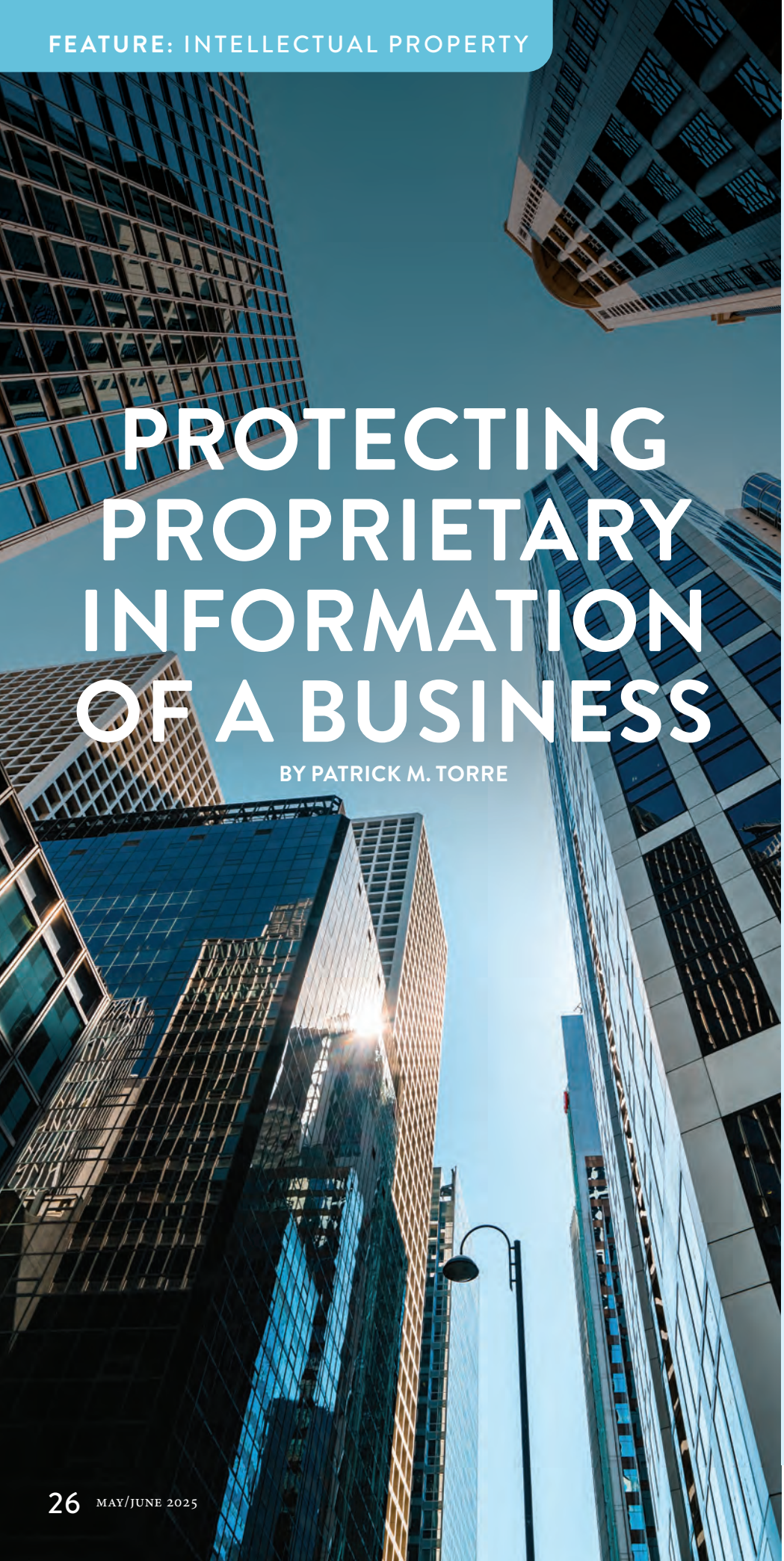

PROTECTING PROPRIETARY INFORMATION OF A BUSINESS

BY PATRICK M. TORRE

Patent, trademark, and copyright most immediately come to mind when the topics of protection of intellectual property (IP) and proprietary business information are raised. However, alternative protection schemes are available which if properly utilized can be as, if not more, important to many business owners and which indeed may be turned to for protection even when more traditional methods of IP protection are not available or appropriate.

