

Choosing Between Trade Secret and Patent Protection

Dean W. Russell, James F. Bogan, III and Kristin M. Crall¹

The phrase “intellectual property” conjures visions of patents issued to pioneering inventors and famous trademarks and copyrights covering great works of art, literature, and music. But intellectual property is not limited solely to these three well-recognized forms; certain subject matter can also be protected as a “trade secret.” Indeed, headlines have featured large and high profile trade secret cases, such as those describing DuPont Co.’s \$920 million verdict for theft of its trade secrets relating to its anti-ballistic fiber, Kevlar;² a \$525 arbitration award to hard disk drive maker Seagate Technologies in its trade secret suit against Western Digital Corp;³ a \$44 million judgment against Accenture LLP for misappropriating the software and source code trade secrets of a competitor;⁴ and the three-year federal prison sentence of the General Motors engineer for copying thousands of sensitive documents valued at \$40 million to the company.⁵

These cases illustrate how, in the light of increased use of the Internet for storing and accessing data and a mobile workforce, choosing trade secret protection can be a viable—and in many instances, preferable—way to protect valuable company information. However, choosing the proper weapon from the intellectual property arsenal involves more than just knowing the labels of the available options. With the increasing importance of technology (and the corresponding increase in infringements, misappropriation, and aggressive hiring of key employees), it is important to understand the costs and benefits of, and the steps to implement, each form of protection to choose correctly from the alternatives. Proper selection is further complicated by the fact that some forms of protection, such as trade secret and patent protection, can be used to protect the same subject matter. For example, various inventions that are fully patentable may instead be protected by trade secret law. This article outlines what trade secret protection is, why a company might choose trade secret protection over patent protection, and how to implement trade secret protection.⁶

I. What is a Trade Secret?

Courts have struggled with developing a particularized definition of what a trade secret is and what type of intellectual property it protects. The definition recited in the Uniform Trade Secrets Act, adopted by forty-seven jurisdictions and the District of Columbia, has been influential. The Uniform Trade Secrets Act defines a trade secret as:

[I]nformation, including a formula, pattern, compilation, program, device, method, technique, or process,

¹ The present authors would like to acknowledge and thank the authors of an earlier version of this article, Russell A. Korn and Christopher M. Durkee.

² Jef Feeley, *Kolon Loses \$920 Million Verdict to DuPont in Trial Over Kevlar*, BUSINESSWEEK.COM (Sept. 15, 2011), <http://www.businessweek.com/news/2011-09-15/kolon-loses-920-million-verdict-to-dupont-in-trial-over-kevlar.html>.

³ Jacqueline Bell, *Seagate Wins \$525M in Western Digital Secrets Row*, LAW360 (Nov. 21, 2011, 1:06 PM), http://www.law360.com/ip/articles/287459?nl_pk=86604097-1f36-4bfa-a7ca96c7182cf1bc&utm_source=newsletter&utm_medium=email&utm_campaign=ip (which was vacated by Minnesota District Court: http://www.theregister.co.uk/2012/10/16/wd_off_arbitration_hook/).

⁴ Ciaran McEvoy, *5th Circ. Affirms \$44M Willogix Jury Award in IP Fight*, LAW360 (May 15, 2013, 5:54 PM), <http://www.law360.com/articles/442011/5th-circ-affirms-44m-wellogix-jury-award-in-ip-fight>.

⁵ Dan Prochilo, *GM Trade Secret Suspect Gets 3 Years for \$40M Theft*, LAW360 (May 1, 2013, 10:24 PM), <http://www.law360.com/articles/437921/gm-trade-secret-suspect-gets-3-years-for-40m-theft>.

⁶ Discussion of trademark and copyright protection is beyond the scope of this article. Additionally, some basic familiarity with patents is presumed.

that:

- (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
- (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.⁷

This general language does not define the subject matter of a trade secret as much as establish a functional definition that grants trade secret protection to those who vigorously police access to and maintain the secrecy of the trade secret. This functional definition covers virtually any material that (1) is appropriate subject matter, (2) is maintained as a secret, (3) is not generally known to the industry or public, (4) is either commercialized or of some value, and (5) has a certain degree of particularity or concreteness.⁸

The potential subject matter is extremely broad, although the requirement for concreteness or particularity serves somewhat to limit it. The requirements that the material be not generally known and secret work together. Information that is generally known may include published and/or distributed material, albeit in an obscure or limited distribution form. This may render the information “generally known” and unprotectable.

Value generally is established by showing that the secret is an advancement in the industry or offers a competitive advantage. As a practical matter, courts tend to protect information that was developed with a significant expenditure of time and money, that was difficult to obtain, and that is not generally known. Some jurisdictions protect “negative” information, i.e., information about processes or techniques that do not work, since knowing a certain approach is unsuccessful may offer a competitive advantage over others who must expend resources discovering the same.⁹

The party asserting the alleged trade secret must prove that one exists, which will generally involve a fact-sensitive determination.¹⁰ Documenting steps taken to protect and develop a trade secret is accordingly crucial. Once trade secret protection is effectively established, however, the owner may be able to prevent:

- (1) unauthorized disclosure by those formerly or presently in an express or implied confidential relationship with the owner; or
- (2) discovery of the trade secret by improper or unethical means.

