer data alone did not lead to a finding of misappropriation. *See* Kelly Servs., Inc. v. Greene, 535 F. Supp. 2d 180, 186 & n.8 (D. Me. 2008) (finding that the fact that defendant transferred files to a USB drive prior to resignation did not establish misappropriation in face of sworn statements that she did not retain protected information and in absence of proof that she had used any of the information); Spinal Dimensions, Inc. v. Chepenuk, No. 51533(U), slip op. at 5 & n.1 (N.Y. Sup. Ct. Aug. 9, 2007) (finding defendant's actions in emailing employer's documents to a personal email account not sufficient to establish a likelihood of success on a claim of "actual misappropriation"); *see also* Quaker Chem. Corp. v. Varga, 509 F. Supp. 2d 469, 474, 483 (E.D. Pa. 2007) (concluding that defendant's possible possession of plaintiff's confidential information was "basically irrelevant" in view of the following: a forensic expert discovered that defendant had copied 4,496 files from his work computer to a USB storage device and failed to disclose that fact to plaintiff; defendant deleted all files from the storage device after the lawsuit was filed and said he had "a lapse of judgment, but that he no longer possesses any of [plaintiff's] confidential information nor intends to disclose any of [plaintiff's] information to [his new employer]"; the court nonetheless granted an injunction enforcing a non-compete agreement on other grounds and noted that whether defendant was liable for violating the CFAA was an issue for a later day).

[142] A review of competitors' websites can provide a variety of useful evidence in a trade secrets suit. *See, e.g.*, NewInno, Inc. v. Peregrim Dev., Inc., No. CV010390074S, 2002 WL 31875450, at *2–3 (Conn. Super. Ct. Dec 3, 2002) (website clearly revealed former employees' methods of unfair competition).

employees think their supervisor is a "jerk" is hardly a trade secret.[143] Concern that companies could use lawsuits ostensibly directed to securing trade secrets to stifle off-hour complaints has led many courts to be particularly wary of actions filed to remove Internet posts—even when actual trade secrets are placed at risk.

Periodic Internet searches can provide early warning that true trade secrets have been compromised, either inadvertently (by the company or third parties) or maliciously. The earlier the trade secret owner detects such postings, the greater the potential for getting the secret removed.

II. TRADE SECRETS ON THE INTERNET: SUDDEN DEATH?

Sometimes trade secret owners, or the authorized recipients of a secret, post secrets on the Internet in error. Trade secret owners should detect and correct such errors as early as possible. They should also contact leading search engines to provide notice of the posting, seek removal of the secret and seek assistance in removing the secrets from online search caches as well.[144] While the trade secret owner may never be completely certain that the trade secret has not been widely accessed, demanding its removal from the Internet should reduce the risk of further access and dissemination and assist in rebutting a claim that the trade secret owner did not follow reasonable precautions to protect secrets.

Sometimes, however, the posting of a trade secret is no accident. Some communities regard posting trade secrets on the Internet as a sport. There are numerous examples of damaging information that has made its way onto the Internet, including the DVD Copy Control Association's algorithm for copy-protecting DVDs,[145] early versions of upcoming movies,[146] portions of the Mi-

---

143 *See, e.g.*, Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 249 (Cal. Ct. App. 2008) (noting that online comments regarding company executives were "unquestionably vulgar and insulting, but nothing in this post suggested that the author was imparting knowledge of actual facts to the reader"; finding plaintiff had not stated libel claim and thus was not entitled to learn identity of anonymous poster).

144 A useful guide to working with major search engines and ISPs to delete improper postings can be found at Rutgers University, Office of Information Technologies, Removing Information From Search Engines: Information Protection and Security, http://rusecure.rutgers.edu/content/removing-information-search-engines (last visited Apr. 21, 2009).

145 DVD Copy Control Ass'n v. McLaughlin, No. CV 786804, 2000 WL 48512, at *1 (Cal. Super. Ct. Jan. 21, 2000).

146 Alan Durke, *'X-Men Origins: Wolverine' Leaked to Web*, CNN.com, Apr. 3, 2009, http://cnn.com/2009/SHOWBIZ/Movies/04/02/xmen.piracy (last visited Apr. 25, 2009).

crosoft and Cisco source codes,[147] Apple Computer and Ford Motor Company's product plans,[148] and the business, acquisition and new product plans of a whole host of companies. Such postings have sparked protracted, hard-fought litigation going to the heart of trade secret law and have raised a host of constitutional issues.