TRADE SECRETS

One such mechanism to protect proprietary information is trade secret protection. Trade secrets are an often overlooked type of intellectual property which can be as or more important to a business as are patents, trademarks, and copyrights. Trade secrets provide no exclusivity to the owner. However, unlike other forms of IP protection, trade secrets maintain their value indefinitely when properly protected. Specific definitions of "trade secret" vary but the core requirements for a trade secret are that: 1) it is information that is in fact kept secret; 2) the information derives actual or potential economic value to a business from that secrecy; and 3) reasonable efforts made by the business to maintain that secrecy.

Stated differently, as the name implies a trade secret is any information that provides a competitive business edge, and which derives its true economic value to a business from not being generally known by others. Trade secrets can include formulas/formulations, data/databases, industrial processes, laboratory notebooks, technical know-how, blueprints, computer software that cannot lawfully be reverse engineered, training manuals, supplier identity, pricing/financial information, customer lists, and others. It is important to note that trade secret status, once established, provides protection only against misappropriation, i.e., improper acquisition and/or use of the information by others. Third parties may discover a trade secret by fair means such as by independent discovery, permissible disclosure by another, reverse engineering, or by other lawful means.

PROTECT BUSINESS PROPRIETARY INFORMATION/TRADE SECRETS

Many businesses are unaware of the broad scope of information, in-house procedures, etc., that can and should be protected as trade secrets and fail to take the needed steps to protect their rights in the first place. Businesses must take early and ongoing steps to identify sensitive business information such as by conducting periodic audits. Once proprietary information of a business has been identified, consideration should be given to how to best protect that information. In general, it is wise to implement a company-wide practice of compartmentalizing, i.e., restricting access to potentially sensitive or confidential information exclusively to employees who require access to such information to perform their duties. If the information is not appropriate for traditional intellectual property protections and has been kept secret, trade secret protection may be appropriate.

Businesses must clearly communicate the importance of preserving trade secrets to existing, new and prospective employees, such as by clearly spelled-out provisions addressing trade secrets in employment agreements. In addition, employers must be diligent in reminding soon-to-be former employees of their ongoing duty to maintain trade secret confidentiality in exit interviews, and in requiring such employees to sign Employee Separation Agreements or Termination Statements listing business information known to the employee to be trade secrets and acknowledging the employee's obligation to maintain the proprietary nature of the trade secrets.

Businesses should also consider requiring employees and new hires, particularly those who will require or may have access to sensitive business information/trade secrets while performing their duties, to sign non-disclosure agreements (NDAs) as a condition of employment. A well-drafted NDA addresses at least the following points:

- Who are the parties to the NDA? In this situation the parties are typically the employer and the employee/new hire.
- What information is deemed to be sensitive, confidential or proprietary? Is all information disclosed to the employee deemed confidential or only information so marked? Does the information have to be specifically marked "Confidential" to fall under the scope of the NDA? Is the confidentiality restricted to written disclosures, or is orally disclosed information also subject to confidentiality provisions? If confidential information is to be disclosed orally, what are the specifics of how the confidentiality of the information is conveyed? Conventionally, oral information can be deemed confidential if the employer confirms in writing to the receiving party that the information is confidential. The NDA should clearly delineate how confidential information is to be identified by the employer.
- The NDA should clearly define the obligation of the receiving party to: 1) keep the disclosed confidential information a secret; and 2) take reasonable steps to prevent access to the confidential information by third parties.
- What is excluded from the obligation of confidentiality? Typically information is excluded if it is: 1) already known to the recipient; 2) already public information, as long as the recipient was not the person who disclosed the information to the public; 3) independently developed by the recipient without use of the confidential information of the employer; 4) disclosed to the recipient by a third party who has no obligation of confidentiality to the employer; or 5) disclosed by the recipient as a requirement of a legal process.
- What is the term of the agreement? While certainly the employer would like the NDA to remain in force forever, this must be balanced against the reality that courts do not view perpetual obligations favorably and in any event most information has a limited shelf life. The "reasonable" term for an NDA will vary by industry, although 2 to 5 years is common.

Other clauses important to a well-drafted NDA may include: specifying jurisdiction, *i.e.*, in what court(s) can action be brought in to enforce the NDA; specifying availability of injunctive relief to the employer to stop a breaching act rather than solely relying on monetary damages after the act has occurred; and specifying that the disclosure of information by the employer does not in any way represent a transfer of any rights to the employee.

WHAT IF BUSINESS PROPRIETARY INFORMATION/TRADE SECRETS HAVE BEEN MISAPPROPRIATED?

