PUBLIC DISCLOSURE POLICIES: CAN A COMPANY STILL PROTECT ITS TRADE SECRETS?

Stephen R. Wilson

INTRODUCTION

The recent focus on corporate wrongdoers has prompted Congress and the Security Exchange Commission (SEC) to enforce stricter accountability laws and rules. At the core of these changes rests the policy issues surrounding mandatory disclosure. Many of the new statutes and rules compel corporate directors, officers, analysts and investment bankers to disclose any non-impartial relationship. Additionally, many of these new disclosure provisions afford employees “whistleblower” protection when disclosing evidence of corporate wrongdoing. For all its benefits, however, an inherent conflict exists between rewarding or encouraging disclosure and protecting a company’s trade secrets.

In an attempt to encourage internal-policing, President Bush recently signed the Corporate and Criminal Fraud Accountability Act (criminal component of the Sarbanes-Oxley Act) (CCFAA). Specific provisions of the CCFAA provide whistleblower protection for employees who disclose evidence relating to corporate fraud. While the CCFAA implicitly provides a trade secret disclosure exemption, companies appear to have limited recourse against employees who mistakenly disclose trade secrets. Generally, whistleblower protection provisions raise potential conflicts

* Law Clerk to the Justices of the Massachusetts Superior Court; J.D. 2003, Suffolk University Law School; M.A. 2000, University of Massachusetts; B.A. 1998, University of Massachusetts. This article won first prize in the 2003 Heyman Memorial Writing Competition on Corporate Governance.


3. See id.
between permissive disclosure and trade secret law.

Aside from employee watchdog concerns, many companies need to address regulatory concerns relating to trade secret treatment. As a regulatory obstacle, companies must often acquiesce to informational requests by government agencies. Once an agency receives and processes confidential data, business competitors may request that information under the Freedom of Information Act (FOIA). While the FOIA includes an exemption from trade secret disclosure, competitors may still succeed in acquiring the information. Most trade secret owners are aware of the FOIA disclosure problems, though other public disclosure policies may raise concerns. This article seeks to unravel these conflicts and determine to what extent any conflicts remain unanswered.

Part I gives a basic overview of the state and federal statutory and authoritative provisions for both criminal and civil trade secret misappropriation. Part II discusses statutory protection for whistleblowers, qui tam plaintiffs, and other permissive disclosure rules that raise conflict with trade secret law. Part III focuses on mandatory disclosure issues such as procuring a government contract, satisfying regulatory rules, and petitioning for information under the FOIA. Part IV attempts to resolve any conflicts and offer practical business suggestions to reduce corporate harm. Lastly, the conclusion suggests that despite the apparent attack on trade secret protection, conscientious and well-managed companies will continue to prosper.

I. HISTORICAL DEVELOPMENT OF TRADE SECRET LAW

State law primarily controls the majority of trade secret cases. State courts routinely apply a combination of common law and statutory

---

4. 5 U.S.C. § 552(a) (2000). But see 5 U.S.C. § 552(b)(4) (2000) (“This section does not apply to matters that are . . . trade secrets and commercial or financial information obtained from a person and privileged or confidential.”).
5. Chrysler Corp. v. Brown, 441 U.S. 281, 293 (1979) (stating that “Congress did not design the FOIA exemptions to be mandatory bars to disclosure”).
6. See Vincent J. Schodolski, Advocates of Openness Fight Sealing of Civil Court Records, THE CHICAGO TRIBUNE, Sept. 25, 2002, at 11. In one example of a pending public disclosure policy, South Carolina federal district court judges have recently voted to eliminate sealed settlements. See id. Proponents of this court rule argue that unsealing settlements will assist the public by revealing the identity of child abusers, defective products, negligent surgeons and crooked attorneys. See id. Several state governments have enacted similar court rules with mixed results. See Gregory From, Comments Note Drawbacks, Benefits Secrecy Ban, SOUTH CAROLINA LAWYERS WEEKLY, Oct. 28, 2002, at 11. By revealing secret settlements, however, trade secret owners will lose their ability to maintain secrecy during and after litigation. Id. The potential consequence of this proposed rule will adversely impact trade secret owners. See id.
provisions when addressing trade secret misappropriation inquiries. Often, courts analyze trade secret law within the ambit of unfair competition. In addition to state authority, federal statutory schemes exist, which address trade secret misappropriation in both civil and criminal contexts.

In an effort to codify existing common law, the American Bar Association urged the National Conference of Commissioners on Uniform State Laws to draft a uniform set of trade secret laws.\(^7\) The primary objective for establishing a uniform set of rules was, at a minimum, to reconcile the disparity among the states regarding the definitions of a “trade secret” and “misappropriation.”\(^8\) Many states have adopted the majority of Uniform Trade Secrets Act (UTSA) provisions. Other states, however, continue to apply their own definitions and standards.\(^9\) In some ways, the UTSA may have further complicated an already complex legal scheme.\(^10\)

Between 1939 and 1979, state courts universally cited the Restatement


\(^8\) Id. § 2.03[a]. The UTSA defines a “trade secret” as:

[I]nformation, including a formula, pattern, compilation, program, device, method, technique, or process, that 1) derives independent economic value, actual or potential, from not being generally known, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and 2) is subject of efforts that are reasonable under the circumstances to maintain its secrecy.

\(^9\) Id. The UTSA defines “misappropriation” as:

(i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (ii) disclosure or use of a trade secret of another without express or implied consent by a person who (A) used improper means to acquire knowledge of the trade secret; or (B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was (I) derived from or through a person who had utilized improper means to acquire it; (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or (C) before a material change of his position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

\(^10\) Id.

Id.

Mass. Gen. Laws ch. 266, § 30(4) (2002). In Massachusetts, the term trade secret is defined as “anything tangible or intangible . . . which constitutes . . . a secret scientific, technical, merchandising, production or management information, design, process, procedure, formula, invention or improvement.” Id.; see also Mass. Gen. Laws ch. 93, § 42 (2002).

Pooley, *supra* note 7, § 2.03[1]. The National Conference of Commissioners promulgated two versions of the UTSA. See id. § 2.03[7][b]. Many states have either adopted the first UTSA, the second UTSA, a combination thereof, or amended specific provisions to remain with their common law. See id.
of Torts in cases addressing trade secret misappropriation. The Restatement of Torts included three consecutive sections addressing the acquisition and misappropriation of trade secrets. The drafters of the Restatement of Torts abandoned trade secret law in 1979 due to the development of the UTSA.¹¹

In 1995, however, the Restatement’s drafters included trade secret law in the Restatement (Third) of Unfair Competition.¹³ This Restatement closely resembles the UTSA in its articulation.¹⁴ Like the UTSA, the Restatement (Third) of Unfair Competition addresses innocent misappropriation and improper acquisition without the necessity of disclosure.¹⁵ Unlike the UTSA, however, the Restatement (Third) of Unfair Competition does not include language indicating that reasonable efforts to maintain secrecy are necessary.¹⁶ That said, the misappropriation elements are fundamentally similar to those articulated in the UTSA.

