WHAT'S REASONABLE?—PROTECTING AND ENFORCING TRADE SECRETS IN THE DIGITAL AGE

Prepared for AIPLA 2016 Spring Meeting

BY:
JEANNE M. GILLS
FOLEY & LARDNER[1]

On May 11, 2016, President Obama signed into law the Defend Trade Secrets Act of 2016 ("DTSA") bringing one of the most common and prevalent forms of intellectual property protection onto the national stage. By providing a company with a private cause of action in federal court for trade secret misappropriation, the DTSA put trade secrets on par with other well-known intellectual property ("IP") assets such as copyrights, trademarks, and patents. Even with its most controversial provision of allowing *ex parte* seizures in extraordinary circumstances, the Act enjoyed widespread bi-partisan support and, for many, was a long time coming.[2]

The importance of trade secrets and IP assets generally to the American economy and the need to ward against theft has been recognized in both the public and private sectors. It has been estimated that up to 75% of the value of U.S. Fortune 500 companies is attributable to intangible assets, including trade secrets and other IP.[3] In a 2013 Report by the Commission on the Theft of American Intellectual Property, they observed:

> The effects of [IP] theft are twofold. The **first** is the tremendous loss of revenue and reward for those who made the inventions or who have purchased licenses to provide goods and services based on them, as well as of the jobs associated with those losses. ... The **second** and even more pernicious effect is that illegal theft of intellectual property is undermining both the means and the incentive for entrepreneurs to innovate, which will slow the development of new inventions and industries that can further expand the world economy and continue to raise the prosperity and quality of life for everyone.[4]

---

[1] The views expressed in this article are those solely of the author and do not necessarily reflect the views of the firm, Foley & Lardner, or any of its other attorneys or clients.

[2] The bill (S. 1890) passed the Senate 87-0 and the House 410-2. *See* https://www.congress.gov/bill/114th-congress/senate-bill/1890/actions

[3] "*Reasonable Steps*" *To Protect Trade Secrets Leading Practices in an Evolving Legal Landscape*, Report by CREATE.org (2015), available at http://www.tradesecretsinsider.com/wp-content/uploads/sites/323/2015/07/Reasonable-Steps.pdf.

[4] The IP Commission, *The Report of the Commission on the Theft of American Intellectual Property* (May 2013), available at www.ipcommission.org/report/IP_Commission_Report_052213.pdf (emphasis added).

The Commission estimated that the American economy suffered annual losses caused by trade secret theft to the tune of $300 billion, which is comparable to the annual level of U.S. exports to Asia. Likewise, the same Report found that trade secret theft accounted for the loss of over two million American jobs annually and impeded and undermined the incentive to innovate.[5]

Protecting trade secrets has also become more challenging in the digital age given: technological innovations; pervasive use and access to "smart" devices; the ease at which data can be downloaded, copied and transferred; and increased employee mobility. Those challenges are often compounded by inconsistency in the courts given that trade secret owners have mostly pursued their claims in state courts under varying state statutes and in venues where courts and jurors see complex technical cases less frequently. While 48 of the 50 States have adopted some form of the Uniform Trade Secrets Act ("UTSA"), the interpretation of key provisions often varies and leads to differing results depending on the jurisdiction, including on such key issues as: what constitutes a "trade secret"; what constitutes "misappropriation"; and did the trade secret owner employ "reasonable efforts" to maintain the secrecy of the trade secret. One of the goals of the DTSA therefore is to bring uniformity to trade secret laws and to provide litigants with more guidance on protection and enforcement.

The aim of this article is to explore some of the DTSA's key provisions and to ponder whether the DTSA will aid in providing more clarity on what federal courts will require in trade secrets cases, particularly as to what they will deem "reasonable efforts" given the current landscape.