Causes of action for trade secret misappropriation are available under a wide range of common law, state law, and federal law sources:

Common law tort/unfair competition. Prior the development of the Uniform Trade Secrets Act "UTSA" (see below), improper use or disclosure of a trade secret was traditionally a common law tort. There are three fundamental elements to a trade secret tort claim:

(1) The subject matter involved must qualify for trade secret protection. U.S. courts widely adopted basic

principles of trade secret law that were set forth in 757 and 758 of the Restatement of Torts (1939). In particular, § 757, comment b, listed six factors to be considered in determining whether information constitutes a trade secret: 1) The extent to which the information is known outside the claimant's business; 2) the extent to which it is known by employees and others involved in the business; 3) the extent of measures taken by the claimant to guard the secrecy of the information; 4) the value of the information to the business and its competitors; 5) the amount of effort or money expended by the business in developing the information; and, 6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

(2) The holder of the subject matter must establish that reasonable precautions were taken to prevent disclosure of the subject matter.

(3) The trade secret holder must prove the information was misappropriated or wrongfully taken, that is, where it is acquired through improper means, or where the acquisition involves a breach of confidence. Section 43 of the Restatement (Third) of Unfair Competition describes improper acquisition of trade secrets as; acquiring another's trade secrets by fraud, theft, unauthorized interception of communications, inducement of or knowing participation in a breach of confidence, and other means wrongful in themselves. Section 41 of the Restatement states that a duty of confidence is owed by a person whom a trade secret has been disclosed if 1) an express promise of confidentiality was made prior to disclosure, or 2) the person knew or had reason to know the disclosure was intended to be in confidence, and the disclosing party was reasonable in inferring that the person consented to an obligation of confidentiality. Section 44 provides for the award of injunctive relief to prevent a continuing or threatened appropriation of another's trade secret. Section 45 provides that one who is liable to another for misappropriation of the other's trade secret is liable for monetary relief caused by the misappropriation or for the actor's own pecuniary gain resulting from the misappropriation.

UNIFORM TRADE SECRETS ACT (UTSA) OF 1985. Forty-eight states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted some version of the UTSA, with state-to-state distinctions that require careful consideration. State courts generally have jurisdiction over UTSA claims, but standalone UTSA claims can be filed in federal court if diversity jurisdiction requirements are met. Civil remedies for trade secret misappropriation under UTSA include injunctive relief, payment of reasonable royalties for continued future use, and monetary damages such as plaintiff's lost profits and costs to enforce potentially including attorney's fees, defendant's unjust enrichment and profits resulting from the misappropriation, and punitive damages in appropriate circumstances.

ECONOMIC ESPIONAGE ACT (EEA) OF 1996.[1] EEA is primarily directed to industrial espionage, is the first federal law criminalizing trade secret misappropriation, and imposes criminal sanctions relating to theft or misappropriation of trade secrets. One provision of this legislation criminalizes misappropriation of trade secrets with the knowledge or intent that the theft would benefit a foreign power (economic espionage), providing for imposing fines (up to $5,000,000) and prison sentences of up to 15 years. Another provision of EEA imposes criminal penalties for the misappropriation of trade secrets related to or included in a product that is produced for or placed in interstate or international commerce with the knowledge that the misappropriation would injure the owner of the trade secret (commercial theft), and provides for fines (up to $250,000) and prison sentences of up to 10 years.

SECTION 337 OF THE TARIFF ACT OF 1930[2] provides a mechanism for trade

secret owners to file trade secret misappropriation claims at the U.S. International Trade Commission (ITC). The statute prohibits unfair trade/unfair competition in importation and sale of imported articles. The ITC is authorized to issue Exclusion Orders to stop importation of products that harm U.S. industry and are made using misappropriated trade secrets. Relief can be granted even if acts of misappropriation take place outside the U.S. Monetary damages are not provided for.