Although trade secrets are generally governed by state law, one development in trade secret law legislation has increased the scope and power of *federal* protection of trade secrets under the Economic Espionage Act (EEA).¹¹ This Act expands the EEA to cover not only products that are *actually* related to or included in a product placed in interstate or foreign commerce, but also to cover to products or services that are “intended” for such use.¹² Trade secrets that are used internally to help a company gain a competitive advantage may be protected under the EEA, which imposes criminal sanctions.

II. What to Consider in Choosing Between Trade Secret and Patent Protection

Given the all-inclusive (yet tenuously defined) scope of trade secret subject matter, one would correctly suspect

⁷ UNIF. TRADE SECRETS ACT § 1 (Condensed 1985), 14 U.L.A. 537-38 (2005).

⁸ 1 INTELLECTUAL PROPERTY COUNSELING AND LITIGATION, § 5.01 (2), at 5-5 through 5-6 (Lester Horwitz & Ethan Horwitz eds. 1994).

⁹ See, e.g., UNIF. TRADE SECRETS ACT § 1 cmts., 14 U.L.A. 538-39 (2005).

¹⁰ See generally, *Lear Siegler, Inc. v. Ark-Ell Springs, Inc.*, 569 F.2d 286, 288-89 (5th Cir. 1978) (footnote omitted) (“The term ‘trade secret’ is one of the most elusive and difficult concepts in the law to define. The question of whether an item taken from an employer constitutes a ‘trade secret,’ is of the type normally resolved by a fact finder after full presentation of evidence from each side.”); *Capital Asset Research Corp. v. Finnegan*, 160 F.3d 683, 685-86 (11th Cir. 1998).

¹¹ 18 U.S.C. § 1831 (2006).

¹² This legislation was passed in response to the Second Circuit Court of Appeal’s decision in *United States v. Aleynikov*, in which the conviction of a Goldman Sachs ex-programmer (sentenced to prison time for encrypting and uploading substantial portions of source code for Goldman’s high frequency trading (HFT) platform system to a server, and then downloading the material to a portable storage drive and sharing the material with his new employer) was overturned. 676 F.3d 71 (2d Cir. 2012) (in which the EEA was found not to extend to the trade secrets at issue because, although the HFT system generated enormous profits, it was not produced for nor placed in interstate commerce). See also Max Stendahl, *Ex-Goldman Coder Loses Double Jeopardy Bid In Theft Case*, LAW360 (Apr. 30, 2013, 6:48 PM), <http://www.law360.com/articles/437403/ex-goldman-coder-loses-double-jeopardy-bid-in-theft-case>; Scott Flaherty, *2nd Circ. Limits Prosecution in Goldman Trade Secret Case*, LAW360 (Apr. 11, 2012), <http://www.law360.com/articles/329043/2nd-circ-limits-prosecution-in-goldman-trade-secret-case>.

that it overlaps with the scope of patentable subject matter under federal patent law.¹³ Generally, it helps to divide this overlap between patent and trade secret protection into categories:

- (1) inventions that are not patentable;
- (2) inventions of dubious patentability; and
- (3) clearly patentable inventions.

Deciding between patent and trade secret protection for non-patentable inventions is easy: one should protect such material to the extent possible under trade secret law, which “encourages the development and exploitation of those items of lesser or different invention than might be accorded protection under the patent laws, but which items still have an important part to play in the technological and scientific advancement of the Nation.”¹⁴ Where, however, the invention falls into category (2) or (3), it may be protected through either patent or trade secret protection. What are the ramifications of choosing between the two?

A. Characteristics of Patent and Trade Secret Protection

Whether to pursue patent protection of a potentially valuable idea that the owner believes to be of dubious patentability can present a difficult question. Faced with a risk of expending time and money and failing to obtain a patent, or obtaining a patent that is too narrow to provide protection in the marketplace or that may eventually be invalidated, a technology owner may turn to trade secret protection. Seeking patent protection remains tempting; since issued patents are presumed valid,¹⁵ the expense associated with patent infringement suits can encourage competitors to opt to pay at least a modest royalty rather than engage in litigation.

Knowing the relative strengths and weaknesses of patent versus trade secret protection helps a company determine whether to maintain the invention as a trade secret or seek a patent. One crucial distinction is that a patent provides a period of exclusive use—generally, twenty years from its earliest non-provisional filing date—in return for full disclosure of the invention.¹⁶ By contrast, trade secret protection is potentially unlimited in duration: it continues so long as competitors do not reverse engineer or independently develop the subject matter of the trade secret, or so long as it is not disclosed. For instance, The Coca Cola Company has maintained its famous formula for the Coca Cola® beverage as a trade secret for decades. If the owner had patented the formula, it would have become publicly available and usable after the patent’s expiration.

However, “[t]rade secret law provides far weaker protection in many respects than the patent law. While trade secret law does not forbid the discovery of the trade secret by fair and honest means, e.g., independent creation or reverse engineering, patent law operates ‘against the world,’ forbidding any use of the invention for whatever purpose for a significant length of time.”¹⁷ Instead of the absolute barrier patent law provides against even those who independently develop the subject matter of the invention, “trade secret law functions relatively as a sieve,” and “[t]he holder of a trade secret . . . takes a substantial risk that the secret will be passed on to his competitors, by theft or by breach of a confidential relationship, in a manner not easily susceptible of discovery or proof.”¹⁸ If accidental or wrongful public disclosure occurs, the only remedy is to obtain damages against the disclosing or misappropriating party. The trade secret is lost forever—it is no longer a “secret” and the public may use it.