The DTSA's Key Provisions

The DTSA was signed into law by President Obama on May 11, 2016 and went into immediate effect. It passed the Senate and the House of Representatives on April 11 and April 27, 2016, respectively. It applies to any act of trade secret misappropriation occurring on or after the date of enactment. The DTSA amends the Economic Espionage Act of 1996 ("EEA," 18 U.S.C. § 1831 *et seq.*) to provide a civil remedy for misappropriation of trade secrets. Specifically, new § 1836(b) allows a trade secret owner to bring a civil action in federal court if the trade secret is related to a product or service used in, or intended to be used in, interstate or foreign commerce. As a result, litigants can now more easily pursue trade secret misappropriation claims in federal court. Previously, civil claims were only available under state law, and hence many suits were filed in state court (unless federal jurisdiction was met another way, *e.g.*, diversity or supplemental jurisdiction).[6]

---

[5] *Id.*

[6] Such federal supplemental jurisdiction was also at risk if a related federal claim was dismissed. *See Koninklijke Philips N.V., et al. v. Elec-tech Int'l Co., Ltd.*, 2015 U.S. Dist. LEXIS 35285 (N.D. Cal. Mar. 20, 2015) (holding plaintiff could not use the Computer Fraud and Abuse Act ("CFAA") to bring trade secret claims in federal court where the plaintiff had argued an indirect access or agency theory between an insider with access to trade secrets and an outsider without access which the court found didn't suffice to prove a hacking claim under CFAA; to do so, the court found would federalize all trade secret claims where a computer was used to download the confidential or trade secret information).

While a company could lobby federal prosecutors to bring federal criminal charges under the EEA, such actions were more rare. New § 1836(c) also provides that district courts shall have original jurisdiction of civil actions brought under the DTSA.

The DTSA has several key provisions directed to: (i) harmonizing or unifying existing trade secret law; (ii) remedies, most significantly ***seizures***, in addition to injunctive relief (that cannot unfairly restrain employee mobility), monetary damages, enhanced damages, and attorneys' fees; (iii) providing notice to worker of immunity from trade secret disclosure in certain instances as precursor to recovering enhanced damages and attorneys' fees from that worker; and (iv) no preemption (*e.g.*, state law claims can still be brought).

- **Uniformity**

Of the fifty States, all but two (New York and Massachusetts) have adopted or modified some form of the "UTSA." However, there remains variance among each State, including how the UTSA has been interpreted, and on the key dispositive issues of: what constitutes a "trade secret"; what constitutes "misappropriation"; and whether a party has taken "reasonable efforts or safeguards" to protect or maintain the trade secret. The DTSA's creation of a private right of action should lead to development of more uniformity among the federal courts on how its provisions are interpreted and provide more certainty to litigants. The DTSA's definitions of "misappropriation" and "improper means" are essentially identical to those definitions as used in §§ 1(1) and 1(2) of the UTSA and was an apparent attempt to still have the current body of law provide guidance in future proceedings.

- **Remedies—Now Includes Seizures**
  - **Seizures**

The DTSA's most controversial provision includes the ability to seek a civil seizure for trade secret misappropriation. New § 1836(b) authorizes a federal court to issue an order in extraordinary circumstances and upon an *ex parte* application (based on a sworn declaration or verified complaint) to provide for seizure of property where necessary to preserve evidence or prevent dissemination of the trade secret. Subsection A(ii) lists requirements for issuing a seizure order and such an order is not available if an injunction under the existing Fed. R. Civ. P. would suffice. An example of when a seizure order is appropriate is where the defendant is seeking to flee the country or is planning to disclose the trade secret to a third party immediately or is otherwise not amenable to enforcement of the court's orders. In the legislative history, it notes that: "it is the Committee's expectation that the courts will require applicants to describe the trade secret that would be the subject of [seizure] the order with sufficient particularity so that the court may evaluate the request."

Indeed, subparagraph (B) of the new § 1836(b)(2) delineates all the requirements of the seizure order, including: setting forth findings of fact/conclusions of law; providing for the narrowest seizure necessary to protect the trade secret and minimizing interruption to the business operations of third parties (and the legitimate operations of

the target (where possible); protecting the seized property from disclosure; preventing applicant's access to the seized property; providing guidance to law enforcement effecting the seizure (*e.g.*, hours to perform and whether force can be used); setting a hearing date at the earliest possible time (but not later than 7 days after order issued); and the applicant providing a security.

Subparagraph (C) of the new § 1836(b)(2) requires that the court take appropriate action to protect the target of the seizure order from publicity by or at the behest of the applicant regarding the order or any seizure under the order.

The DTSA acknowledges that seizures may encompass electronically stored information ("ESI") and therefore allows for the use of independent experts and special masters appointed by the court to identify and protect the trade secrets. Additionally, the DTSA provides that the target of a seizure has a private right of action against the applicant if the target suffers damages from a wrongful or excessive seizure, and such recovery is not limited to the amount of the security put up by the applicant.