Though courts are increasingly taking the view that posting a trade secret on the Internet does not necessarily destroy the information's status as a trade secret *if* it is removed before a significant portion of the relevant public has had the opportunity to access it, those who post trade secrets online often widely publicize the secrets' availability *for the very purpose* of spreading them. When the code for overwriting copyright protection on Blu-ray and high-definition DVDs showed up on the Internet and a trade group sent cease-and-desist letters requesting the code to be pulled down, for example, scores of individuals, angry that the protection code had been developed in the first place, worked quickly to spread the overwrite code more widely in the name of "public service."[149] Some wrote songs incorporating the code and posted them on YouTube; some printed the code on t-shirts;[150] and at least one person got a tattoo of the code.[151] The vision feared by one of the early judges confronting the posting of the DVD decryption code—of a world where misappropriators of trade secrets "post the fruits of their wrongdoings on the Internet as quickly as possible and as widely as possible thereby destroying a trade secret forever"[152]—seems to have come to pass.

But the law has not left trade secret owners, who can establish that bona fide trade secrets are at risk, without relief. There are meaningful remedies

---

147 United States v. Genovese, 409 F. Supp. 2d 253, 257–58 (S.D.N.Y. 2005); Robert Lemos, *Cisco Investigates Source Code Leak*, CNET NEWS BLOG, May 17, 2004, http://news.cnet.com/Cisco-investigates-source-code-leak/2100-7349_3-5213724.html?tag=mncol (last visited Apr. 25, 2009).

148 O'Grady v. Superior Court, 139 Cal. App. 4th, 1423, 1432 (Cal. App. Ct. 2006) (Apple's "secret plans to release a device that would facilitate the creation of digital live sound recordings on Apple computers" were released on the Internet); Ford Motor Co. v. Lane, 67 F. Supp. 2d 745, 746–47 (E.D. Mich. 1999) (photos of upcoming Ford products leaked onto the Internet).

149 Brad Stone, *In Web Uproar, Antipiracy Code Spreads Wildly*, N.Y. TIMES, May 3, 2007, at A1, *available at* http://www.nytimes.com/2007/05/03/technology/03code.html?_r=1.

150 *Id.*

151 *Takedown This!*, BMENEWS, May 3, 2007, http://news.bmezine.com/2007/05/03/takedown-this (last visited Apr. 24, 2009).

152 DVD Copy Control Ass'n v. McLaughlin, No. CV 786804, 2000 WL 48512, at *3 (Cal. Super. Ct. Jan. 21, 2000) (the trial court decision in what came to be the *Bunner* case).

ranging from interim injunctive relief to damages to remediation/disgorgement to, in some cases, criminal penalties.

A. Posting Does Not Necessarily Destroy Information's Status as a Trade Secret

Much of the most contentious litigation over the posting of trade secrets on the Internet has focused on postings made by those who do not own the secret and claim that the public has a right to know it. Unauthorized posters' primary defenses have focused on "free speech" considerations[153] and on the claim that, once the secret has been posted, others are free to further publicize it since its secrecy has been destroyed.

Both arguments were considered at length during the protracted and widely followed California *Bunner* litigation over the DVD encryption/decryption code. That closely-watched litigation resulted in two key rulings by the California Supreme Court. First, an injunction requiring trade secrets to be removed from the Internet does not necessarily violate the First Amendment and may be necessary to protect a Fifth Amendment property right.[154] In *HiRel Connectors Inc. v. United States*,[155] a California federal district court reached the same legal conclusion—that injunctive relief to remove the secret from the Internet *could* be warranted if the information has not yet become generally known to the relevant public.[156]

Second, if injunctive relief is sought only *after* a trade secret posted online has become generally known to the relevant public—and thus is no longer a trade secret—an injunction serves no legitimate purpose and does violate the First Amendment.[157] Ultimately on remand, the California Court of Appeal

---

153 The "news reporter's privilege" has taken on a new stripe as bloggers have asserted it as a defense to protect the identities of those who have given them trade. *See* discussion *infra* Part II.B.6.

154 DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 192–93 (Cal. Ct. App. 2004). For a detailed discussion of the *Bunner* decisions, see Victoria Cundiff, *Trade Secrets on the Internet: The Latest Installments*, *in* PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES 801 (Practising Law Inst. 2004); Victoria Cundiff, *Hot Topics in Trade Secrets Law: Keeping Your Intellectual Property Off the Internet: Two Approaches*, *in* PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES 716 (Practising Law Inst. 2002).

155 No. CV01-11069, 2006 WL 3618011 (C.D. Cal. Jan. 25, 2006).

156 *Id.* at *10–11.