B. Business Factors Affecting the Decision

An owner must weigh factors other than just the legal scope of trade secrets and patents in determining how to protect an idea. Factors favoring patent protection may include:

- (1) the deterrent effect patents provide to competitors who otherwise might be tempted to make and sell similar products;

¹³ A patent may be granted to “[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof,” 35 U.S.C. § 101 (2006), subject to the requirements of novelty, utility, nonobviousness and appropriate disclosure. *Id.* § 102 (Supp. V 2011); § 103 (Supp. V. 2011); § 112 (Supp. V 2011).

¹⁴ *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 493 (1974).

¹⁵ See 35 U.S.C. § 285 (2006).

¹⁶ See 35 U.S.C. § 154 (West Law 2001 & Supp. II 2013).

¹⁷ *Kewanee Oil*, 416 U.S. at 489-490 (footnote & citation omitted).

- (2) the protection it supplies for inventions that can be reverse-engineered;
- (3) the avoidance of security procedures needed to maintain internal secrecy¹⁹; and
- (4) the value patents furnish for potential cross-licensing or settlement of patent infringement (or other) litigation.

By contrast, factors favoring trade secret protection may include:

- (1) the expense of obtaining the patent, which does not immediately provide a revenue stream (unless licensed) and, similarly, protection in foreign jurisdictions without the difficulty and expense of obtaining foreign patents;²⁰
- (2) the potential for delay (e.g., of product launch) while a patent application is prepared and filed (particularly in foreign jurisdictions where no grace period between use or sale of the invention and filing an application is available);
- (3) the fact that the disclosure in a patent (after issuance or publication) can provide a “roadmap” to facilitate copying or slight modifications by an unscrupulous competitor; and
- (4) the expense of detecting infringement and enforcing patent rights through litigation.

These factors illustrate the need to evaluate the subject matter carefully in order to determine whether competitors will be able easily to reverse engineer the invention and develop competing or similar products. This is especially true where the end product is freely available to the public, i.e., where competitors are free to examine all of the details of that product. As the Supreme Court wisely observed, “[i]f the invention, though still a trade secret, is put into public use, the competition is alerted to the existence of the inventor’s solution to the problem and may be encouraged to make an extra effort to independently find the solution thus known to be possible.”²¹ Such competitive pressure is of little concern where the end product is not readily adaptable to reverse engineering. For instance, trade secret protection is a popular option for protecting secret manufacturing or chemical processes, where the processes are not readily ascertainable from the end product.²²

C. Ramifications of the Trade Secret Choice and Techniques for Maximizing Intellectual Property Protection

Technology owners often wonder whether they can still obtain a patent on an invention even after they choose trade secret protection. The answer depends on whether the subject matter or end product of the invention has been published, in public use, on sale, or otherwise available to the public prior to the date that a patent application is filed. In the U.S., there is a one-year grace period for certain inventor disclosures.²³ Otherwise, this “statutory bar” applies to “commercial [exploitation by the inventor] of a machine or process . . . even if the machine or process is held secret.”²⁴ For example, suppose a company develops a secret process for producing a product (e.g., a chemical), sells that product for more than a year while holding the process as a trade secret

¹⁸ *Id.* at 490 (citations omitted).

¹⁹ Procedures for maintaining trade secret protection are discussed *infra*, at Section III.

²⁰ A general discussion of trade secret protection available in Pacific Rim countries is outlined by Sue Holloway, Comment, “Black Box” Agreements: The Marketing of U.S. Technical Know-how in the Pacific Rim, 23 CAL. W. INT’L L.J. 199 (1992).

²¹ *Kewanee Oil*, 416 U.S. at 491.

²² See, e.g., *Salsbury Labs., Inc. v. Merieux Labs., Inc.*, 908 F.2d 706 (11th Cir. 1990) (concerning vaccines); *FMC Corp. v. Taiwan Tainan Giant Indus. Co.*, 730 F.2d 61 (2d Cir. 1984) (concerning insecticides); *Johns-Manville Corp. v. Guardian Indus. Corp.*, 586 F. Supp. 1034 (E.D. Mich. 1983) (concerning a process for producing fiberglass), *amended*, 223 U.S.P.Q. 974 (E.D. Mich. 1984), *aff’d without op.*, 770 F.2d 178 (Fed. Cir. 1985).

²³ By statute, a valid patent cannot be obtained for an invention that was “described in a printed publication, or in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention,” with the exception for certain inventor disclosures that are accorded a one-year grace period. 35 U.S.C. § 102 (Supp. V 2011). It is important to note that “on sale” covers more than actual sales of the product. Offers to sell an invention may also bar the grant of a valid patent, if made outside the one year grace period.

²⁴ 2 DONALD S. CHISUM, CHISUM ON PATENTS § 6.02[5][b] (2008). This comports with the underlying policies of the statutory bars: to avoid ‘detrimental public reliance.’ When a new product or process appears publicly for a significant period of time without an assertion of patent rights, persons are justifiably led to believe that anyone may make, use or sell the product or process. The second [policy] is to encourage prompt disclosure of new useful information. The third is to discourage attempts to extend the length of the effective patent monopoly by commercially exploiting a new invention and only applying for a patent when faced with competition.