Proponents of this provision noted that seizures are available under the Copyright and Lanham Acts and were necessary here to give more teeth to trade secret enforcement. Notably, the DTSA balances the interests of both the trade secret owner and the accused defendant by making such a seizure available only in "extraordinary" circumstances and where narrowly tailored and many other requirements are met.

- **Additional Remedies**

The DTSA (§ 1836(b)(3)) provides for additional remedies, including: (i) injunctive relief; (ii) monetary damages; (iii) enhanced damages; and (iv) attorneys' fees.

Regarding injunctions (drawn from § 2 of the UTSA), the DTSA cannot be used to prevent a person from entering into an employment relationship or otherwise conflict with applicable state laws prohibiting restraints on trade. Any injunction (and employee restrictions therein) must be narrowly tailored to prevent actual or threatened trade secret misappropriation and not be based solely on what information that employee knows. Section (3)(A)(i)(1)(I) reinforces the importance of employee mobility and hence, the DTSA is not a back-door mechanism to get a non-compete provision. These provisions were designed to avoid any federal expansion of the inevitable disclosure doctrine, which many States reject or minimally highly disfavor, *e.g.*, California, Colorado, Louisiana, Maryland, and Virginia. Hence, in some cases, a state law claim for trade secret misappropriation against a former employee may be preferred over a DTSA claim in those States that have applied the inevitable disclosure doctrine at least in some contexts, *e.g.*, Arkansas, Connecticut, Delaware, Illinois, Massachusetts, Minnesota, North Carolina, Pennsylvania, and Utah.[7]

[7] *See* R. Wiesner, "A State-By-State Analysis of Inevitable Disclosure: A Need for Uniformity and a Workable Standard," *Marquette Intellectual Property Law Review*, vol. 15, iss. 1, art. 2, available at http://scholarship.law.marquette.edu/cgi/viewcontent.cgi?article=1187&context=iplr.

Regarding monetary damages (§ 1836(b)(3)(B), drawn from § 3 of the UTSA), the DTSA specifies that the court may award damages for the actual loss and any unjust enrichment caused by the trade secret misappropriation, or alternatively an award of a reasonable royalty. Enhanced damages (of up to two times the amount of monetary damages) and attorneys' fees and are also available where the misappropriation was "willful and malicious." *See* § 1836(b)(3)(C) and (D) (akin to §§ 3(b) and 4 of the UTSA).

The DTSA also provides the accused defendant with a potential award for attorneys' fees upon showing that there was "bad faith" in bringing the trade secret claim or where a motion to terminate an injunction was opposed in "bad faith." *See* § 1836(b)(3)(D).

- **Additional Provisions**

The DTSA includes other key noteworthy provisions. New § 1836(d) provides for a three-year period of limitations on which a claim may be brought, which is identical to the UTSA (although some States have modified this provision).

Subsection 2(f) of the Act clarifies that the DTSA also does not preempt any other state trade secret laws, nor does it affect any lawful disclosure under FOIA.

Subsection 3(a) of the Act amends § 1832(b) (in the context of criminal violations) to provide for a maximum penalty to be the greater of $5,000,000 or three times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided.

Section 4 of the Act requires, not later than one year after the date of enactment of the Act and biannually thereafter, the Attorney General to provide a report, in consultation with the Intellectual Property Enforcement Coordinator, the Director of the Patent & Trademark Office, and the heads of other appropriate agencies, to the Committees on the Judiciary of the Senate and the House, on theft of trade secrets occurring abroad.

Subsection 7(a) of the Act amends § 1833 to provide whistleblower immunity from liability for confidential disclosure of a trade secret to the Government or an attorney for reporting or investigating a suspected legal violation, or in a filing under seal in a judicial proceeding. The DTSA further provides that an "employer shall provide notice of the immunity" relating to lawful disclosures "in any contract or agreement with an employee that governs the use of a trade secret or other confidential information." Employers can comply with this requirement by cross-referencing another policy document provided to the employee regarding the employer's reporting policy for a suspected violation of law. Additionally, the DTSA ties the ability to collect enhanced damages or attorneys' fees against that employee in a private cause of action to providing notice of the immunity. "Employee" also includes any individual working as a contractor or consultant.