157 *Bunner*, 10 Cal. Rptr. 3d at 192–93. For thoughtful discussions of the First Amendment issues relating to removing online postings of trade secrets, see Elizabeth A. Rowe, *Saving Trade Secret Disclosures on the Internet Through Sequential Preservation*, 42 WAKE FOREST

concluded in *Bunner* that by the time Bunner posted the decryption code, it had already become generally known to the relevant public, because it had been widely posted throughout the Internet in print publications and even appeared on t-shirts distributed outside the courthouse.[158] Accordingly, injunctive relief was not necessary to prevent irreparable harm; the harm had already occurred. The federal district court reached the same factual conclusion in *HiRel Connectors*, since by the time relief was sought, the trade secret information had already been viewed on the Internet by members of the relevant industry for several years and was therefore no longer a "secret."[159]

By contrast, in *Silicon Image* the court found that the online posting of a trade secret by a third party had not destroyed the trade secret.[160] There, a trade secret owner commenced a misappropriation suit against a defendant for "conventional," offline misappropriation.[161] During the course of the litigation, defendant conducted an online investigation which revealed that a third party had posted portions of the plaintiff's source code on the Internet.[162] Defendant had not obtained the secret from that third-party site and the plaintiff had not previously been aware of it.[163] Defendant urged, however, that simply because the posting had occurred, the information had become generally known and defendant was therefore free to use it. The court rejected this argument because "there [wa]s a serious question as to whether the information that was published on [the Chinese] website actually revealed enough information . . . to be useful to competitors" and had apparently not been seen or used by any other competitor, including the defendant.[164] The court concluded that the information had not become "generally known to the relevant people" and had not, by reason of that posting, lost its status as a protectable trade secret by reason of the posting.[165] The fact that defendant had offered a significant "bounty" to gain information

---

L. REV. 1, 24–25 (2007). *See generally* Pamela Samuelson, *Principles For Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777 (2007).

158 *Bunner*, 10 Cal. Rptr. 3d at 192–93.

159 *HiRel*, 2006 WL 3618011, at *10.

160 Silicon Image, Inc. v. Analogix Semiconductor, No. C-07-00635, 2008 WL 166950, at *16 (N.D. Cal. Jan. 17, 2008).

161 *Id.*

162 *Id.*

163 *Id.*

164 *Id.*

165 *Id.*

about the program reinforced this conclusion, since the defendant would have had no reason to offer the bounty if he had learned the secret on the Internet.[166]

Having overcome the challenge that part of its trade secret had been posted on the Internet, however, the trade secret owner in *Silicon Image* lost the case for a more low-tech reason: the plaintiff's non-disclosure agreements concerning many of the secrets had included a fixed time limit, which had expired, on the non-disclosure obligation.[167] The court found that the information had ceased to be a trade secret for that reason.[168]

While *Bunner* and other cases recognize that damages and even criminal remedies[169] may be available when trade secrets are posted on the Internet, they also make clear that to win preliminary or permanent injunctive relief, the trade secret owner must act quickly. Although some have argued for legislation providing for a reliable, expedited process for disabling access to a trade secret in the period between discovery of the information on the Internet and a final ruling by the court on whether the posting constitutes trade secret misappropriation,[170] there is no such statute currently in effect. Accordingly, the following approach is suggested by current case law.

B. Acting Promptly to Remove Trade Secrets From the Internet

1. Give Notice

A trade secret owner should be diligent in monitoring whether its secrets have been placed on the Internet. If a posting is detected and the trade secret owner does not act quickly, there may be no secret left for an injunction to protect. As the California Supreme Court stated in *Bunner*, injunctive relief is only appropriate where the posting is "sufficiently obscure or transient or otherwise limited so that it does not become generally known to relevant people, *i.e.*, potential competitors or other persons to whom the information would have some economic value."[171]

---

166 *Id.*

167 *Id.* at *15.

168 *Id.*

169 *See, e.g.*, United States v. Genovese, 409 F. Supp. 2d 253, 257–58 (S.D.N.Y. 2005) (imposing criminal penalties for posting portions of a "jacked" Microsoft computer program online as a *teaser* and offering to sell more of the code).

170 *See* Elizabeth A. Rowe, *Introducing a Takedown for Trade Secrets on the Internet*, 2007 WIS. L. REV. 1041, 1041–43 (2007) (suggesting adoption of procedures similar to those afforded to copyright owners under the Digital Millenium Copyright Act).

171 DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 192–93 (Cal. Ct. App. 2004).

Once it has detected an unauthorized posting, the trade secret owner must consider whether challenging the posting is, under the circumstances, likely to lead to further dissemination of the secret. If the trade secret owner wishes to try to preserve the secret, it should provide immediate notice to the poster (as identified in the posting) and to the operator of the website on which the posting appears demanding immediate removal. To prevent a *Bunner*-type situation from occurring in which individuals other than the website operator further publicize the information, the trade secret owner should also consider giving notice to the public that the information is not to be freely used or disclosed.[172] The benefit of providing notice of its rights must be carefully weighed, however, against the risk of drawing greater public attention to the posting.[173]

While the trade secret owner will naturally want to know exactly *who* is behind a particular posting or site, it is more important from a legal standpoint to provide immediate notice of the problem to the misappropriator and the website, *whoever* they may be, even if that notice must be provided to an alias name. Lookup sites like *register.com* or *whois.com* permit the trade secret owner to give notice to the legally designated contact for the website and permit the trade