Prior to 1996, the federal government did not have a specific criminal statute to prosecute trade secret misappropriation in the private sector.¹⁷ The lack of specific statutes forced federal authorities to prosecute trade secret misappropriation using a myriad of other tangentially related statutes such as wire and mail fraud.¹⁸ The advent of the Economic Espionage Act (EEA) empowered federal prosecutors with the authority to specifically charge criminal offenders with trade secret misappropriation.¹⁹

¹¹. Id. § 2.02[1].
¹². Id. § 2.04[1].
¹³. Id.
¹⁴. See RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995). The drafters defined a trade secret as “any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.” Id.
¹⁵. See id.
¹⁶. See id.
¹⁸. 18 U.S.C. § 2511 (2000) (providing for civil and/or criminal penalties for mail and wire fraud including disclosing privileged information).
¹⁹. 18 U.S.C. §§ 1831-1839 (2000). The EEA broadly states the definition of what constitutes a trade secret. See § 1839(3). The EEA amended Title 18 of the United States Code to include nine specific provisions involving economic espionage and trade secret misappropriation. See §§ 1831–1839. The first statutory section addresses the impetus for the legislation, largely to address theft by foreign governments. See § 1831. The second section applies to occasions when the offender intends to convert a trade secret that is related to a product intended for interstate commerce. See § 1832. Offenders face severe consequences when violating the EEA with guilty defendants potentially imprisoned for up
Surprisingly, since the EEA’s enactment, federal prosecutors have not diminished the application of other federal statutes but rather, often use the EEA in conjunction with, or as a companion to, other federal laws. In addition to utilizing the EEA and federal mail and wire fraud statutes, federal authorities used the RICO statute, albeit sparingly, to criminally prosecute trade secret misappropriators. Congress originally enacted RICO as a tool to fight organized crime. Since its enactment, however, plaintiffs have used RICO in the context of business litigation. To succeed on a RICO claim, the plaintiff will have to prove that the defendant engaged in a “pattern of racketeering activity” and was, in effect, involved in a “criminal organization.” Today, prosecutors often use the RICO statute to impose civil remedies.

II. WHISTLEBLOWER DISCLOSURE

Disclosing trade secrets becomes permissive when the trade secret owner grants permission or when statutory or regulatory authority compels disclosure. When permissive disclosures exist, an individual may disclose trade secret information without breaking the law. For example, state and federal whistleblower statutes “may” protect employees who mistakenly disclose trade secrets from employer retaliation. Additionally, under the...
False Claims Act (FCA), the federal government may actually reward individuals for disclosing confidential information. 28

A. Whistleblower Protection Statutes

Congress unanimously enacted the Whistleblower Protection Act of 1989 (WPA) and amended it in 1994. 29 The WPA was the first of many federal whistleblower protection type acts. Generally, whistleblower provisions expressly prohibit employer retaliation against employees who report violations concerning fraud, waste or abuse. 30 The statute initially created a protected class of employees consisting of government employees retaliation protection for employees who disclose information that is “reasonably” believed to be in violation of the law. See id. In effect, the statute gives the employee complete discretion to determine whether any “secret” activity constitutes fraud. See id. The employee has two years to bring a civil action for any employer retaliation. See id. § 185(5)(d). Essentially, the statute requires the employer to keep the employee on the payroll until the two years from the employee’s date of disclosure. See id. The court may only award reasonable attorney fees and court costs to employers for baseless allegations (no explicit recourse for trade secret misappropriation). See id. § 185(e)(1).

28. 31 U.S.C. § 3730(d) (2000). If the Government proceeds as a co-plaintiff, the whistleblower will receive at least 15%, but not more than 25%, of the proceeds resulting from the action. See id. § 3730(d)(1). If the whistleblower proceeds without the government, he or she shall receive not less than 25% and not more than 30%, in addition to compensation for other reasonable expenses. See id. § 3730(d)(2).


30. See id. § 1213(a). This section provides that:

(1) any disclosure of information by an employee, former employee, or applicant for employment which the employee, former employee or applicant reasonably believes evidences—

(A) a violation of any law, rule, or regulation; or
(B) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety; if such disclosure is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs; and

(2) any disclosure by an employee, former employee, or applicant for employment to the Special Counsel or to the Inspector General of an agency or another employee designated by the head of the agency to receive such disclosures of information which the employee, former employee, or applicant reasonably believes evidences—

(A) a violation of any law, rule, or regulation; or
(B) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

Id.
and employees of corporations that contract with the government.\textsuperscript{31}

The whistleblower provisions developed out of the public policy need to encourage internal policing while offering employment protection. The statutory objective sought to limit fraud on the government. The federal government has since included whistleblower protection provisions in over fifty federal statutes.\textsuperscript{32} The federal government pursues most whistleblower complaints administratively, though exceptions exist.\textsuperscript{33} For example, the United States Court of Appeals for the Federal Circuit has exclusive jurisdiction for whistleblowers who are federal government employees and federal district courts provide jurisdiction for \textit{qui tam} whistleblowers.\textsuperscript{34}

Most whistleblower statutes impose severe penalties against retaliating employers. For example, if the employer discharges or discriminates against the whistleblower for “lawfully” disclosing government fraud, the employee may bring a protective action resulting in reinstatement, double backpay, compensatory damages, and in certain circumstances, punitive

\begin{footnotesize}
\begin{enumerate}
\item See id.
\item See \textit{Whistleblower Statutes}, at http://whistleblowerlaws.com/statutes.htm (last visited Feb. 7, 2004); see also 31 U.S.C. § 3730 (2000). Section 3730(h) provides the following:

\begin{quote}
Any employee who is discharged, demoted, suspended, threatened, harassed, or in any other manner discriminated against in the terms and conditions of employment by his or her employer because of lawful acts done by the employee on behalf of the employee or others in furtherance of an action under this section, including investigation for, initiation of, testimony for, or assistance in an action filed or to be filed under this section, shall be entitled to all relief necessary to make the employee whole. Such relief shall include reinstatement with the same seniority status such employee would have had but for the discrimination, 2 times the amount of back pay, interest on the back pay, and compensation for any special damages sustained as a result of the discrimination, including litigation costs and reasonable attorneys’ fees. An employee may bring an action in the appropriate district court of the United States for the relief provided in this subsection.
\end{quote}

\textit{Id.}
\item See, e.g., \textit{Whistleblower Laws} at http://whistleblowerlaws.com/law.htm#Conduct (last visited Feb. 7, 2004); \textit{The Law: An Overview, False Claims Act Whistleblower Employee Protections}, at http://whistleblowerlaws.com/protection.htm (last visited Feb. 7, 2004) [hereinafter \textit{Whistleblower Employee Protections}]. A \textit{qui tam} action is “an action brought by an informer, under a statute which establishes a penalty for the commission or omission of a certain act, and provides that the same shall be recoverable in a civil action, part of the penalty to go to any person who will bring such action and the remainder to the state or some other institution ….” BLA"
\end{enumerate}
\end{footnotesize}
B. Corporate and Criminal Fraud Accountability Act of 2002

The Sarbanes-Oxley Act expressly provides protection for employees of publicly traded companies who provide evidence of fraud. The CCFAA contains provisional language explicitly protecting corporate whistleblowers from employer retaliation. Under the whistleblower provision, whistleblowers may file the complaint with the Secretary of Labor who investigates and adjudicates the matter. The CCFAA uses the term “reasonably believes” to describe the threshold when an employee may disclose evidence of fraud. Like many other whistleblower provisions, the CCFAA explicitly states that an employer cannot retaliate against a corporate whistleblower without facing severe consequences.