Reasonable Efforts To Protect Trade Secrets

To be protectable as a trade secret, a plaintiff must prove that the trade secret is information that derives economic value (actual or potential) because it is not generally known and that such information is the subject of reasonable efforts to maintain its secrecy. Often the toughest aspect of a plaintiff's trade secret action is proving that the trade secret was the subject of "reasonable efforts" to maintain its secrecy. The secrecy requirement has been shown or fulfilled in many ways, including by:

- Restricting access to the information (*e.g.*, locking it away in a secure place such as a vault or via computer or network security);
- Limiting the number of people who know the information;
- Having the people who know, or who come into contact with the trade secret, directly or indirectly, agree in writing not to disclose the information (*e.g.*, sign non-disclosure agreements (in the case of third parties) or confidentiality or employment agreements (in the case of employees and consultants/contractors)); and/or
- Marking any written material pertaining to the trade secret as confidential and proprietary and following up (as practical) in writing if verbal disclosure.

• Components Of An Effective Trade Secret Policy

"Reasonable efforts" to maintain such secrecy often starts with a defined or understood intellectual property policy and protection strategy. Components of an effective trade secret policy or program can include:

- Mechanisms to identify, assess, and manage trade secret assets and any risks of trade secret theft;
- Appointment of the right people to develop the procedures;
- Making sure internal and third party agreements (*e.g.*, those noted above) are in place;
- Conducting trade secret procedures, both internal procedures (*e.g.*, that addresses employment practices, physical and data security, and confidentiality program and records managements) and for external collaboration (*e.g.*, collaboration with third parties);
- Developing and implementing the procedures, including monitoring, auditing, and taking of corrective actions as needed;
- Educating employees, contractors, and consultants;
- Extending physical and network/computer security; and/or

- Enforcing it (*e.g.*, have enforcement/response plans, incorporate procedures in employee code of conduct, and have consistent enforcement).

However, it is not necessary to have all such components in place, and a court will typically examine the specific facts of the case, the nature of the trade secrets at issue, and even the type or size of the business.[8]

Courts across the country have analyzed a serious of factors in assessing whether such reasonable efforts have been demonstrated.[9] For example, courts will look to the level of physical and computer security[10], whether the trade secret is provided in discrete parts or shared as a whole[11], whether copies have been restricted or marked as confidential, and the use of agreements (with insiders and third parties) to maintain confidentiality and/or limit competition.[12]

- **Reasonable Safeguards With Insiders And Outsiders**

With employees and in-house contractors or consultants, a multi-pronged approach may be needed, including: issuing ID badges to employees and contractors and limiting access to certain areas based on type of badge; having employees and

---

[8] For example, a smaller company may meet "reasonable efforts" standards with fewer requirements. *Elm City Cheese Co. v. Federico*, 1999 Conn. LEXIS 369 (1999) (within small family-owned company, reasonable efforts satisfied where trade secrets shared only among family members and accountant and where plaintiff "kept confidential enough information to make it virtually impossible for its employees to use the rest of the information constituting its trade secret.").

[9] *See, e.g., Paramount Tax & Acc't, LLC v. H&R Block Eastern Enterprises, Inc.*, 2009 Ga. App. LEXIS 912, *17 (Ga. 2009) (customer list deemed a trade secret where it was company policy not to publish its client list, company had established company-wide policies to protect information from disclosure to third parties and had educated employees on the policies; company also limited access to customer database to certain employees; and information was password protected); *Wyeth v. Natural Biologics, Inc.*, 395 F.3d 897 (8th Cir. 2005) (despite defendant's arguments that visitors toured facility with no signed confidentiality agreements, lack of posted confidentiality signs, non-marked confidential documents were unsecured, and that not all employees signed confidentiality agreements, court said "[a]bsolute secrecy is not required," and instead relied on fact that there was lack of repeated losses of confidential information regarding the Brandon Process, company's use of physical security, limited access to confidential information, employee training, and both oral and written understandings of confidentiality).

[10] *See U.S. v. Howley*, 707 F.3d 575 (6th Cir. 2013) (Goodyear used multiple physical security mechanisms to protect trade secrets associated with its steel-reinforced tires, including fences, requiring permission to visit premises, passing visitors through security checkpoints and requiring them to sign confidentiality agreements, and preventing use of cameras).