---

[172] Examples of such communications include those made by Microsoft when portions of its secret source code appeared online. *See, e.g.*, Robert Lemos, *Microsoft Cracks Down on Source Code Traders*, CNET NEWS, Feb. 18, 2004, http://news.cnet.com/Microsoft-cracks-down-on-source-code-traders/2100-7355-3-5161205.html?tag=mncol (last visited Apr. 26, 2009) (reporting that Microsoft placed alerts on several peer-to-peer file-sharing networks where it believed unlawful file sharing of certain portions of its code had taken place). Microsoft's warnings appeared when "a user searche[d] the network using certain keywords related to the source code." *Id.* Microsoft also released a statement that "stressed that the source code files are both copyrighted and protected as a trade secret" and "'[a]s such, it is illegal to post it, make it available to others, download it or use it'" and that "'Microsoft will take all appropriate legal actions to protect its intellectual property.'" *Id.*

Facebook reacted in a similar manner when portions of its source code appeared online. Nik Cubrilevic, *Facebook Source Code Leaked,* TECH CRUNCH, Aug. 11, 2007, http://www.techcrunch.com/2007/08/11/facebook-source-code-leaked (last visited Apr. 26, 2009). A Facebook executive posted a comment stating:

> "A small fraction of the code that displays Facebook web pages was exposed to a small number of users due to a single misconfigured web server that was fixed immediately. It was not a security breach and did not compromise user data in any way. Because the code that was released only powers the Facebook user interface, it offers no useful insight into the inner workings of Facebook. The reprinting of this code violates several laws and we ask that people not distribute it further."

Id.

[173] *See, e.g.*, Ian Fried, *Apple Suit Calls Attention to iBook Rumor*, CNET NEWS, Aug. 3, 2000, http://www.news.cnet.com/ (search "apple suit calls attention") (last visited Apr. 23, 2009).

secret owner to argue that, at least as of the notice date, the website operator and poster had "reason to know" that it was not authorized to display the secret—a critical element in establishing third-party liability for misappropriation.[174] The website registration should also help the trade secret owner establish at least one of the locations in which the website operator can be sued, because the register indicates a physical location for the administrator and technical contact for the site.

2. Make the Case

If the protest letter does not lead to an immediate takedown, the trade secret owner should consider seeking an injunction ordering its removal. The trade secret owner will need to establish a prima facie case of misappropriation to secure relief,[175] namely, first, that it has taken reasonable measures to maintain secrecy. The emerging case law as articulated in *Bunner* and *HiRel* suggests that the owner must also prove the following two elements: (1) the specific information that has been posted must itself be a trade secret (not simply that a larger document of which it is a part is a trade secret)[176] and (2) the information must not yet have been viewed by any material portion of the relevant public.[177]

3. What To Ask For in Discovery

While a diligent trade secret owner should be readily able to establish the first and second elements, it may need to conduct discovery to establish whether the public has viewed the posted secret. If the secret has been posted only briefly, it may be fair to ask the court to presume that the secret has not

---

174 Uniform Trade Secrets Act § 1(2) (1985).

175 *See, e.g.*, Immunomedics, Inc. v. Jean Doe, 775 A.2d 773, 776–78 (N.J. Super. Ct. App. Div. 2001) (affirming order permitting issuance of subpoena to determine identity of poster of trade secret on Internet only because Immunomedics had first offered sufficient evidence that defendant was likely its employee bound by a confidentiality agreement). Again, note the importance, at least in the Internet sphere, of disclosing trade secrets only under contractual obligations. That policy enables the trade secret owner to present evidence that anyone who knew the secret either is bound by contractual obligations of secrecy or acquired it through misappropriation.

176 If a partial posting is not itself a trade secret but simply suggests that the poster possesses the complete secret, the trade secret owner may face the task of establishing the "threatened" disclosure of trade secrets. Uniform Trade Secrets Act § 2(a) (1985).

177 *See supra* notes 157–159 and accompanying text.

been accessed by any material portion of the relevant public. The same is true if the site offers to sell secret information beyond what appears on the site.[178]

If the secret has been posted for some time or if there is a question as to whether a particular site is likely to have been accessed by relevant members of the public, however, the trade secret owner will likely want to conduct discovery. It can attempt to do so by filing a lawsuit against the poster, setting out a prima facie case of misappropriation and then seeking expedited discovery from the website and the Internet Service Provider ("ISP") directed solely to the issues of the extent to which the site has been accessed.