The CCFAA does not provide insight into what constitutes a “reasonable belief” or, as the Congressional record states, “lawful activity.” The term “lawful activity” appears unambiguous, but it loses clarity when examining the steps generally required to uncover the alleged fraud. In a realistic effort to investigate corporate fraud, the employee would likely have to examine confidential information. By merely investigating confidential documents, the employee may be outside the scope of “lawful activity” and therefore engaging in illegal conduct.

In practice, companies restrict knowledge of trade secrets to essential employees. Non-essential employees may have difficulty distinguishing between covert activity to ensure trade secret protection and covert activity to cover up fraud. The “reasonable belief” standard gives employees broad discretion to determine what constitutes a violation of the enumerated securities statutes and when to investigate such corporate...

36. See id. § 1514A.
37. See id.
38. See id. § 1514A(b)(1); see also Whistleblower Employee Protections, supra note 34.
39. 18 U.S.C. § 1514A(a)(2000 & Supp. 2004). But see 148 CONG. REC. S7420 (daily ed. July 26, 2002). “Since the only acts protected are ‘lawful’ ones, the provision would not protect illegal actions, such as the improper public disclosure of trade secret information.” Id. The provision provides a limited protection for employees that take lawful action to disclose information reasonably believed to be fraudulent. See id. The intention is to impose the normal reasonable person standard. See id. at S7420; see also Passaic Valley Sewerage Comm’rs v. Dep’t of Labor, 992 F.2d 474, 478 (3d Cir. 1993).
40. 18 U.S.C. § 1514A(c).
41. See id.; 148 CONG. REC. S7420, supra note 39.
activities. Accordingly, a “would be whistleblower” may view any clandestine activity as a fraud cover-up.

Acquiring this guarded information would be the employee’s next logical step. In accordance with a pure whistleblower claim, the employee would turn over the acquired information to the appropriate state or federal agency. Of course, if the employee’s fraud allegations are correct, the corporation will be unable to assert trade secret misappropriation. If the employee is incorrect in his belief, the corporation may not have an adequate remedy to address the harm.

C. False Claims Act (Qui tam Statute)

The qui tam provisions of the FCA permit a party who discovers a specified fraud against the United States to bring the matter to the attention of the Attorney General. Upon reviewing the matter, the Attorney General may discretionarily pursue a civil lawsuit against the fraudulent party or allow the plaintiff party (a.k.a. relator or whistleblower) who discovered the fraud to bring the action on behalf of herself and the government.

In accordance with procedural rules, the relator serves a copy of the complaint on the U.S. Attorney General along with disclosure of all material evidence. The relator files the “in camera” complaint with the court and the complaint remains sealed for at least sixty days. During this period the government decides whether to intervene and proceed with the civil action. Federal rules do not require the unsuspecting defendant to respond to the complaint until sixty days after the court unseals the complaint and serves the defendant.

In FCA actions, whistleblower protection subsists regardless of the employee acknowledging its existence and implementation. The court is less likely to protect employees, however, whose job description obligates them (i.e., accountants) to disclose financial inconsistencies to the

---

42. See 18 U.S.C. § 1514A(a)(1). The employee may “provide information . . . which the employee reasonably believes constitutes a violation of section 1341, 1343, 1344, or 1348, any rule or regulation of the Securities and Exchange Commission . . . .” Id.
44. See id. § 3730(b)(4).
45. See id. § 3730(b)(2); see also FED. R. CIV. P. 4(i).
48. Id.
company. On those occasions, the employee should express his or her intent to investigate actual fraud in order for the court to consider retaliation protection. The court is likely to offer whistleblower protection if investigating such fraud is beyond the employee’s responsibilities.

The FCA statute does not contain language detailing the trade secret owner’s recourse upon mistaken disclosure. The sole reference to the employee’s conduct is the provision stating that the employee may assert whistleblower protection, if discharged or otherwise discriminated against, for “lawful acts” done in accordance with the false claim allegation. The FCA does not address instances when an employee discloses both false claims and legally protected trade secrets.

The court will look at the employee’s activities to determine whether the investigative conduct is within FCA’s statutory language. To illustrate, the Ninth Circuit Court of Appeals held that a special education school teacher’s activities had no connection to the FCA because she was not acting “in furtherance” of investigating fraud. The court posited that the teacher did not inform her employer that she was investigating a potential fraud claim when complaining that the school did not comply with regulations. The court could not find a connection between the employee’s subsequent suspension and her prior investigative activities.

One may infer that the court found the employee’s conduct lacked substantive fraud investigation. Alternatively, one may infer that the court

50. See Fried, Frank Memorandum supra note 33.
51. Id.
52. Id.
55. See id.
56. See Fried, Frank Memorandum, supra note 33.
57. Hopper v. Anton, 91 F.3d 1261,1269 (9th Cir. 1996). The school teacher, Sheila Hopper, complained to her superiors that the absence of classroom teachers in the evaluation process of special needs students was not in regulatory compliance. See id. at 1263. The teacher’s complaints to state and federal authorities did not yield compliance. See id. at 1263-64. The school district brought unrelated charges against the teacher and she was suspended. See id. at 1264. The court held that Hopper was not investigating fraud; rather, she was merely attempting to get the school district to comply with state and federal laws. See id. at 1269.
58. See id. at 1269-70.
59. See id. at 1270; see also United States ex rel. Ramseyer v. Century Healthcare Corp., 90 F.3d 1514, 1522-23 (10th Cir. 1996) (holding that the employer’s retaliation was not connected to the employee’s “conduct in furtherance of” her FCA claim and her discharge).
60. See Hopper, 91 F.3d at 1270.
correctly identified a disgruntled employee who waged an after-the-fact “False Claim Act/Whistleblower” claim. Either way, if an employee plans on asserting a *qui tam* action and availing herself to the whistleblower protection provision, it is reasonable to conclude that her conduct or expression must indicate that she is investigating fraud. When investigating fraud, however, the employee is likely to stumble upon non-fraudulent trade secrets.

The language of the FCA may actually encourage the whistleblower to disclose trade secrets. The FCA prohibits claims based upon publicly disclosed information. If the whistleblower’s complaint contains previously disclosed information, such as information publicly known or disseminated by the media, the court may dismiss the case for lack of jurisdiction. The rationale for this prohibition is to discourage potential whistleblowers from offering information readily known by the government.