[11] *See Otis* Elevator *Co. v. Intelligent Systems Inc.*, 17 U.S.P.Q.2d 1773, 1775 (Conn. 1990) (third party did not receive critical data nor source code).

[12] *See, e.g., Aetna, Inc. v. Flugel*, 2008 Conn. Super. LEXIS 326, *14 (Conn. 2008) (though permanent injunction premised on alleged "inevitable disclosure" was denied, court noted with approval Aetna's employee nondisclosure agreements and related secrecy efforts, *e.g.*, marking of documents as confidential, annual review of confidentiality obligations, and use of passwords and encryption technology); *Delcath Systems, Inc. v. Foltz*, 2007 Conn. Super. LEXIS 101, *4-5, 16 (Conn. 2007) (though court ultimately found that the defendant did not misappropriate any trade secrets, the court referred to plaintiff's efforts to maintain secrecy as "scant," where no aspect of defendant's employment with plaintiff included any confidentiality or trade secret obligations in any agreement, and plaintiff did not produce any evidence that it had any company policies or standards regarding trade secrets or the confidentiality of company information).

contractors sign employee, confidentiality and/or non-compete agreements; alerting employees and contractors of what information the company considers confidential/trade secrets and how the information should be treated; conducting both entrance and exit interviews wherein certain procedures are carried out; making employees aware of company policies and issuing periodic reminders; and reinforcing the importance of the company's overall IP and the need to respect the IP rights of others. A key component is limiting access to those insiders who truly need to know the trade secret information.[13] The importance of rigid exit procedures, including obtaining the return of company issued documents and equipment and reminding the departing employee (often the defendant in a trade secret misappropriation case) of his/her duties to the company has been observed by a few courts.[14]

Likewise, the trade secret owner must take due care with outsiders, including visitors to the company as well as potential business partners. Reasonable efforts may consist of limiting visitor access to certain areas, requiring the signing of confidentiality and NDA agreements, marking documents as confidential and proprietary, limiting or restricting what can leave the company's premises, restricting copies, and precluding the use of cameras or other recording equipment. In a recent case, a Texas jury awarded over $48.7 million (disgorging the defendant's profits) where plaintiff successfully prevailed on its trade secrets claim against a potential business partner upon showing breach of an NDA and the defendant's misappropriation. In *Texas Advanced Optoelectronic Solutions,* the case involved failed merger talks in the light sensor market and highlighted the necessity of using confidentiality agreements even in preliminary business negotiations where trade secrets are at stake.[15]

Courts have also been reluctant to dismiss a plaintiff's trade secret claim at the complaint stage where the plaintiff has made some showing of reasonable efforts.[16]

---

[13] *See U.S. v. Zhang,* No. 13-0143 (9th Cir. Nov. 5, 2014) (9th Cir. held there was sufficient evidence beyond reasonable doubt that Marvell took "reasonable steps" to protect its trade secrets by advising users of the existence of trade secrets, **limiting access to need to know basis**, and controlled access to passwords).

[14] *See, e.g., Agilent Tech., Inc. v. Kirkland et al.,* 2010 Del. Ch. LEXIS 34 (2010) (court found that Agilent used "commercially reasonable procedures" to protect its trade secrets including use of exit procedures where departing employees reminded of confidentiality obligations and duties to Agilent and were required to sign a "Functional Exit Interview Memo"); *PatientPoint Network Solutions, LLC v. Contextmedia, Inc.,* 2014 U.S. Dist. LEXIS 37443 (S.D. Ohio March 21, 2014) (TRO denied due to lack of reasonable efforts where: employee was not required to sign confidentiality/non-compete agreement until one year after he started and one month before his termination; other employees with access to trade secrets did not sign confidentiality agreements; no written request to employee to return company issued laptop/iPad or other company trade secret information; TRO was also denied despite extensive forensic evidence showing employee had repeatedly downloaded trade secrets on flash drives after termination).