Specifically, the plaintiff will want to obtain copies of the website's server log and administrative data. This information will reveal the number of site views and page views, can help identify the existence of links or mirror sites (such information should also be specifically requested) and may reveal the internet protocol addresses of the visitors to the relevant page. This information may help the trade secret owner persuasively establish that the secret has not yet become generally known and that a court order is necessary to protect the secret from destruction.

4. Scope of the Order

If the trade secret owner is able to establish the need for immediate relief, it will want the order to provide:

- An order that the posting be removed.

- A method for serving the order, possibly including Internet-based means of service in addition to conventional means.[179] Typically the trade secret owner would want to serve the order on the owner of the original website and to any linked or mirrored pages.

- Notice to the relevant search engines to delete the pages containing the trade secret from their cache files immediately (rather than at the date

---

178 *See, e.g.*, United States v. Genovese, 409 F. Supp. 2d 253, 254 (S.D.N.Y. 2005).

179 For discussion of considerations permitting orders authorizing service via e-mail, see, for example, *Rio Props. v. Rio Int'l Interlink*, 284 F.3d 1007, 1017–19 (9th Cir. 2004) and *Bank Julius Baer & Co. Ltd. v. Wikileaks*, No. C 08-00824 JSW, 2008 WL 413737 , at *1–2(N.D. Cal. Feb. 13, 2008). *See also* Ronald J. Hedges, Kenneth N. Rashbaum & Adam C. Losey, *Virtual Jurisdiction: Does* International Shoe *Fit in the Age of the Internet?*, FIOS, Feb. 1, 2009, http://www.fiosinc.com/e-discovery-knowledge-center/electronic-discoveryarticle.aspx?id=507&2=1 (last visited Apr. 25, 2009).

the services regularly update their caches); to ensure cooperation, such an order may need to provide for payment of related remediation costs to the search engines.

- Notice on the website where the improper posting occurred stating that the posting was without authorization and that any use or disclosure of the information (described by subject matter and with reference to the dates it was on the Internet) after the date of the order is unauthorized except as provided in any further order. This notice should not itself further publicize the secret.

The trade secret owner may also want to seek provisions ordering an injunction against creating additional postings or links or other websites displaying the trade secret.

5. Identify the Poster?

If the secret is removed from the Internet, the trade secret owner may be satisfied. If the posting has in fact destroyed the secret, however, or if the trade secret owner wishes to prevent further misappropriation by the same individuals and the poster has not come forward to contest the injunction, the trade secret owner may wish to determine the poster's identity. Some ISPs advise users in their terms of use that they may provide information about the accounts in response to subpoenas, but that in a non-emergency context they will provide users with notice of and an opportunity to contest any civil subpoenas directed to providing identifying information about them.[180] Accordingly, a trade secret owner should be sure to check the specific terms of use to be sure what notice policies apply.

A trade secret owner cannot assume that the ISP will quickly identify the poster or that the court will readily order such relief. Courts are increasingly receptive to arguments that Internet users' rights may include a possibly rebuttable, but quite significant, right of anonymity.

---

[180] *See, e.g.*, AOL Legal Department, Civil Subpoena Policy, http://legal.web.aol.com/aol/aolpol/civilsubpoena.html (last visited Apr. 29, 2009) (stating that "it is AOL's policy to promptly notify the Member(s) whose information is sought" and that "AOL will not produce the subpoenaed Member identity information until 10 days after receipt of the subpoena, so that the Member whose information is sought will have adequate opportunity to move to quash the subpoena in court"); 2009 Comcast Customer Privacy Notice, http://www.comcast.com/customerprivacy (last visited Apr. 25, 2009) (stating that in the case of a subpoena from a non-governmental entity it will inform the customer of the subpoena).

A number of courts have followed tests initially developed in the Northern District of California in *Columbia Insurance Co. v. Seescandy.com*[181] for invading anonymity in the libel context.[182] This approach was recently discussed in detail by the California Court of Appeal in *Krinsky v. Doe 6*.[183] Under this approach the plaintiff must first make a prima facie showing of liability before the ISP can be required to disclose identifying information.[184] At that point, however, courts have held that the defendant should no longer be permitted to remain anonymous. The defendant "should not be afforded an advantageous position based on the media in which she chose to commit the breach of contract or because she committed that alleged breach anonymously."[185]

6. Bloggers' Sources

In *Apple Computer, Inc. v. Doe 1*,[186] the California Superior Court ruled that when a trade secret is posted on a "blog," a journalism privilege may apply to set the terms under which the blogger can be required to identify the source of trade secrets that the blogger has posted.[187] The dispute in that case arose when

---

181 185 F.R.D. 573 (N.D. Cal. 1999).