The bar against claiming previously known or released information effectively eliminates one form of after-the-fact plaintiffs. Arguably, however, the prohibition actually encourages a “would-be” plaintiff to dig deeper in the targeted defendant’s confidential files. In an effort to identify and produce unreleased information, the whistleblower may review and extract confidential documents and trade secrets. The employee may not conclusively know if the confidential information relates to criminal activity or lawful activity. If it is the latter, the employee is engaging in criminal conduct by “acquiring” trade secrets. The defendant company may not know about the pending case or the relator’s identity until months after the plaintiff filed the complaint. During that time, the relator is likely sifting through business records trying to bolster his claim.

---

61. Id. The employee need not know about the existence of the False Claim Act to later assert it. See id. at 1269. The court here, however, simply held that the employee’s conduct and subsequent discharge did not give rise to the False Claim Act. See id. at 1270.


63. 31 U.S.C. § 3730(e)(4) (2000) (limiting claims based upon publicly disclosed information unless the Attorney General or the original source brings the action).

64. Id. § 3730(e)(4)(A).

65. See id.; see also id. § 3730(e)(4)(B). As a companion to this prohibition, the “original source” rule provides an exception to whistleblowers whose information gives rise to the lawsuit. See id.

66. See id. § 3730(e)(4) (limiting the potential plaintiffs to only the Attorney General and the original source).

67. See id.

68. 18 U.S.C. § 1831 (2000); see also MASS. GEN. LAWS ch. 266, § 33A (2002).
III. GOVERNMENT DISCLOSURE

On occasion, companies must disclose their trade secrets to procure business contracts. For example, the government often compels companies to disclose their trade secrets as a contractual condition. Similarly, regulatory agencies compel companies to disclose their trade secrets when applying for licensure or complying with regulations. Although a trade secret exemption exists, the general public, as well as business competitors may use the provisions set forth in the FOIA to compel trade secret disclosure.69

A. Government Contracts

Cost-cutting opportunities prompt companies to outsource their manufacturing requirements. In doing so, non-disclosure agreements become an integral part of the contractual relationship. It is commonplace for companies to share trade secrets in conjunction with a non-disclosure agreement (NDA).70 When a company contracts with the government, however, trade secret disclosure requires special attention.

The government outsources many of its servicing and manufacturing requirements to private vendors. Companies seeking to engage in business with the government should attempt to negotiate a mandatory NDA. As a matter of public policy, however, the government will likely resist signing an NDA. Alternatively, in rare instances, the government may provide an exception when it needs the vendor’s proprietary information.

Trade secret ownership issues occur when the company jointly develops new trade secrets with the government. Therefore, the private party must pay special attention to trade secrets developed after the original agreement with the government. This scenario is particularly realistic when the government works closely with the contractor in developing a product that is at least partially government funded.71

A question of trade secret ownership arose in a 1997 case between Inslaw, a software company, and the Department of Justice (DOJ).72 The DOJ contracted with Inslaw to customize and install Inslaw’s case management system in specified United States Attorney Offices.73 During the course of the contract term, Inslaw alleged that it used private funding to enhance the case management system program and thus, the enhanced

---

70. Pooley, supra note 7, § 8.02.
71. See Cohen & Gutterman, supra note 20, at 359.
73. Id. at 310.
software was proprietary to Inslaw. Subsequently, Inslaw alleged that the DOJ misappropriated Inslaw’s trade secrets by sharing the enhanced software with unauthorized third parties.

Unfortunately, the court never addressed the trade secret misappropriation claim because Inslaw was unable to prove that the enhancements qualified as proprietary software. Accordingly, unless prohibited by contract or preempted by other intellectual property protection, the government could share the “trade secret” portion of the information without restriction because the government shared in the ownership.

B. Agency Relations

Aside from the ill effects of the mandatory disclosure requirement for business-to-government contracts, businesses often disclose trade secrets to regulatory agencies to obtain the proper licenses or to prove compliance with a regulatory standard. Certain agencies adhere to specific statutory and regulatory guidelines involving disclosure restrictions. For example, the Federal Rules of Acquisition expressly prohibit government employees from disclosing trade secrets if the owner of such identifies and marks it with a specified legend. This federal rule persists even in unsolicited

---

74. Id.
75. Id. at 310-11.
76. Id. at 359. The court’s decision covered numerous legal issues, including the transfer of copyright, that go beyond the scope of this paper. See id. at 340. The court did find, however, that the government contract stipulated for certain bug fixes and other enhancements. See id. at 359.
77. 48 C.F.R. § 15.609 (2002) (illustrating how the Federal Rules of Acquisition expressly prohibit government employees from disclosing trade secrets if the owner of such secret identifies it and marks it with a specified legend).
78. Id. If the offeror seeks to restrict data, she must mark the title page with the following legend:

Use and Disclosure of Data

This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this proposal. However, if a contract is awarded to this offeror as a result of—or in connection with—the submission of these data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government’s right to use information contained in these data if they are obtained from another source without restriction. The data subject to this restriction are contained in Sheets [insert numbers or other identification of sheets].

Id.
proposals. The DOJ would subject any government employee who discloses such data to criminal charges.

In some instances, permissive disclosure amounts to mandatory disclosure. Specific federal statutes grant certain government agencies, such as the Food and Drug Administration (FDA) and the Environmental Protection Agency (EPA), permissive authority to disclose trade secret information when it is necessary to protect the public from unreasonable risks. Those agencies will not risk public harm and welfare for the sake of protecting a company’s trade secret.

Government agencies have the unenviable task of balancing public policy concerns with the interests of trade secret owners. As a result, public disclosure regulations such as the FDA’s ‘Fair Packaging and Labeling Act’ (FPLA) seemingly clash with the trade secret rights of private companies. Like many other agency rules, the FPLA provides an exemption for trade secret disclosure. On occasion, however, the FDA and the private company disagree on whether the information, such as an ingredient, qualifies as a trade secret.

In Zotos International, Inc. v. Young, a cosmetics manufacturer sought to qualify an ingredient as a trade secret. After providing the FDA with the formula for the secret ingredients, the FDA refused to qualify the formula as a trade secret because the ingredients were widely used in the industry. In federal district court, the plaintiff unsuccessfully challenged the FDA’s refusal to acknowledge the ingredients as a trade secret. Upon appeal, the court found the agency’s decision was “arbitrary and capricious.” The court remanded the case to the FDA to resolve the discrepancies without declaring the ingredient a “trade secret.”

While the private company

---

82. See generally 5 U.S.C. § 552(b)(1)-(9) (2000)(providing a list of the matters that are not accessible to the public due to their confidential nature).
83. 15 U.S.C. § 1454(c)(3)(B) (2000). The FPLA requires the manufacturer to list the product ingredients in descending order of predominance. See 21 C.F.R. § 701.3(a) (1987). The FPLA does permit, however, a manufacturer to withhold “secret ingredients” by adding the simple phrase “and other ingredients.” Id.
84. 21 C.F.R. § 720.8(a) (1987).
86. Id.
88. Id.
89. See Zotos Int’l, Inc., 830 F.2d at 354.
90. Id. at 353. The court’s findings indicated that it had a problem reconciling the FDA’s regulatory definition of a trade secret with the FDA’s determination that the
seemingly prevailed, the public policy consideration regarding disclosure cost the company significant expenses.