Id. § 6.02.

and then decides to seek patent protection. The statutory bar prevents the company from patenting either the product (which was in public use and on sale for more than one year) or the trade secret process (which was used to make the publicly-available product for more than one year). In any event, once a product produced by a trade secret machine or process is on sale or in public use beyond any available grace period, patent protection is no longer available—for either the product or the trade secret machine or process.

A related question is whether an owner may combine or mix trade secrets and patents to maximize protection. For instance, suppose a company develops a product, such as a rifle, and obtains a patent on the parts that go into the product. May it also protect as a trade secret the methods for manufacturing the product, i.e., the rifle?

In *Christianson v. Colt Industries Operating Corp.*,²⁵ two federal courts of appeals approved just such a course. Colt produced the M-16 rifle for the United States. Despite acquiring nine patents related to various parts of the M-16, Colt opted to maintain as a trade secret the information required to mass produce entire M-16s and make their parts interchangeable, as required by the government. Christianson argued that both Colt's patents and its trade secrets were invalid because Colt had failed to disclose the production and interchangeability data.²⁶ Both the Federal Circuit (the court responsible for hearing all patent appeals) and the Seventh Circuit firmly rejected that contention. As the Federal Circuit explained, "[p]atents are not production documents, and nothing in the patent law requires that a patentee must disclose data on how to mass-produce the invented product, in patents obtained on either individual parts of the product or on the entire product."²⁷

The owner may therefore protect "certain inventive features under patent principles and, with respect to the same general process, hold others subject to trade secret principles."²⁸ Nevertheless, when choosing to protect a product with a patent and the methods of producing that product with a trade secret, it is crucial to (1) make the proper disclosure in the patent application while (2) assuring that the application does not disclose separately protectable trade secrets. Extremely careful planning is necessary to satisfy such disclosure requirements and tread the fine line between disclosing too little, jeopardizing the patent, and disclosing more than is necessary, thus jeopardizing the trade secret.²⁹

Where subject matter is clearly patentable (i.e., category 3), an additional consideration counsels caution in choosing trade secret in lieu of patent protection. Suppose, for example, that Company A develops a clearly patentable chemical process, yet because the process is not easily reverse engineered from the resulting product, Company A opts for trade secret protection of the process. Assume several years later, after Company A has been selling the chemical products produced from the secret process, Competitor Z independently develops the process and applies for a United States patent on the process. Under United States patent law, Competitor Z could obtain such a patent.³⁰

Competitor Z, armed with the newly issued patent, now sues Company A (or Company A's customers) for infringement. Trade secret law may not protect Company A, even though it invented first, from liability for patent infringement of Competitor Z's patent.

²⁵ 822 F.2d 1544 (Fed. Cir. 1987) [hereinafter "*Christianson I*"], vacated on jurisdictional grounds, 486 U.S. 800 (1988), on subsequent appeal, 870 F.2d 1292 (7th Cir. 1989) [hereinafter "*Christianson II*"].

²⁶ 35 U.S.C. § 112 (Supp. V 2011) requires that a patent disclosure enable one skilled in the art to make and use the invention described in the claims. Additionally and independently, the inventor must disclose the best mode of working the invention known to him/her at the time of filing the patent application. These requirements ensure that "the subject matter of the claimed invention is generally in the possession of the public and ready to be reproduced following the expiration of the patent period." *Christianson II*, 870 F.2d at 1299.

²⁷ *Christianson I*, 822 F.2d at 1562.

²⁸ 2 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 9.02[4] [a], at 9-56 (2007).

²⁹ See *Wahl Instruments, Inc. v. Acvious, Inc.*, 950 F.2d 1575, 1580 (Fed. Cir. 1991):
[T]here is no mechanical rule that a best mode violation occurs because the inventor failed to disclose particular manufacturing procedures beyond the information sufficient for enablement. One must look at the scope of the invention, the skill in the art, the evidence as to the inventor's belief, and all of the circumstances in order to evaluate [the disclosure's sufficiency].
See also *Bayer AG v. Schein Pharms., Inc.*, 301 F.3d 1306, 1325 (Fed. Cir. 2002).

³⁰ See *W.L. Gore & Assocs. v. Garlock, Inc.*, 721 F.2d 1540, 1550 (Fed. Cir. 1983) ("There is no reason or statutory basis, however, on which [the first inventor's - trade secret user's] secret commercialization of a process, . . . could be held a bar to the grant of a patent to [the later inventor] on that process."), abrogated on other grounds by *Markman v. Westview Instruments, Inc.*, 52 F.3d 967 (Fed. Cir. 1995) (en banc); *OddzOn Prods., Inc. v. Just Toys, Inc.*, 122 F.3d 1396, 1402 (Fed. Cir. 1997); *Jacobson v. Cox Paving Co.*, 19 U.S.P.Q.2d 1641, 1648 (D. Ariz. 1991), *aff'd*, 949 F.2d 404 (Fed. Cir. 1991). Despite the absence of cases involving this scenario, numerous commentators have recognized this possibility under United States patent law. See generally Frank E. Robbins, *The Rights of the First Inventor Trade Secret User as Against Those of the Second Inventor Patentee (Part 1)*, 61 J. PAT. OFF. SOC'Y 574 (1979); Karl F. Jorda, *The Rights of the First Inventor Trade Secret User as Against Those of the Second Inventor Patentee (Part 11)*, 61 J. PAT. OFF. SOC'Y 593 (1979); Philip L. Burke, Note, *The 'Non-informing Public Use' Concept and its Application to Patent-Trade Secret Conflicts*, 45 ALB. L. REV. 1060 (1981).