182 *See Immunomedics*, 775 A.2d at 778 (affirming order permitting issuance of subpoena to determine identity of poster of trade secret on Internet because Immunomedics first had offered sufficient evidence that defendant was likely its employee bound by a confidentiality agreement). There are many cases that discuss the standards for ordering disclosure of the identity of anonymous posters in the defamation context. *See* Rocker Mgmt. L.L.C. v. John Does 1 through 20, No. 03-MC-33, 2003 WL 22149380 (N.D. Cal. May 29, 2003); Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231 (Cal. Ct. App. 2008); *In re* Ottinger, No. 08-03892, 2008 WL 4375330, 3–4 (N.Y. Sup. Ct. June 27, 2008) (following Doe No. 1 v. Cahill, 884 A.2d 451 (Del. 2005) and Dendrite Int'l, Inc. v. Doe, No. 3, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001)) (holding that a plaintiff seeking the identity of a poster of allegedly defamatory remarks must undertake efforts to give the anonymous poster notice, identify the specific statement that constitutes actionable speech and establish and support a prima facie cause of action that the statement is defamatory (recognizing that a public figure plaintiff may not be able to establish malice without discovery), at which point the court then will "balance the defendant's First Amendment right of anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure of the anonymous defendant's identity to allow the plaintiff properly to proceed."). For further discussion, see generally Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 DUKE L.J. 855 (2000).

183 72 Cal. Rptr. 3d 231 (Cal. Ct. App. 2008).

184 *Id.* at 244–46.

185 *Immunomedics*, 775 A.2d at 778.

186 No. 1-04-CV-032178, 2005 WL 578641 (Cal. Super. Ct. Mar. 11, 2005), *vacated*, 139 Cal. App. 4th 1423 (Cal. App. Ct. 2006).

187 *Id.* at *8.

one of Apple's confidential product plans was posted on a blog.[188] After receiving a protest from Apple, the blogger removed the documents from his blog,[189] so injunctive relief to remove the postings was not an issue. Concerned, however, that the poster appeared to be an Apple insider who might well have continuing access to Apple's trade secrets, Apple served the blogger with a subpoena seeking the identity of the source.[190] The blogger objected on First Amendment grounds and invoked the California shield law, which controls the circumstances under which journalists can be compelled to reveal their sources.[191] That statute, however, does not provide journalists with an absolute immunity from disclosing their sources.[192]

The trial court was prepared to accept, *arguendo*, that the blogger was subject to the shield law.[193] While not every poster on the Internet is a blogger, the court noted that the very word "journalism" is derived from "journal"[194] and that an online journal maintained by a blogger might indeed constitute journalism for purposes of the shield law.[195] The trial court, however, also said that "[r]eporters and their sources do not have a license to violate criminal laws."[196] Equating the blogger who posts trade secrets with a "fence" of stolen tangible goods, the court found that there is no public interest served by "publishing private, proprietary product information that was ostensibly stolen and turned over to those with no business reason for getting it."[197] Accordingly, the trial court ordered the blogger to reveal the source.[198]

The Court of Appeal reversed,[199] holding that, under the California shield laws, before a journalist can be forced to reveal a source, the movant must show that it has no other practical means of obtaining the information.[200] The court found that although Apple had interviewed its employees about the

---

188 *Id.* at *1.

189 *Id.* at *5.

190 *Id.* at *1.

191 *Id.* at *2.

192 *Id.* at *6.

193 *Id.* at *5.

194 *Id.* at *5 n.6.

195 *Id.* at *7.

196 *Id.* at *5.

197 *Id.* at *8.

198 *Id.* at *1.

199 O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 115–16 (Cal. Ct. App. 2006).

200 *Id.* at 109.

leaked document, it had neither questioned them under oath[201] nor "fully exploited internal computer forensics."[202] Accordingly, the court quashed the subpoena requiring the blogger to identify the source.[203] The court also concluded that under the Stored Communications Act,[204] Apple could not compel an ISP to reveal stored communications in the blogger's account even in response to a subpoena.[205]

Journalists' privileges are governed by common law and state statutes,[206] and so it is unclear whether other courts will follow California's lead. What is clear, however, is that litigation to identify the source of trade secrets that make their way onto the Internet is likely to be time consuming, expensive and possibly futile.

7. To Sue or Not Sue

Litigating to remove trade secrets from the Internet can in theory be a viable remedy, as noted by the California Supreme Court in *Bunner*.[207] Under emerging legal rules, however, actually achieving relief may require the plaintiff to make factual showings regarding the scope of actual access, which can be extremely difficult to establish.[208]

Perhaps more important from a practical standpoint, bringing suit also can provoke a chatting frenzy on the Internet, lead to hostile commentary[209] or even trigger further online discussion or disclosure of the trade secrets. This phenomenon, which formed the basis for the final decision in *Bunner*,[210] has

---

201 *Id.*

202 *Id.* at 111.

203 *Id.* at 92.

204 18 U.S.C. §§ 2701–11 (2006).

205 *O'Grady*, 44 Cal. Rptr. 3d at 94.