Public policy concerns form the genesis of agency regulations. In addition to protecting the public from health hazards, government agencies promulgate rules to protect the public from financial harm. Under the Securities Exchange Act of 1934, the SEC requires a corporation to disclose specific information in its application for registration. Similarly to other agencies, the SEC promulgated a rule providing an exemption for trade secrets. Unlike many other exemptions, however, the statute grants the SEC explicit authority to disclose trade secrets when it serves the public interest.

When the SEC considers disclosing trade secrets, they must balance public interests with the potential corporate harm. The mere existence of this discretionary disclosure provision has caused corporations to file written objections. In one example, a prestigious watch manufacturer objected to disclosing financial information regarding the cost of goods sold and the mark-up rates. One may speculate that the watch manufacturer’s fear of disclosure relates to the consumer’s likely outrage resulting from the manufacturer’s egregious profit margin. In this case, the SEC believed the public policy to inform consumers outweighed the manufacturer’s trade secret rights.

Corporations have other trade secret concerns beyond the SEC’s registration process. Upon receiving valuable information, corporate officers and directors must determine whether trading securities based on the information violates insider-trading rules. If the corporate insider first determines that certain information is a trade secret and then subsequently withholds public disclosure, the corporate insider may be violating securities regulations.

ingredient is not a trade secret. See id. at 352-53. The FDA had adopted the Restatement of Torts definition of a trade secret. Id. at 352. Upon reviewing each factor, the court refused trade secret protection, thereby denying the FDA’s argument that a secret ingredient has value. See id.

91. MILGRIM, supra note 81, § 12.02[2][a].
92. 15 U.S.C. § 78x(c) (2000) (providing the SEC the authority to use its discretion when deciding whether to provide records and information that may otherwise be confidential).
93. Id. § 24(b).
94. MILGRIM, supra note 81, § 12.02[2][a].
95. Id.
96. See id. This speculation persists because, unlike consumers, corporate investors would be pleased to see a positive raw-cost to sales ratio.
97. See id.
A 1968 case, SEC v. Texas Gulf Sulphur Co., illustrates the difficulty of determining whether to protect information as a trade secret or disclose it pursuant to security regulations. Upon core drilling in the Ontario area, Texas Gulf discovered significant and previously untapped natural resources. Mineral tests indicated that the land was favorable for mining copper and zinc ore. Corporate officers instructed employees to keep the mineral find confidential until the company completed the land acquisition. During this time, employees who knew about the discovery exercised stock options and purchased stock on the open market. In response to the SEC’s requirement to disclose this type of information, Texas Gulf argued that requiring disclosure of this confidential information violated company policy. The court rejected Texas Gulf’s argument finding that the SEC disclosure requirement trumps company policy.

Generally, agencies and the judicial system recognize that certain kinds of company information constitute business property. Corporate officers and directors face severe consequences, however, when incorrectly classifying material information as business property. As Texas Gulf illustrates, withholding material information causes corporate injury. That said, disclosing confidential information to satisfy a public policy regulation may also result in corporate harm.

C. Freedom of Information Act

In 1966, Congress enacted the Freedom of Information Act (FOIA) to ensure public access to government documents. The FOIA enables individuals to gather information submitted to the government by another party. Upon an FOIA request, the government agency must disclose the

99. 401 F.2d 833 (2d Cir. 1968).
100. Id. at 843-44; see generally MILGRIM, supra note 81, § 1.09[8][f] (commenting that business information, such as geophysical data, may qualify as a trade secret).
101. See Texas Gulf, 401 F.2d at 844.
102. Id.
103. Id.
104. Id.
105. See id. at 852 (reasoning that certain defendants withheld material facts, thus injuring other investors which constituted a 10(b) violation).
106. See, e.g., Carpenter v. United States, 484 U.S. 19 (1987) (holding that an employee leaking information breached a fiduciary obligation because the employer had a business property right in confidential information).
107. 5 U.S.C. § 552(a) (2000) (listing the types of documents available and the procedures necessary to obtain these documents).
108. See id. § 552(a)(2)(A) (requiring each agency to make final opinions, including concurring and dissenting opinions, and orders made in the adjudication of cases available for public inspection and copying).
requested information within a specified time unless the information falls within an exempted class. Among the exemptions are “trade secrets and commercial or financial information obtained from a person and privileged or confidential.” The business contracting with or seeking regulatory approval from the government must identify the information designated as trade secrets.

Since 1992, agencies have differentiated between a contractor’s voluntary submission of information and the agency’s required submission of information. Generally, upon an FOIA request, agencies will more readily disclose “required submission” data rather than “voluntary submission” data. In government contract cases, the party requesting the “required submission” data may compel the agency to prove that revealing the requested information will substantially harm the contractor.

The FOIA requires mandatory disclosure of general information; however, the trade secret exemption ostensibly protects trade secrets, commercial information, and financial information from disclosure. Case law, however, reveals a contrary result. In *Chrysler Corp. v. Brown*, the government disclosed the plaintiff’s trade secret after an FOIA request. Even though the request identified trade secrets, the government exercised its discretion and disclosed the information. The Court found that Congress did not intend the FOIA exemptions to automatically prohibit disclosure; therefore, the government had the discretionary ability to disclose known trade secrets to a requesting party.

Many federal regulations require the government agency to provide notice to the trade secret owner if the agency determines that it must disclose the requested information pursuant to the FOIA. If the government agency, notwithstanding opposition, decides to disclose the

109. See id. § 552(a)(3)(A). See also *Milgrim, supra* note 81, § 12.03.
111. *Milgrim, supra* note 81, § 12.02.
113. See id.
117. Id. at 287.
118. Id. at 294.
119. *Milgrim, supra* note 81, § 12.02[1]. Where the federal agency did not promulgate a regulation requiring notice, the trade secret owner should, when possible, obtain a formal agreement with the agency requiring reasonable notice prior to trade secret disclosure. See id.
trade secret, the owner’s sole recourse is to seek review through the Administrative Procedure Act (APA).\(^{120}\) This review will not reverse an agency’s decision unless the decision was “arbitrary, capricious, [or] an abuse of discretion.”\(^{121}\) If the APA finds an improper disclosure, the trade secret owner’s sole remedy is a claim for compensation under the Fifth Amendment Takings Clause.\(^{122}\)

Ultimately, engaging in business with the government may expose trade secrets to competitors. In 1987, President Ronald Reagan issued an executive order encouraging agencies to investigate alternatives to litigation.\(^{123}\) The order effectively empowered agencies to give advance notice to trade secret owners, require data collection fees, and request the advice of the trade secret owner prior to disclosing the information.\(^{124}\) Further, in 1998, the United States Department of Justice issued a guide to government agencies directing the agencies to exercise discretion in favor of disclosure unless the agency could detect a foreseeable harm in doing so.\(^{125}\) Agencies that mistakenly or arbitrarily release trade secret information, however, may trigger a Federal Trade Secrets Act charge, commonly referred to as a “reverse FOIA” lawsuit.\(^{126}\)

The government agency, of course, may still decide to reject a submitter’s request under the trade secret exemption provision. Nonetheless, anecdotal evidence indicates that competitors have nothing to lose when seeking information under the FOIA.\(^{127}\) In recognizing the concerns of private businesses, agencies often release aggregations or summaries of valuable information in an attempt to reduce corporate

\(^{120}\) *Chrysler Corp.*, 441 U.S. at 318 (recognizing the APA authority for judicial review of an agency’s decision to disclose confidential information).