Indeed, Company A may have express or implied indemnification obligations requiring Company A to reimburse its customers for patent infringement damages, or even costs related to the litigation. Even worse, because the invention of Company A is now disclosed in the patent of Competitor Z, Company A will likely not be able to enforce its trade secret, as it is no longer a secret.

Concerned that such an outcome is unfair, at least with respect to methods of doing or conducting business, Congress enacted the First Inventor Defense Act of 1999,³¹ which is subtitle C of the American Inventors Protection Act. The First Inventor Defense Act provides a patent infringement defense to a good faith party that, at least one year before either (a) the effective filing date of a patent or (b) the date on which the invention was disclosed to the public under the inventor exemption of 35 U.S.C. 102(b), commercially used the subject matter of that patent. Successful establishment of this defense allows Company A to continue practicing the invention, but does not invalidate the patent.³²

The risk of litigation should prompt an owner of a patentable invention such as Company A to carefully assess its choice of protection. As a practical matter, however, it may be difficult for Competitor Z to discover Company A's use and bring an infringement suit. Even if such use is discovered, Competitor Z may be averse to placing its patent in suit against Company A, who will likely mount a vigorous challenge to the validity of that patent. Moreover, Company A may implement creative approaches to limit the consequences of choosing trade secret protection over patent protection. For instance, Company A could license the trade secret or sell the secret manufacturing apparatus, with appropriate confidentiality restrictions.³³ Licensing or sale activity may persuade a court that the invention was not suppressed or concealed, and was in public use. That may invalidate Competitor Z's patent, leaving Company A free of an infringement suit and free to practice the invention.

If the expense of filing and prosecuting patent applications is not of overriding significance to the owner of the technology, one approach may be to file such applications (at least in the United States) while concurrently maintaining the secret status of the invention. Even under present law, the pending applications will remain confidential unless and until a United States patent issues, or until the patent application is published.³⁴ This time window offers an opportunity to gauge the competition, assess the likely scope of available patent protection, and better determine its value to the company, e.g., through commercialization or licensing.³⁵ If sufficiently broad protection can be obtained, if the invention appears to be commercially viable, and/or if a competitor could reverse engineer the technology, the owner could permit the United States patent to issue and enforce the patent. Alternatively, if the secret status of the invention remains intact and/or inadequate patent protection is available, the owner could abandon the application while still relying on trade secret law to protect the invention.

III. Protecting and Enforcing Trade Secrets

Assume that the owner has carefully weighed the risks and benefits of obtaining a patent or establishing trade secret protection and has decided to protect the invention as a trade secret. What must the owner do to protect and, if necessary, enforce the trade secret?

³¹ 35 U.S.C. § 273(b) (Supp. V 2011).

³² "Other countries, such as Germany and France, have solved the dilemma by legislation providing a personal right to the first secret inventor to continue using the invention for his own purposes." 2 MELVIN F. JAGER, *TRADE SECRETS LAW* § 10:3, at 10-10 (2004) (footnotes omitted).

³³ Albert C. Smith & Jared A. Slosberg, *Beware! Trade Secret Software May be Patented By a Later Inventor*, 7 *COMPUTER LAWYER* 15 (Nov. 1990).

³⁴ 35 U.S.C.A. § 122(b) (West 2001 & Supp. 2013) provides that U.S. applications will generally be published 18 months after the earliest filing date for which benefit is sought. However, the applicant may request non-publication of the application by certifying that the invention disclosed in the application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement that requires publication of applications 18 months after filing. Furthermore, nothing prevents the applicant from abandoning the application before publication and thereby preserving its secrecy. In fact, that is one reason for the 18-month delay during that delay, prosecution should advance sufficiently to let the applicant assess whether to continue pursuing a patent or rely on trade secret protection by abandoning the application.

³⁵ *Id.* Confidentiality is maintained even if no patent issues on the application or it is purposefully abandoned by the applicant. 37 C.F.R. § 1.14 (2008). In contrast to the United States application process, some other countries may not maintain a patent application in confidence, or may make public the disclosure of the patent application after a fixed length of time. See generally Patent Cooperation Treaty art. 21, June 19, 1970, 28 U.S.T. 7047, 7666-67.

A. Maintaining Secrecy

Common sense correctly suggests that protecting a trade secret centers on secrecy.³⁶ Because disclosure of a trade secret destroys its enforceability, the owner must remain constantly vigilant to protect it. For instance, if the owner's policy was previously lax enough to allow disclosure, yet stringent precautions were later implemented to protect the trade secret, some courts may still find that a trade secret is not protectable. This is not to say, however, that the owner must go to every imaginable length to protect the trade secret. The law recognizes that disclosure to licensees, co-venturers, employees and the like is often necessary to extract the commercial value of the trade secret.

Generally, the Uniform Trade Secrets Act, as well as most courts, requires only that the owner undertake protective measures "reasonable" under the circumstances. Some common types of disclosure that the owner must guard against by implementing "reasonable" protective measures include:

- (1) disclosure following "industrial espionage" type activities by unscrupulous competitors;
- (2) inadvertent disclosure occurring upon failure properly to protect the trade secret;
- (3) disclosure by key employees who leave and develop a competing enterprise, seek employment with a competitor or are induced to work for a competitor;
- (4) disclosure or misappropriation by others who are in some business relationship with the owner; or
- (5) disclosure by a government agency.