206 FED. R. EVID. 501. Forty-nine states plus the District of Columbia have adopted some form of journalists' privilege, but they are not identical. *See* HENRY COHEN, CRS REPORT FOR CONGRESS, JOURNALISTS' PRIVILEGE TO WITHHOLD INFORMATION IN JUDICIAL AND OTHER PROCEEDINGS: STATE SHIELD STATUTES 2 (2005).

207 *See* DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 187–195 (Cal. Ct. App. 2004).

208 *See id.* ("[T]his court [must] determine whether the evidence . . . supports the factual findings necessary to establish that the preliminary injunction was warranted."); *see also supra* Parts II.B.2-3.

209 *See, e.g.*, Tom McNichol, *Think Belligerent*, WIRED, May 2005, http://www.wired.com/wired/archive/13.05/apple.html (last visited Apr. 25, 2009).

210 *See Bunner*, 10 Cal. Rptr. 3d at 195 (noting that once the trade secret is out, if the trade secret becomes generally known, there is nothing left to protect with a preliminary injunction).

been dubbed "The Streisand Effect," in recognition of the fact that after Barbra Streisand sued to remove an aerial photo of her house from an online collection of 12,000 California coastline photographs, copies of the photograph spread widely throughout the Internet.[211] Similarly, when the movie industry began undertaking efforts to delete the HD-DVD decryption key from the Internet, the code promptly spread to nearly 300,000 sites.[212] When "Wikileaks," a website that solicits and aggregates purportedly leaked governmental and business information, was shut down temporarily by a far-reaching injunction, a number of mirror sites and links sprang up immediately thereafter.[213] The court in that case found that its broad injunction

> had exactly the opposite effect as was intended. The private, stolen material was transmitted over the internet via mirror websites which are maintained in different countries all over the world. Further, the press generated by this Court's action increased public attention to the fact that such information was readily accessible online. The Court is not convinced that Plaintiffs have made an adequate showing that any restraining injunction in this case would serve its intended purpose.[214]

Lawyers' protest letters are frequently posted to sites alleged to contain trade secrets, leading to further online criticism by the posters and claims that the trade secret owner thereby has confirmed the value and authenticity of the secret. Thus, sometimes the costs of seeking removal of trade secrets from the Internet, in terms of reputational injury vs. efficacy, are simply unreasonably high.

Some victims of online postings therefore adopt a counterintuitive approach to reasonably protect what remains of their secret: they ignore the posting and concentrate their attention on following precautions such as those described in this article to prevent further leaks. This approach may well be a reasonable tradeoff, particularly where the posting is only of modest value. A trade

---

211 *See* Andy Greenberg, *The Streisand Effect*, FORBES.COM, May 11, 2007, http://www.forbes.com/2007/05/10/streisand-digg-web-tech-cx_ag_0511streisand.html (last visited Feb. 12, 2009); Mike Masnick, *Photo of Streisand Home Becomes an Internet Hit*, TechDirect, June 24, 2003, http://www.techdirt.com/articles/20030624/1231228.shtml (last visited Apr. 24, 2009).

212 *See* Brad Stone, *In Web Uproar, Antipiracy Code Spreads Wildly*, NYTIMES.COM, May 3, 2007, http://www.nytimes.com/2007/05/03/technology/03code.html?fta=y (last visited Feb. 12, 2009).

213 Bank Julius Baer & Co. v. Wikileaks, 535 F. Supp. 2d 980, 985 (N.D. Cal. 2008).

214 *Id.* The reasoning in this case and in the decision to remand in *Bunner* is consistent with the admonition in *eBay, Inc. v. MercExchange L.L.C.*, 547 U.S. 388, 393–94 (2006) that injunctive relief is not presumptively the best solution for all intrusions on an intellectual property owner's rights.

secret owner that takes no effort to remove a posting, however, should be aware that it may face a claim that it has failed to take reasonable measures to maintain secrecy if it later files a suit against others to protect that very information.[215]

Some companies decide to take different tacks to online leaks. For example, protests from irate consumers led Dell Computer to retreat from its cease-and-desist letter demanding that a posting called "22 Confessions of a Former Dell Sales Manager" be removed from the *Consumerist.com* website.[216] Dell had initially complained that the posting contained information that was "confidential and proprietary to Dell."[217] After numerous critical postings, Dell, embarrassed by the negative publicity, released an announcement stating: "We blew it . . . . Instead of trying to control information that was made public, we should have simply corrected anything that was inaccurate. We didn't do that, and now we're paying for it."[218]

Finally, in a modern version of Gresham's law,[219] some victims of online postings—or those who anticipate them—may choose to engage in self-help campaigns of "misinformation" to leave Internet viewers uncertain whether information posted on the Internet is a genuine secret or simply false rumor, thereby potentially reducing the impact of improper postings.[220]