\(^{124}\) See id.

\(^{125}\) See U.S. DEPT. OF JUSTICE, FREEDOM OF INFORMATION ACT GUIDE & PRIVACY ACT OVERVIEW 431, 436 (Sept. 1998).

\(^{126}\) *OSHA Data/CIH Inc. v. United States Dep’t of Labor*, 220 F.3d 153, 160 (3d Cir. 2000); see also 18 U.S.C. § 1905 (2000) (subjecting an officer or employee of the United States or of any department or agency thereof to fines, imprisonment, and termination of their employment for releasing trade secret information).

\(^{127}\) *James T. O’Reilly, Federal Information Disclosure* § 10.1 n.12 (3d ed. 2000) (stating that “[p]erhaps 85% of the FDA’s 30,000 annual FOI requests at the height of its pre-internet FOIA period had come from businesses seeking other firms’ reports.”).
harm. Trade secret owners should research other statutes to protect against complete disclosure. For example, the government agency does not have discretionary authority to disclose an FOIA exemption if another statute, such as the Privacy Act, prohibits disclosure.

IV. RECONCILING CONFLICTS

A. False Claims Act (Qui tam Statute)

As outlined above, individuals bringing qui tam actions under the False Claims Act may seemingly do so without any adverse consequences. If the United States Attorney decides to proceed with the case, the whistleblower virtually has no financial risk associated with bringing the civil action. In the event of an unsuccessful false claim action, the Federal Rules of Civil Procedure bar the defendant from bringing a trade secret misappropriation suit against the whistleblower. The alleged defendant may be able, however, to counterclaim that the whistle-blowing plaintiff misappropriated company trade secrets.

There is very little case law dealing with the defendant’s counterclaim opportunity. In 1993, the Court of Appeals for the Ninth Circuit addressed this matter and found that the defendant could have asserted a counterclaim for independent damages, because those counterclaims were not dependent on the qui tam defendant’s liability (i.e., counterclaim for indemnification). Qui tam relators alleged that the defendant made misrepresentations to the United States Navy regarding the testing and development of a missile system. The defendant filed eight state law

129. Antonelli v. F.B.I., 721 F.2d 615, 616 (7th Cir. 1983); see also Privacy Act, 5 U.S.C. § 552(b) (2000) (stating how no agency shall disclose any record which is contained in a system of records unless the individual to whom the record pertains consents or one of the other twelve exceptions apply).
131. Aside from statutory or common law trade secret misappropriation, an employee who discloses corporate secrets is likely breaching his employment contract. As a condition of employment, the majority of corporations compel their employees to sign a non-disclosure agreement. This contract protects the employer against disclosure of a broad range of confidential information by an employee. In the past, corporations effectively used the NDA to stifle employees from disclosing corporate wrongdoing. Id.; see also Jodi L. Short, Killing the Messenger: The Use of Nondisclosure Agreements to Silence Whistleblowers, 60 U. PITT. L. REV. 1207, 1234 (1999) (suggesting that NDAs should only protect employers from trade secret disclosure).
133. Id. at 829.
counterclaims against the relators alleging, among other things, trade secret misappropriation.\textsuperscript{134}

The court reversed the district court’s dismissal of the counterclaims for independent damages, holding that the dismissal of the counterclaims would violate procedural due process.\textsuperscript{135} The court concluded, however, that if the defendant were found liable under the FCA, then the court should dismiss all counterclaims.\textsuperscript{136}

If the government files a FCA lawsuit, a company should, by default, counterclaim that the employee misappropriated trade secrets. Conversely, if the government and \textit{qui tam} plaintiff decide not to file a civil action (i.e. no fraud or waste), the company must decide whether to proceed with a misappropriation claim. The company should balance resolving the current harm (the misappropriation) with the potential future harm (the disclosure through the discovery process). Unfortunately, even if the company is not engaging in fraudulent activity, a simple accusation of such can be just as damaging.

B. Whistleblower Statutes

Misappropriation includes an acquisition of a trade secret by a person who knows, or has reason to know, that the trade secret was acquired by improper means.\textsuperscript{137} An element of liability for trade secret misappropriation is knowledge of its secrecy.\textsuperscript{138} This element forgives innocent parties who happen upon information not reasonably known to be secretive.\textsuperscript{139} Accordingly, an employee who acquires unreleased confidential information will probably fall within the definition of a misappropriator because he would likely know that the information is secretive due to the difficulty in acquiring it.

Identifying whether an employee is a \textit{qui tam} relator/whistleblower or a trade secret misappropriator is a challenging task. Case law indicates that an employee must acquire information beyond what he would ordinarily acquire when performing his regular job activities.\textsuperscript{140} Thus, the employee must either engage in clandestine activity to acquire this information or

\begin{thebibliography}{9}
\item \textsuperscript{134} \textit{Id.}
\item \textsuperscript{135} \textit{Id.} at 831 (stating that a \textit{qui tam} defendant’s counterclaims would often be compulsory under Rule 13 of the Federal Rules of Civil Procedure and could not be asserted in a separate action).
\item \textsuperscript{136} \textit{Id.}
\item \textsuperscript{137} \textit{Restatement (Third) of Unfair Competition} § 40, cmt. b. (1995).
\item \textsuperscript{138} \textit{Cohen & Gutterman}, \textsuperscript{supra} note 20, at 116.
\item \textsuperscript{139} \textit{See id.}
\item \textsuperscript{140} \textit{See generally} Fried, Frank Memorandum, \textit{supra} note 33.
\end{thebibliography}
inform his employer that he is investigating corporate fraud.\footnote{141}{See id.}

Once a company recognizes that an employee is collecting or reviewing confidential information, the company should delicately inquire about his activity because the employee could actually be a misappropriator rather than a whistleblower. Upon notification that the employee is investigating fraud in accordance with a \textit{qui tam} or whistleblower provision, however, the company should attempt to restrict the employee’s access to privileged information without discriminating against the employee.\footnote{142}{See id.} Of course, this resolution applies to instances when the company is protecting a trade secret rather than concealing fraud.