A number of techniques of varying cost, inconvenience, and efficacy exist for preventing disclosure and protecting a trade secret. As a practical matter the owner of the trade secret will exercise an amount of care corresponding to the value of the trade secret.³⁷ Nevertheless, to protect the trade secret, the owner must implement some measures—several common protective measures that courts may focus on are described below.³⁸

When choosing among these approaches, it is crucial to determine realistically the scope of the information that is truly valuable and needs to be protected. Over-protection of all information may actually cost the owner of the trade secret significantly, in direct costs associated with protecting the information and in reduced creativity of employees when overly-rigorous protections interrupt the free flow of ideas. The reasonable measures standard is not a high burden; the measures need only be reasonable under the circumstances. Requiring more stringent measures than necessary may drive up the cost of innovation, a result that is inconsistent with public policy of promoting innovation.³⁹ It is worth noting, however, that courts examine the overall balance of procedures in litigation. Very restrictive procedures in one or two areas and laxity in others may be insufficient.

1. Develop a Written Policy

Promulgating written directions reminding employees that certain data, machinery, processes or entire projects are trade secrets, and describing how employees can protect such information, may be crucial to both protecting the secret from inadvertent disclosure and enforcing trade secret rights in litigation. Written policies also provide persuasive proof of the existence and scope of trade secrets.

2. Inform Employees of Their Obligation to Protect the Company's Trade Secrets

An often crucial first step is to require employees to sign noncompetition, nonsolicitation, or nondisclosure

³⁶ *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002 (1984) ("Information that is public knowledge or that is generally known in an industry cannot be a trade secret. If an individual discloses his trade secret to others who are under no obligation to protect the confidentiality of the information, or otherwise publicly discloses the secret his property right is extinguished.") (citations omitted).

³⁷ 1 MILGRIM, *supra* note 28, § 1.04, at 1-196.

³⁸ See generally 1 MILGRIM, *supra* note 28, § 1.04, at 1-177 -1-196.

³⁹ See *United States v. Chung*, 659 F.3d 815 (9th Cir. 2011), *cert denied*, 132 S.Ct. 195 (2012); Mark L. Krotoski & Richard S. Scott, *US V. Chung—A Study of Economic Espionage*, LAW360 (Dec. 20, 2011, 12:21 PM), http://www.law360.com/technology/articles/294952?nl_pk=62b3babc-5d9a-49fd-9376-875446d815f3&utm_source=newsletter&utm_medium=email&utm_campaign=technology.

agreements (which should be carefully drafted due to enforceability issues that may vary state by state).⁴⁰ As one commentator has observed, “[a] written agreement clearly and unequivocally puts an employee or an independent contractor on notice of the trade secret owner’s claims.”⁴¹

3. Restrict or Condition Access to the Trade Secret

A guiding principle is that the owner should only distribute trade secret information on a “need to know” basis.⁴² Steps that further establish protection and may prevent disclosure include restricting access to sensitive plant or office areas, requiring nondisclosure and confidentiality agreements, or using code names for certain processes or ingredients.

4. Mark or Secure All Forms of Media in Which the Trade Secret is Stored

If the trade secret is embodied in documents, they should be stamped with an indication, such as “CONFIDENTIAL,” “PROPRIETARY INFORMATION,” or other terms indicating the nature of the document. Likewise, if the information is stored on some other media, such as a computer hard drive or other memory device, access should be restricted via passwords or by locking the computer drive. One of the new ways that employees are taking data is through online data storing sites, where workers can set up personal accounts and upload data.⁴³ Other social networks, such as Facebook, Twitter, and LinkedIn, can also be used to improperly share and/or move sensitive data. Employers need to remain savvy on how their employees can potentially move and share company data, and update their policies accordingly.

5. Take Steps to Ensure that Government Agencies to Which the Trade Secret may be Disclosed Maintain Secrecy

Various regulations—such as the Environmental Protection Act—may require the owner to disclose information that is protected by a trade secret. The owner must therefore comply with applicable procedures to inform the government that the information is protected by a trade secret to prevent disclosure while the government performs its duties, or if it receives a Freedom of Information Act (“FOIA”) request.⁴⁴ According to one commentator, one of the most damaging documented losses in this area was the EPA’s disclosure of a half-billion dollar Monsanto herbicide formula.⁴⁵ Ultimately, in *Ruckelshaus v. Monsanto Co.*,⁴⁶ the Supreme Court recognized that the EPA’s disclosure of Monsanto’s trade secrets could constitute a government “taking” of property entitling Monsanto to compensation. But Monsanto could establish a taking only by showing, among other things, that it had followed proper procedure to designate its trade secrets.⁴⁷ Accordingly, it is critical to follow proper procedures to avoid uncompensated loss of trade secrets through government action.⁴⁸

⁴⁰ Court decisions have defined narrowly the restrictions that may be imposed on an individual’s freedom to work, normally permitting only reasonable restraints that protect an employer’s “legitimate interests” while avoiding harm to either the employee or public. Accordingly, careful drafting of such agreements to comply with applicable law and to tailor the noncompetition or nonsolicitation agreement to the circumstances is crucial to later successful enforcement against a defecting employee.

⁴¹ 1 MILGRIM, *supra* note 28, § 4.02[1][c], at 4-22 (2007).