---

215 The resolution of such challenges will be fact specific. In the previously discussed case of *Silicon Image, Inc. v. Analogix Semiconductor, Inc.*, No. C-07-00635 JCS, 2008 WL 166950 (N.D. Cal. Jan. 17, 2008), for example, the plaintiff had not been previously aware of the third-party posting, and thus had not been in a position to seek removal. *Id.* at *10. Notwithstanding the plaintiff's ignorance of the posting, the defendant urged that the unchecked posting had destroyed the secret. *Id.* at *16. The court rejected this defense under the specific facts presented. *Id.*

216 Declan McCullagh, *Dell Apologizes for Remove-This-Blog-Post-or-Else Nastygram*, CNET NEWS BLOG, June 18, 2007, http://news.cnet.com/8301-10784_3-9730579-7.html (last visited Feb. 12, 2009).

217 *Id.*

218 *Id.*

219 Gresham's law—that "bad money drives out good"—is an economic principle attributed to Thomas Gresham, a sixteenth-century English economist. Robert Goldscheider, *The Negotiation of Royalties and Other Sources of Income from Licensing*, 36 IDEA 1, 17 n. 6 (1995).

220 Lemos, *supra* note 147, notes that within two days of an alleged leak of Cisco source code, the full source code could not be located online by *CNET News.com* and there was speculation about the authenticity of two brief excerpts on a Russian website. Whether the real code had ever actually been posted or whether the original posting had been replaced and, if so, by whom, was uncertain. *Id.*

III. THE HOLE IN THE INTERNET

The suggestions discussed above may, in some instances, permit the trade secret owner to secure an order from a court in the United States directing the takedown of trade secrets from servers in the United States or from servers controlled from the United States. But not every server is in or controlled from the United States. So what is the trade secret owner to do if the trade secret appears on a server located outside of the United States? In that instance, the trade secret owner has stumbled into a danger zone. While it is possible that in an egregious case a trade secret owner may be able to persuade a U.S. prosecutor that the violation triggers the extraterritorial scope of the Economic Espionage Act, that effort can take a significant amount of time, during which the postings may continue to spread and render the secrets more widely known. The trade secret owner may be unlikely to secure rapid injunctive relief abroad. The particular foreign sovereign may not grant interim injunctive relief in civil cases absent direct evidence of misappropriation. Or, the specific foreign court may not yet have accepted the proposition that information can still be a trade secret once it has been posted on the Internet. The trade secret owner faced with foreign postings may thus be forced to rely primarily on other legal remedies besides injunctive relief in civil litigation.

IV. SELF-DESTRUCTION

It should go without saying that no company should intentionally post its own secrets on the Internet without restriction nor should it permit its affiliated companies to do so. Posting trade secrets on generally accessible portions of the Internet obviously is not a reasonable means to maintain their secrecy. Yet it happens, frequently and thoughtlessly. The following scenarios illustrate ways companies effectively can destroy their own trade secrets online: (1) proud companies placing their lists of customers or employees on their websites; (2) high-tech companies pre-announcing products under development along with their projected release timetables; (3) companies seeking business partners posting their inventors' confidential technical papers online; and (4) parties interested in forming strategic alliances prematurely announcing what business partners they are pursuing and for what reasons.[221] The lesson to learn: avoid these self-destructive practices altogether.

---

[221] *See, e.g.*, PartyLite Gifts, Inc. v. Swiss Colony Occasions, No. 06-6107, 2007 WL 2478582, at *5 (6th Cir. Aug. 29, 2007) (finding that identities of customers and other operational data at issue were not trade secrets because they had been disclosed by plaintiff's franchisees on hundreds of websites and franchisor had taken no steps to demand removal). More shocking-

V. CONCLUSION

Increased digitization of information and the Internet's ability to widely disseminate that information means that, more than ever before, the trade secret owner must be relentlessly focused on protecting its secrets. There is little margin for error in preventing misappropriation and little time to lose in seeking relief if it occurs. However, digital tools can also help trade secret owners build strong digital locks for their secrets and develop solid evidence of misappropriation. Using new contracting and statutory tools to implement old legal principles (restricting access, segregating information, using well-crafted nondisclosure agreements) and constantly evaluating and reinforcing protection strategies can assist the trade secret owner to take reasonable measures appropriate to new circumstances to keep its proprietary information safe.

ly, see *Paramanandam v. Hermann*, where the court denied a preliminary injunction against misappropriation of trade secrets because a trade secret owner had revealed most of the information on its web site and its principal had testified: "[W]e chose not to be secretive. We chose to show all our cards to our competition so that . . . it would look odd . . . no one hides everything in their computer. It's left out for the general public to see. So we chose not to hide a bunch of information." 827 N.E.2d 1173, 1180 (Ind. Ct. App. 2005) (emphasis omitted).