The company should keep a watchful eye on the employee while allowing him to contribute to the workload.\footnote{143}{See, e.g., GTE Prods. Corp. v. Stewart, 653 N.E.2d 161, 168 (Mass. 1995) (analyzing the difference between quitting voluntarily and a constructive discharge).} The company may have a difficult time identifying the whistleblower unless the employee explains his conduct. Case law indicates that an employee should admit to the purpose for his investigation if he is accessing confidential files.\footnote{144}{See id.}

Identifying the whistleblower becomes increasingly difficult, however, when the whistleblower is an employee who routinely has access to confidential information. On those occasions, the insider would probably be able to differentiate between a trade secret and a fraud cover-up. Thus, depending on the insider’s ability to investigate and make accurate assessments, he is likely to either protect the trade secret or disclose fraud. Conversely, the company would not be able to identify the insider as a whistleblower until government intervention exposes his identity.\footnote{145}{Cf. Hutchins v. Wilentz, 253 F.3d 176 (3d Cir. 2001). For qui tam actions that trigger the whistleblower provision, the employee must show two things: that the employer knew the employee was engaged in protected conduct pursuant to § 3730 (False Claim Act), and that retaliation was motivated by the employee’s protected conduct. See \textit{id.} at 186. Thus, in many whistleblower cases, in order to show that the employer retaliated, the employee must provide notice to the employer that he is investigating fraud. See \textit{id.} at 188-89. Accordingly, the employee’s identity may be disclosed early in the process. See \textit{id.} at 189.}

Similarly, under the CCFAA, a publicly traded corporation would be unable to silence a whistleblower from disclosing corporate fraud.\footnote{146}{See 18 U.S.C. § 1514(a)(1) (2000).} If the conveyed information constitutes fraud, the corporation would not have an actionable claim. Conversely, if the corporation is found innocent of fraud, the company may have a valid breach of contract claim against the employee. In addition to a trade secret misappropriation charge, the
corporation may claim that the employee breached the NDA by disclosing trade secrets to the government.\textsuperscript{147}

Unlike \textit{qui tam} plaintiffs, a pure whistleblower does not file a civil action against the employer unless retaliation ensues. Thus, any aggressive action by the company will likely trigger the whistleblower retaliation protection provision even if the company has an actionable misappropriation claim. If the government does not bring fraud charges, however, it is unclear whether the company may subsequently discharge the employee without giving rise to whistleblower protection.\textsuperscript{148} The company is in the precarious position of deciding whether to retaliate against an employee for incorrectly alleging fraud, or allowing the employee to remain in a potentially hostile workplace.

Aside from acting lawfully, the most efficient way for a company to restrict potential whistleblower damage is to develop and implement a comprehensive trade secret program.\textsuperscript{149} Once in-house legal counsel and security personnel implement the program, the employer should compel current and future employees to sign a document adhering to the specified procedures for handling trade secrets and other confidential information.\textsuperscript{150} The trade secret program document should explain the definition of a trade secret and differentiate it from other confidential information. The document should also explain the relevance of the program and insist on strict compliance. The inherent checks and balances of a comprehensive program should detect unauthorized access and enable companies to address employee interference before any substantive damage ensues.\textsuperscript{151}

C. Government Contracts

A crucial and necessary element of a government contract is the non-disclosure agreement.\textsuperscript{152} Without it, companies risk losing trade secret protection through public disclosure upon an FOIA request or in a government publication. When engaging in business with the private sector, the government must abide by statutory and regulatory

\begin{itemize}
  \item \textsuperscript{147} COHEN \& GUTTERMAN, \textit{supra} note 20, at 116.
  \item \textsuperscript{148} \textit{But see} Gonzalez \textit{v. Superior Court}, 33 Cal. App. 4th 1539, 1550 (1995) (stating that “employers may discipline or discharge an employee who copies the employer’s confidential documents even though the copies are to be used in opposing the employer’s discriminatory practices.”).
  \item \textsuperscript{149} \textit{See generally} COHEN \& GUTTERMAN, \textit{supra} note 20, at 113.
  \item \textsuperscript{150} \textit{See id.} at 113. In addition to an NDA, the authors suggest using a signed document acknowledging the existence of a trade secret program to give employees ample notice. \textit{See id.} at 116.
  \item \textsuperscript{151} \textit{See id.} at 113.
  \item \textsuperscript{152} \textit{See id.} at 116.
\end{itemize}
guidelines. Among the sensitive areas are rules pertaining to the government’s treatment of trade secrets.

The first step in limiting accidental disclosure is ensuring that the government knows that the trade secret exists. The government contractor should create a specific legend to identify each piece of information qualified to receive trade secret protection. In accordance with state statutes regarding maintaining secrecy, the company should continue to follow the security steps and document controls as articulated by its trade secret program. Secondly, if practical, the contractor should notify the government entity of the drastic steps the company takes to retain trade secret protection.

As previously noted, trade secret ownership is another potential concern. The party drafting the contract should try to address as many contingencies as possible to limit questions of ownership. Areas of particular concern are ownership questions relating to “undeveloped” trade secrets. Determining who owns the trade secrets once the contract term expires is a critical inquiry. Additionally, an important contract provision is determining proportional ownership when and if the company accepts government funds to help develop the product.

As a default rule, the company should only share trade secret information on a “need to know” basis. In practical terms, however, the government has considerable leverage to demand information of products currently under development. Of course, the ownership issue undoubtedly relates to the disclosure issue because the owner has the authority to discretionarily disclose trade secrets to third parties.

The facts of Inslaw v. United States illustrate the importance of specificity in government contracts and NDAs. Companies should first look to other forms of intellectual property (IP) protection and investigate any preemption issues for products that cross over into multiple IP protection schemes. For example, the contractor will find it easier to assert its patent right to the data even if the contractor created the product using government funds. While questions of ownership may persist with other forms of IP protection, the federal statutes offer more consistent

---

153. See generally, MILGRIM, supra note 81, § 12.02.
154. Id.
155. See id.
156. See e.g., COHEN & GUTTERMAN, supra note 20, at 113.
157. See MILGRIM, supra note 81, § 12.02.
159. See id. at 310-11.
160. Id. at 359.
161. See COHEN & GUTTERMAN, supra note 20, at 359.
dispositive guidelines. Engaging in contract relations with the government may raise unique concerns, but careful lawyering should alleviate the majority of potential disclosure problems.

D. Government Agencies

Corporations may strategically eliminate disclosure problems relating to securities exchange registration by omitting trade secrets from the application. If the SEC rejects the application, the corporation could file a court action requiring the SEC to issue registration. After an in-camera inspection, the court would determine whether the information qualifies as a trade secret. If the court finds that the information does qualify as a trade secret, the corporation may successfully assert exemption from trade secret disclosure pursuant to Section 24(a) of the Securities and Exchange Act. The SEC may alternatively reassert its authority to disclose if the public interest warrants disclosure. In practice, however, the SEC is likely to carefully deliberate before disclosing information deemed by the court to receive “trade secret” status.