⁴² *See, e.g., Specialty Chems. & Servs., Inc. v. Chandler*, 9 U.S.P.Q.2d 1793, 1797 (N.D. Ga. 1988) (limiting access on a “need to know” basis important factor in showing secrecy).

⁴³ Erin Coe, *Employers Slow to Guard Data Amid Social Media, Tech Boom*, LAW360 (May 3, 2013, 10:11 PM), <http://www.law360.com/articles/433863/employers-slow-to-guard-data-amid-social-media-tech-boom>.

⁴⁴ 5 U.S.C. § 552 (2006 & Supp. V 2011). The FOIA mandates disclosure of public documents and records unless they fall into specified exemptions. Numerous states also have enacted similar versions of the FOIA. *See* 3 JAGER, *supra* note 35, at App. F.

⁴⁵ Monsanto’s problem is not isolated – it was reported that the EPA admitted losing “200 confidential documents containing sensitive data belonging to chemical companies, including trade-secret formulas ... worth millions of dollars.” Karen Gullo, *EPA admits to losing confidential papers from chemical firms*, CHICAGO SUN-TIMES, Nov. 14, 1996.

⁴⁶ 467 U.S. 986, 1013-14 (1984).

⁴⁷ *Id.*

⁴⁸ 2 JAGER, *supra* note 31, § 12:2, at 12-7.

B. Enforcing the Trade Secret: Identifying and Pursuing Potential Defendants

An owner may bring a trade secret suit against employees, licensees, business partners or co-venturers, or, in some situations, even third parties. The legal theories supporting these suits range from breach of an express or implied contract, breach of a fiduciary relationship, and misappropriation. A brief overview of the legal theories is provided below.

1. The Trade Secret Owner's Contractual Rights

Numerous advantages exist to having an express (preferably written) contract binding the defendant to not disclose a trade secret. For instance, a contract may delineate ownership of the trade secret, outline the precise subject matter of the trade secret, and set out remedies available upon disclosure or threatened disclosure of the trade secret. Contracts may also include restrictive covenants to prohibit the entity to which the secret is disclosed from engaging in activities that could jeopardize the trade secret or to prevent unfair competition with the owner of the trade secret. Contracts may also be used to cover disclosed material that otherwise might not be considered appropriate subject matter for trade secret protection.

Particularly where restrictive covenants are at issue, there is a potential downside to having an express agreement. Numerous courts have declared invalid agreements containing overly broad restrictive covenants, especially when those covenants applied to a former employee. Even so, properly drafted written agreements offer one of the best tools to address the many situations under which trade secrets can be disclosed.

Absent an express agreement imposing contractual obligation(s) upon a defendant, courts often have implied an obligation not to disclose a trade secret given the parties' relationship. As one commentator explains, "it is an implied obligation in every contract of employment that an employee will protect and preserve the trade secrets of his employer which are acquired in the course of employment . . . This is a duty that the employee assumes, not only during its employment but after its termination. It is an absolute and not a relative duty."⁴⁹ This "absolute duty" exists whether or not the employee signs a confidentiality or nonsolicitation agreement. Such an implied obligation may also arise in relationships other than solely employment; for example, "[l]icensees, purchasers, suppliers and members of joint ventures have similar obligations implied by law."⁵⁰

2. Misappropriation

In those jurisdictions that have adopted most or all of the Uniform Trade Secrets Act, an owner may bring an action for misappropriation upon a showing that the trade secret was

- (1) acquired by one who knew it was discovered by improper means;
- (2) disclosed or used by one who knew it was derived through another party who used improper means to acquire it or had a duty to maintain its secrecy; or
- (3) disclosed or used by one who knew it was a trade secret and that the trade secret had been acquired by accident or mistake.⁵¹

Generally, these actions require either a confidential relationship by which the trade secret was communicated (and typically arise with the defendant subsequently misappropriating the trade secret and injuring the owner) or the improper acquisition of a trade secret.⁵² The broad definition finds misappropriation upon mere "acquisition" of the trade secret, rather than disclosure or use. Improper acquisition may include illegal, fraudulent, or even legal conduct that is improper under the circumstances.

One well-publicized example occurred in the case between Starwood Hotels and Hilton, in which Starwood

⁴⁹ 2 JAGER, *supra* note 31, § 6:2, at 6-3 (2002) (quoting *L.M. Rabinowitz & Co. v. Dasher*, 82 N.Y.S.2d 431, 435 (Sup. Ct. 1948)).

⁵⁰ *Id.* § 4:1, at 4-8.

⁵¹ See UNIF. TRADE SECRETS ACT, § 1 (amended 1985), 14 U.L.A. 537-38 (2005).

⁵² Courts may sometimes characterize an obligation as either an implied contractual duty or a confidential relationship. This characterization may be important in terms of the type of relief available to the trade secret holder—a breach of confidential relation may sound as tort whereas a breach of a contractual duty is a contract action. See generally 1A MILGRIM, *supra* note 27, at §§ 4.02-4.03. For a general overview of the type of damages available in trade secret suits, see Michael A. Rosenhouse, Annotation, *Proper Measure and Elements of Damages for Misappropriation of Trade Secret*, 11 A.L.R.4th 12 (1982 & Supp. 2005).

accused Hilton and two of its previous executives hired by Hilton of stealing documents containing Starwood's competitively sensitive information relating to the Starwood W hotel chain. The case settled with Hilton making a reported \$75 million payment to Starwood and with the two executives restricted from working at certain hotel companies for two years.⁵³

The case illustrates that it can be crucial to enjoin both ex-employee(s) and the competitor, and to collect damages from both. Action against the competitor is a possibility if the competitor had notice that the information was a trade secret and that the ex-employee's disclosure was a breach of an obligation imposed by an express or implied contract.⁵⁴ On the other hand, if a company hires a competitor's key employee, it should document the fact that the new employee is being hired for his or her skills rather than knowledge of the competitor's trade secrets and instruct the new employee in writing not to use the competitor's trade secret.