DEFEND TRADE SECRETS ACT (DTSA) OF 2016.[3] DTSA is a more recent civil cause of action that allows uniform nationwide application in Federal court to address trade secret misappropriation. DTSA standing exists only where the trade secret is "related to a product or service used in, or intended for use in, interstate or foreign commerce.[4] DTSA does not replace the UTSA or preempt state law, but provides a parallel right for filing trade secret misappropriation lawsuits in federal court if "the trade secret is related to a product or service used in … interstate or foreign commerce."[5] A three-year statute of limitations tolls from the date on which the misappropriation was, or by the exercise of reasonable diligence should have been, discovered.[6]

Misappropriation under DTSA requires wrongful acquisition of a trade secret and also wrongful use or disclosure of a trade secret. This is the acquisition of a trade secret by a person who knows or has reason to know that the acquisition was made by improper means, followed by the use or disclosure of the trade secret by one who: (1) used improper means to acquire the secret; or (2) knew or had reason to know that the secret was: (a) derived from a person who used improper means to acquire it; (b) acquired under circumstances giving rise to a duty to maintain its secrecy; or (c) derived from or through a person who owed a duty to the owner to maintain its secrecy.[7]

Many key definitions of DTSA are derived from UTSA, with a few important differences. "Improper means" under DTSA includes "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.[8] Lawful means of acquisition such as reverse engineering, independent derivation, and others are expressly excluded from the definition of "improper means."[9] An "owner" of a trade secret under DTSA includes the legal owner, an equitable title holder, and a licensee of the trade secret owner.[10]

DTSA provides for immunization from liability under federal and state law for certain disclosures of trade secret information,[11] including: disclosures made in confidence to a federal, state, or local government official, or to an attorney solely for the purpose of reporting or investigating suspected violations of law (whistleblower safe harbor); disclosures made in a complaint or other document filed under seal in a lawsuit or other proceeding; and disclosures to an attorney or in a court proceeding by an individual who files a lawsuit alleging employer retaliation for reporting a suspected violation of law, as long as court filings are under seal and the individual does not otherwise disclose a trade secret except pursuant to a court order.

There are also key provisions in DTSA relating to employees. Employers are required to provide notice of DTSA's immunity from disclosure provisions in any contract or agreement with an "employee" (traditional employees, independent contractors, and consultants[12]) relating to use of trade secrets or other confidential information. Alternatively, the employer can in a nondisclosure agreement reference a policy document provided to employees and setting forth a formal reporting policy for suspected violations of law.[13] DTSA notice requirements apply only to contracts/agreements entered into after May 11, 2016.[14]

Civil remedies available under DTSA are similar to those of UTSA. However, DTSA limits injunctive relief available to employers. An injunction preventing an employee from entering into an employment relationship must be based on evidence of threatened misappropriation, not merely on information that the person possesses. DTSA bars injunctive relief that would otherwise conflict with state law prohibiting restraints on the practice of a lawful profession, trade, or business. Ex parte civil seizures of property are available under DTSA when necessary to prevent the dissemination of a misappropriated trade secret,[15] but only in "extraordinary circumstances" such as a defendant expected to attempt to flee the country or not otherwise subject to enforcement of a U.S. court's order.

SUMMARY

Businesses are often unaware of the broad scope of proprietary information that can and should be protected as trade secrets, and fail to take the needed steps to protect their rights. Businesses should as a regular practice clearly establish the importance of trade secrets to new and prospective employees, as well as to departing or soon-to-depart employees. Periodic audits to identify confidential business information including trade secrets, reviewing procedures put in place to preserve trade secret confidentiality, and putting NDAs in place to discourage misuse of such information by employees and/or third parties are great investments in a business's future! B&B

ABOUT THE AUTHOR

PATRICK M. TORRE is a registered patent attorney in Stites & Harbison, PLLC's Intellectual Property & Technology Services Group, Lexington office, and is admitted to practice law in Kentucky and before the U.S. Patent and Trademark Office. His practice focuses on intellectual property protection strategy, including counseling clients on issues of infringement, validity, and patentability, patent drafting, prosecution, and appellate proceedings, trademark prosecution, trade secrets and transfer, and intellectual property licensing. Prior to entering the practice of law, he worked in academic research in the areas of life sciences, biotechnology, immunology, and nutrition.

ENDNOTES

1 *18 U.S.C. §1831.*
2 *19 U.S.C. §1337.*
3 *18 USC §1836 et seq.*
4 *18 U.S.C. §1836(b)(1).*
5 *18 U.S.C. §1836(c).*
6 *18 U.S.C. §1836(d).*
7 *18 U.S.C. §§1839(5)(A), 1839(5)(B).*
8 *18 U.S.C. §§1839(6)(A).*
9 *18 U.S.C. §1839(6)(B).*
10 *18 U.S.C. §1839(4).*
11 *18 U.S.C. §1833(b).*
12 *18 U.S.C. §1833(b)(1)(A).*
13 *18 U.S.C. §1833(b)(1)(B).*
14 *18 U.S.C. §1833(b)(1)(D).*
15 *18 U.S.C. §1836(b)(2) et seq.*