[15] *See Texas Advanced Optoelectronic Solutions, Inc. v. Intersil, No. 4:08-cv-451 (E.D. Tex. Mar. 6, 2015).*

[16] *See, e.g., ABB Turbo Systems, AG v. TurboUSA, Inc.,* 774 F. 3d 979 (Fed. Cir. 2014) (reversed district court's dismissal of a trade secrets complaint for failure to alleged "reasonable" efforts where ABB's allegations (*e.g.,* use of confidentiality and NDA agreements, prohibiting reproduction and dissemination of trade secrets, restricting physical and electronic access to third parties) were sufficient at complaint stage); *Schroeder et al. v. Pinterest Inc. et al.,* 2015 N.Y. App. Div. LEXIS 7173 (N.Y. Oct. 6, 2015) (complaint sufficiently pled trade secrets claim against former fiduciary Cohen and reasonable efforts over four years to develop technology and keep it confidential; however, claim against Pinterest

Given the federal courts' recent emphasis on pleading standards following the Supreme Court's decisions in *Twombly* and *Iqbal*[17], it will be interesting to see if claims filed under the DTSA will have to meet any pleadings standards that exceed those required by many courts applying state-based UTSA law. At least one district court in *TE Connectivity Networks* declined to apply the *Iqbal* standard to a party's trade secrets claim under Minnesota law, apparently suggesting that a more lenient pleading standard was appropriate in such cases. There, the court observed that a trade secret plaintiff is "understandably hesitant to reveal [in its complaint] the exact parameters of the trade secrets it believes have been misappropriated because a trade secret made public is not a secret."[18] It is particularly anticipated that in those cases where the trade secret owner is seeking an *ex parte* seizure order under the DTSA, that the trade secret will need be set forth in greater detail, which some courts have already insisted upon even in the absence of a request for injunctive relief.[19]

In some cases, it may be more advantageous for the trade secret owner to pursue its claim solely in state court where proving that the stolen information actually qualifies as a trade secret or was the subject of reasonable efforts may be difficult and thus hard to maintain federal jurisdiction. Yet, the information might qualify as "confidential information" under state law for which there was a breach of an underlying agreement to preserve confidentiality. Such was the case in *Orthofix*, where the Sixth Circuit reversed the district court's ruling on Orthofix' contract claim finding that employee Hunter breached his non-disclosure/non-compete agreement by using and disclosing confidential information that did not necessarily qualify as a trade secret. The court nonetheless found it was confidential information under Texas law that did not require finding such information was also a trade secret in order for Orthofix to prevail.[20] As also noted above, state law trade secret claims against former employees may also be desirable in those jurisdictions that have recognized the inevitable disclosure doctrine and enjoined such employees from taking certain employment even in cases where no non-compete agreement even existed. With claims pursued under the DTSA, it is anticipated that such employee injunctions will be more rare, or where allowed even more narrowly tailored.

---

could not stand where no contractual relationship existed and no evidence that Pinterest obtained the trade secrets through improper means where Pinterest only knew that the idea given to it was not Cohen's own).

[17] *See Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007); *Ashcroft v. Iqbal*, 556 U.S. 662 (2009).

[18] *See TE Connectivity Networks, Inc. v. All Systems Broadband, Inc.*, No. 13-1356 (D. Minn. Mar. 31, *2016*) (court denied defendant's MTD finding that "*Iqbal* and *Twombly* do not require particularity to such an extent; they only require plaintiff to allege facts which make a claim plausible on its face"; instead, court found that complaint allegations were "not generalized or conclusory" and found more than a "mere possibility of misconduct").

[19] *See, e.g., Tucson Embedded Sys., Inc. v. Turbine Powered Tech. LLC,* 2016 U.S. Dist. LEXIS 44696 (D. Az. Mar. 31, 2016) (court granted defendant's summary judgment motion where plaintiff failed to provide detail about its alleged trade secrets ("parameters and settings, including timing, temperatures, flow rates, horsepower settings, pressures"); didn't reach issue of reasonableness of efforts); *Big Vision Private Lt'd v. E.I. DuPont de Nemours & Co.*, No. 11-cv-08511 (S.D.N.Y. Mar. 3, 2014) (court granted summary judgment in favor of defendant where there was a finding of no misappropriation but also where Big Vision had failed to describe its trade secrets with particularity and its definition of its trade secrets changed) (*aff'd* Case No. 14-976, 2nd Cir., May 21, 2015).

[20] *See Orthofix, Inc. v. Hunter,* 2015 U.S. App. LEXIS 20111 (6th Cir. Nov. 17, 2015).