In other instances, misappropriation occurs even though the trade secret is disclosed by accident.

The inevitable disclosure doctrine limits key employees with sensitive company knowledge (i.e., about technical and/or strategic secrets) from leaving one company to join a competitor. If recognized by the particular court deciding the case, the doctrine may allow an employer to use trade secret law to enjoin a former employee from working in a new job that would inevitably result in the use of the employer's trade secrets, even where there is no evidence of an actual disclosure.⁵⁵ States are split in their application of the doctrine. Some have found inevitable disclosure and enjoined employment; some have rejected the doctrine outright;⁵⁶ some seek to narrow its application, particularly in the absence of a non-competition agreement; while others have required bad faith on the part of the employee.

IBM v. Papermaster is an example of a high profile case where a New York court took a broad view of the inevitable disclosure doctrine and allowed an employer the use the inevitable disclosure doctrine to enjoin employment.⁵⁷ During the time that Mark Papermaster was employed by IBM, he learned some of IBM's most sensitive information. He then accepted a position at Apple, where he would report to Mr. Jobs. The court granted IBM's request for a preliminary injunction, finding that because Papermaster had been inculcated with some of IBM's most sensitive and closely-guarded technical and strategic secrets, it was not a great leap to find that IBM met its burden of showing a likelihood of irreparable harm if Papermaster was to continue his employment at Apple. "[I]t is likely that Mr. Papermaster inevitably will draw upon his experience and expertise in microprocessors" which he gained at IBM "and which Apple found so impressive, to make sure that the [new Apple products] are fitted with the best available microprocessor technology and at a lower cost."⁵⁸ The Court clarified that it was not suggesting that Papermaster had intentionally acted dishonorably or with ill-will, simply that the likely inevitability of even inadvertent disclosure is sufficient to establish a real risk of irreparable harm to IBM.⁵⁹ Papermaster has reportedly settled the case with IBM, with the requirement that he make scheduled court appearances to testify that he will protect IBM trade secrets.⁶⁰

Misappropriation can also be found when a competitor uses industrial espionage activities, some of which may be legal, to discover the trade secret. Thus, "[t]he law also protects the holder of a trade secret against disclosure or use when the knowledge is gained, not by the owner's volition, but by some 'improper means . . . which may

⁵³ Peter Lattman, *Hilton and Starwood Settle Dispute*, NYTIMES.COM, (Dec. 22, 2010, 4:39 PM), <http://dealbook.nytimes.com/2010/12/22/hilton-and-starwood-settle-dispute/>.

⁵⁴ See *Metallurgical Indus., Inc. v. Fourtek, Inc.*, 790 F.2d 1195, 1204 (5th Cir. 1986) ("The law imposes liability not only on those who wrongfully misappropriate trade secrets by breach of confidence but also, in certain situations, on others who might benefit from the breach.").

⁵⁵ *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262 (7th Cir. 1995) (a case in which a high-level manager at PepsiCo, with knowledge of its marketing, promotional, and pricing strategies, left to join a rival drink company and was enjoined from taking the new employment).

⁵⁶ For example, in *Holton v. Physician Oncology Servs., LP*, No. S13A0012, 2013 WL 1859294 (Ga. May 6, 2013), the Georgia Supreme Court held that Georgia law does not recognize the inevitable disclosure doctrine as an independent cause of action for trade secret misappropriation; see also *LeJune v. Coin Acceptors, Inc.* 849 A.2d 451 (Md. Ct. App. 2004); *Del Monte Fresh Produce Co. v. Dole Food Co.*, 148 F. Supp. 2d 1326 (S.D. Fla. 2001); *Gov't Tech. Servs., Inc. v. IntelliSys Tech. Corp.*, 51 Va. Cir. 55 (Cir. Ct. 1999); *Standard Brands, Inc. v. Zumpe*, 264 F. Supp. 254 (E.D. La. 1967).

⁵⁷ *IBM v. Papermaster*, No. 08-CV-9078 (KMK), 2008 U.S. Dist. LEXIS 95516 (S.D.N.Y. Nov. 21, 2008).

⁵⁸ See *id.* at *18.

⁵⁹ See *id.*

⁶⁰ Tim Beyers, *Big Blue Is Watching You, Apple*, THE MOTLEY FOOL (January 30, 2009), <http://www.fool.com/investing/general/2009/01/30/big-blue-is-watching-you-apple.aspx>.



include theft, wiretapping, or even aerial reconnaissance.”⁶¹

IV. Conclusion

Maintaining an edge over competitors may depend to a great extent on choosing the right intellectual property protection. Legal counsel may help assess the legal environment framing the decision to select between patent and trade secret protection. Ultimately, however, the owner must decide after considering the relevant business, as well as legal, factors.

⁶¹ *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 475-76 (1974) (internal citation omitted).