Alternatively, in other applications, clearly identifying trade secret information with a specified legend provides the most protection. The SEC

162. Milgrim, supra note 81, § 12.02[a].
163. Id.
164. See Fed. R. Civ. P. 26(c). The trade secret owner may file a motion to petition the court to take protective actions upon disclosure. Id. The motion should include a certification of good faith along with a statement conferring that the parties attempted to resolve the dispute. Id. Additionally, the motion should include language petitioning the court not to reveal the trade secret or reveal it only in a designated way. See id.; see also In re Remington Arms Co., 952 F.2d 1029, 1033 (8th Cir. 1991) (reviewing the documents “in camera” to determine whether the information qualifies as a trade secret); Fed. R. Civ. P. 26(c). Once the court acknowledges that the information qualifies as a trade secret, it uses a balancing system to determine whether the claim to privacy outweighs the need for discovery. Id.; see also Pooley, supra note 7, § 11.03[1]. The party seeking disclosure shoulders the burden of proving the information is both relevant and necessary. See id. In practice, courts have not automatically given trade secrets absolute immunity from disclosure. See id. The court has the discretion to limit trade secret disclosure to the opposing party or, in a more limited sense, to only the opposing parties’ counsel. See id. Recognizing the sensitivity of trade secrets, the court’s objective is to limit disclosure to the current litigants. See id. A whole body of case law exists regarding the limitations of discovery to certain members of the opposing party. See id. Of primary concern to trade secret owners is limiting discovery to the opposition’s outside counsel while restricting it from the opposition’s in-house counsel. See id. § 11.03[3].
165. Milgrim, supra note 81, § 12.02[2][a].
166. See id.
167. See id.
and other agencies have defined rules relating to trade secret protection.\(^{168}\) Information related to public health concerns is unquestionably susceptible to losing trade secret status. Companies that manufacture food, drugs or chemicals are particularly vulnerable to an agency request for confidential information. Accordingly, such companies should investigate alternative forms of economic protection for information identified as potential targets for disclosure. Relying on the government agency to protect the trade secret may be a frustrating and unreliable experience.

In *Chrysler Corp. v. Brown*, the Court settled whether an agency may disclose a trade secret to a third party upon an FOIA request.\(^{169}\) The agency will notify the trade secret owner of its intent to disclose.\(^{170}\) Apparently, the agency makes a determination to disregard the exemption by identifying what the trade secret is and who is requesting it.\(^{171}\) The problem is that the agency uses its own system to value the secrecy of the information. This inherent problem undermines trade secret law precedent.

Nevertheless, if the agency determines that the information should not qualify as a trade secret or if public disclosure outweighs the company’s proprietary right, then disclosure may result.\(^{172}\) Upon mistaken disclosure, however, the federal government provides statutory remedies for trade secret misappropriation by government employees.\(^{173}\) This statute seems to address malicious disclosure, however, as opposed to a regretful FOIA disclosure.\(^{174}\)

**CONCLUSION**

Public policy concerns compel the government to disclose information relating to health, safety, and financial welfare. All the public disclosure cases and conflicts outlined herein relate to these three areas of public information. The statutes and regulations authorizing government disclosure, however, barely protect companies from frivolous or arbitrary disclosure.

The government seemingly gives whistleblowers a virtual license to raid a company’s confidential information. Some companies would rather settle whistleblower claims before the trial date than disclose trade secrets in

---

168. *Id.*
170. *See id. at 316.*
171. *See id.*
172. *See id.*
173. 18 U.S.C. § 1905 (2000) (subjecting an officer or employee of the United States or of any department or agency thereof to fines, imprisonment, and termination of their employment for releasing trade secret information).
174. *See id.*
Once an employee triggers a whistleblower statute, however, he will be unable to assert other employment and labor-related claims. This rule should effectively limit the number of employee watchdogs to those few who have a sound reason to suspect fraud or waste. On occasions when a whistleblower-relator mistakenly accuses a company of fraud and instead discloses trade secrets, the company should use various equitable remedies to limit the damages.

Commentators should give the government some credit for its ability to accurately determine whether a whistleblower claim warrants intervention and action. The government should be able to distinguish disgruntled employees from upstanding employees. The lack of case law in this area indicates that the government filters out frivolous lawsuits and malicious fraud accusations. Commentators should also note that courts are able to distinguish after-the-fact whistleblowers from those who are legitimately trying to expose fraud or waste.

Nevertheless, pure whistleblower concerns are difficult to reconcile with the government’s efforts to protect trade secrets and other confidential information. As a result, companies may be forced to choose between protecting sensitive information and ensuring the public’s right to know.

175. IBC Fires Back, Says Settlement Saves Costs, THE SALT LAKE TRIBUNE, July 31, 2002, at B3. Rather than risking trade secret disclosure through discovery, IBC settled with the government for $1.2 million. See id. The case was brought by the government and a qui tam whistleblower. See id.

176. See http://whistleblowerlaws.com/law.htm#Conduct (last visited Feb. 7, 2004); see also McGrane v. Reader’s Digest Ass’n, 863 F. Supp. 183 (S.D.N.Y. 1994) (finding that employee waived any breach of contract claims when he elected to proceed in accordance with the state’s whistleblower statute).

177. Looking forward, however, companies may soon battle a new court-related disclosure trend. Vincent Schodolski, Advocates of Openness Fight Sealing of Civil Court Records, THE CHICAGO TRIBUNE, Sept. 25, 2002, at 11. In July 2002, all ten South Carolina federal district court judges voted to ban settlements under seal. See id. The judges justified their vote by arguing that sealed settlements block public access to information relating to faulty products, pertaining to the identity of sexual predators, and preventing notice of negligent physicians. See id. The judges cited recent cases where sealed information caused public harm. See id. The judges specifically identified cases including Firestone’s defective tires and the Catholic priest abuse scandals. See id. The newly proposed disclosure rules, however, may have a chilling effect on the protection of trade secrets. See id. Under these new rules, commentators suggest that companies may bring frivolous lawsuits against competitors as a means to compel trade secret disclosure through the discovery process. See Richard A. Epstein, The Disclosure Dilemma, BOSTON GLOBE, Nov. 3, 2002, at D1. More likely, however, competitors may simply track court cases and access the resulting disposition through legal databases. See id.

178. Although a company would be reluctant to publicize that the government decided not to pursue an accusation of fraud. Only practitioners in this area would be able to accurately attest to such a statement.

179. See Archer Daniels Midland Co. v. Whitacre, 60 F. Supp. 2d. 819, 831 (C.D. Ill. 1999) (dismissing employee’s counterclaim that his discharge for theft was pre-textual and that the employer terminated his employment because he was acting as a whistleblower).
because companies would rather not engage in an adverse battle with the
government. Arguably, law-abiding companies have a better opportunity to
defend themselves against a *qui tam*/whistleblower because they are able to
counterclaim trade secret misappropriation. The difficulty associated with
*qui tam* whistleblowers, however, is keeping them employed and trying to
restrict access to confidential information without discriminating against
them.

Developing and implementing a comprehensive trade secret program
should at minimum identify unauthorized employee access to confidential
documents. For responsible companies, early employee identification may
lead to a satisfactory intervention before any substantive damage.
Furthermore, identifying the unauthorized employee who infiltrated the
trade secret program may enable the company to inquire if the employee is
alleging fraud or planning to misappropriate trade secrets. Either way, the
company benefits from knowing who accessed confidential documents.

Public disclosure policies should continue to challenge companies to
consider the importance of trade secrets. Implementing fundamental
business objectives such as: identifying confidential information;
categorizing trade secrets; incorporating other intellectual property
protections; establishing a trade secret program; notifying employees and
vendors of the importance of following the program; and conducting
periodic assessments of the above mentioned activities, should effectively
reduce company harm relating to trade secret disclosure.