- **Reasonable Safeguards With Computer Systems/Electronically Stored Information**

Courts will also look to how the company manages its computer systems or electronically stored information or data, particularly if the nature of the trade secrets taken are those that are stored electronically. Most companies have numerous systems, including for ESI: file servers; email servers; desktops; laptops; portable electronic devices; and portable drives and media (*e.g.*, thumb drives, CDs). Each system should be part of an IP protection strategy, where there is a balance between ease of operation and security. In addition, the company should have a social media policy that is also consistent with its IP protection strategy.

As an initial matter, for trade secrets that are stored on such systems, there should be limited and/or restricted access using passwords or encryption technologies.[21] Passwords should be changed periodically and be complex and not easily discoverable. Likewise, there should be restricted permissions that encompass items such as: disabling copy and printing functions; disabling ability to install programs and applications; limiting access to internet mail, FTP and public ports; and segregating access to sensitive information. The company's IT department should also have the ability to track or log computer activity, including any suspicious activity or heavy download traffic. Additionally, the company should maintain updated virus protection suite and spam filters. It is also advisable to have a policy against the transfer of files onto personal computers (unless certain protections are in place) and to restrict or limit the use of portable or flash drives. Again, such security measures only have to be reasonable, and simply because some employee password protected computers might occasionally be left on will not outweigh a company's overall reasonable efforts to maintain secrecy.[22]

In today's work environments, the use of "smart" devices is pervasive and many companies have defined Bring Your Own Device (or "BYOD") policies. Such smart device use and BYOD policies should also be consistent with the company's overall IP protection strategy, namely where the company is involved in managing copies of files, managing email access, and requiring that appropriate security measures be implemented. For companies with such policies, when dealing with departing employees, the company should have the ability to conduct a forensic examination of any devices for those employees with access to sensitive company trade secrets.[23]

---

[21] *See nClosures Inc. v. Block & Co., Inc.,* No. 13-3906 (7th Cir. Oct. 22, 2014) (Seventh Circuit affirmed the district court where plaintiff did not make additional efforts to have individuals who access the designs at issue sign confidentiality agreements, keep the designs under lock and key, or store the designs on a limited-access computer; Court thus found that nClosures did not engage in "reasonable steps" to protect the confidentiality of its designs).

[22] *See Cellular Accessories for Less Inc., v. Trinitas LLC,* 2014 U.S. Dist. LEXIS 130518 (C.D. Cal. Sept. 16, 2014) (court denied defendant's motion for summary judgment regarding contact information including LinkedIn contacts, despite argument that plaintiff didn't take reasonable efforts to maintain secrecy where while Cellular argued it used layers of passwords and SSL encryption but where defendant argued that employee computers were generally left on and unprotected).

[23] *See Agilent, supra.*

The increased use of social media to drive business development may also lead to increased claims being pursued under the DTSA and arguments by companies of their substantial investment in such efforts and attendant reasonable efforts to maintain confidentiality given the value of social media in driving revenue. For example, in *CDM Media*, the court denied in part defendant's motion to dismiss finding that social media membership lists (LinkedIn) may qualify as trade secrets where former employee transferred control of a LinkedIn group allegedly owned by CDM and used it in competition with CDM.[24] Given the federal courts' greater familiarity with IP claims arising in new media contexts, this case may be cited in future instances where companies argue substantial investment of resources and value in business development through social media.[25]

- **Reasonable Safeguards Regarding Monitoring And Enforcement**

An IP protection strategy is only effective if it is adhered to. There should be scheduled and systematic review of key aspects of the IP protection strategy and audits to ensure insider and third party compliance. There should also be monitoring and corrective actions taken as needed. Likewise, the policy should be enforced. The company needs to act quickly and not sit on its hands and send written demands (especially if a former employee joins a competitor that offers the same or similar products and services), and be prepared to file suit or report criminal activities to the authorities.

At the end of the day, the law requires reasonable precautions, not extraordinary precautions, nor absolute secrecy.[26] Such efforts will not be deemed reasonable if they unduly hamper the operations of the business. However, risk increases as standards are lowered. An effective strategy should focus on information leaking to third parties, managing any departing or disgruntled employees, and preventing unwanted confidential third party information being brought to your company.

[24] *See Cellular Accessories, supra*.
[25] *See CDM Media USA, Inc. v. Simms*, 2015 U.S. Dist. LEXIS 37458 (N.D. Ill. Mar. 25, 2015).
[26] *See Wyeth, supra.*