What's Reasonable? Protecting And Enforcing Trade Secrets

AIPLA 2016 Spring Meeting
May 19, 2016

Jeanne M. Gills

AIPLA
American Intellectual Property Law Association
Serving America's Legal and Creative Community

FOLEY
FOLEY & LARDNER LLP

Agenda

- Trade Secrets—Overview
- Economic Espionage Act of 1996
- Defend Trade Secrets Act of 2016
- Reasonable Efforts to Maintain Secrecy
- Components of An Effective Trade Secret Program
- Recent Trade Secrets Cases
- Patent vs. Trade Secret Protection?

Trade Secrets—Overview

Trade secret information is: (1) information*; (2) that derives economic value (actual or potential) because it is not generally known; and (3) that is the subject of reasonable efforts to maintain its secrecy.

Duration

- Indefinitely, as long as you can keep it a secret!

- Once it's disclosed, it's not a trade secret anymore

*** Comprising all types of financial, scientific, technical, engineering, or other forms of information.**

Examples of Trade Secrets

- Opinions
- Technical Reports
- Technical data (such as the result of tests)
- Negative know-how (knowledge that certain approach does not work)
- Product blueprints, plans and drawings
- Computer software
- Algorithms
- Database compilations
- Manufacturing processes or techniques
- Designs and patterns
- Customer lists
- Social Media contacts (*e.g.*, LinkedIn contacts)
- Market predictions, analyses or forecasts
- Formulas
- Recipes
- Pricing or financial information
- Business strategies
- Business opportunities

Trade Secret Protection

- Rights in trade secrets are **now** provided under **federal law**, **state law**—by statute (*e.g.*, Cal. Civil Code §§ 3426-3426.11; the Uniform Trade Secrets Act ("UTSA") has been adopted or modified in some form in 48 states), or **common law** (*e.g.*, legal decision; still the law in New York)
- No registration system for trade secrets
- Applicable Federal Law
  - Defend Trade Secrets Act of 2016, amending 18 USC § 1831 *et seq*.
  - Economic Espionage Act of 1996, 18 USC § 1831 *et seq*. (previously only criminal law)

Economic Espionage Act of 1996: Overview*

- EEA made trade secret misappropriation a federal crime. However, it was not intended to criminalize every theft of trade secrets for which civil remedies existed under state law. Discretionary factors under § 1831 or § 1832 include:
  - scope of the criminal activity, including evidence of involvement by a foreign government, foreign agent or foreign instrumentality;
  - degree of economic injury to the trade secret owner;
  - type of trade secret misappropriated;
  - effectiveness of available civil remedies; and
  - potential deterrent value of the prosecution.
- 18 U.S.C. § 1831 (Economic espionage): Criminalizes the misappropriation of trade secrets (including conspiracy to misappropriate trade secrets and the subsequent acquisition of such misappropriated trade secrets) with the knowledge or intent that the theft will benefit a foreign power. Penalties are fines of up to $5 Million and imprisonment of up to 15 years for individuals, and fines not more than $10 Million (or three times the value of stolen trade secret) for organizations.
- **18 U.S.C. § 1832 (Theft of trade secrets)*:** Criminalizes the misappropriation of trade secrets related to or included in a product that is produced for or placed in interstate (including international) commerce, with the knowledge or intent that the misappropriation will injure the trade secret owner. Penalties are fines and imprisonment for up to 10 years for individuals and fines of up to $5 Million for organizations.
- 18 U.S.C. § 1833 (Exceptions): Provisions do not apply to lawful activity by government entities, or to the reporting of any suspected violation of law to any such entity.

*** Pre-May 11, 2016 Amendments**

EEA: Overview—cont'd*

- 18 U.S.C. § 1834 (Criminal forfeiture): Requires criminal forfeiture of any proceeds of the crime and property derived from proceeds of the crime, and any property used, or intended to be used, in commission of the crime.
- 18 U.S.C. § 1835 (Confidentiality orders): Provides that the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets.
- 18 U.S.C. § 1836 (Civil proceedings): Authorizes civil proceedings by DOJ to enjoin violations of the Act, but no private cause of action (*e.g.*, victims or putative victims must work with the U.S. Attorney to obtain an injunction). Districts courts have exclusive original jurisdiction.
- 18 U.S.C. § 1837 (Extraterritorial): For conduct outside of the U.S., there is extraterritorial jurisdiction where:
  - The offender is a U.S. citizen or permanent resident; or
  - The offender is an organization organized under U.S. laws; or
  - An act in furtherance of the offense was committed in the U.S.
- 18 U.S.C. § 1838 (Preemption): Act does not affect any other civil or criminal laws with respect to trade secret misappropriation or affect the otherwise lawful disclosure of information by any government employee under the Freedom of Information Act ("FOIA").
- 18 U.S.C. § 1839: Includes various definitions.

*** Pre-May 11, 2016 Amendments**

Defend Trade Secrets Act Of 2016 ("DTSA")

- Signed into law (S. 1890) by President Obama on May 11, 2016. (Passed Senate (87-0) and House (410-2) on April 11 and April 27, 2016, respectively.) ***Effective for acts of misappropriation occurring on or after May 11, 2016.***
- **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. 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.
- **Litigants can now more easily pursue 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). A company could lobby federal prosecutors to bring federal criminal charges under the EEA though such actions were more rare. New § 1836(c) also provides that district courts shall have original jurisdiction of civil actions brought under DTSA.

DTSA—cont'd

- 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).
- Does DTSA provide enough teeth to deal with cybersecurity—perhaps the biggest and fastest growing threat to trade secrets?

DTSA: Brings Uniformity

- Of the 50 States, all but two (New York and Massachusetts) have adopted 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 courts on how its provisions are interpreted and provide more certainty to litigants. The definitions of "misappropriation" and "improper means" are defined essentially identically to those definitions as used in §§ 1(1) and 1(2) of the UTSA.
- Goal of DTSA is to incentivize future innovation while protecting and encouraging the creation of intellectual property and in turn more American jobs.

DTSA: Seizures Available in Extraordinary Circumstances

- DTSA provides the right to seek a civil seizure for trade secret misappropriation, the Act's most controversial provision. (Seizures are available under the Copyright and Lanham Acts.)
- 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."

DTSA—Seizures cont'd

- 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 do and whether force may 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.
- 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.
- DTSA also 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.

DTSA: Additional Remedies

- 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 the 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 may States reject.

DTSA: Additional Remedies—cont'd

- § 1836(b)(3)(B): Regarding monetary damages (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.
- § 1836(b)(3)(C) and (D): 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* §§ 3(b) and 4 of the UTSA.)
- § 1836(b)(3)(D): 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."

DTSA: Other Provisions

- Statute of Limitations: 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).
- Preemption: Subsection 2(f) of the Act clarifies that 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**.

DTSA: Other Provisions—cont'd

- Subsection 7(a) of the Act amends § 1833 to provide whistleblower immunity from liability for confidential disclosure of a trade secret either 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 Maintain Secrecy

"Secrecy" is Required to Maintain a Trade Secret

Ways to Protect Trade Secrets

- Restrict access to the information (*e.g.*, lock it away in a secure place, such as a vault or via computer/network security)
- Limit the number of people who know the information
- Have the people who know, or who come in contact with, the trade secret, directly or indirectly, agree in writing not to disclose the information (*e.g.*, sign non-disclosure agreements or confidentiality agreements)
  - Employee agrees to confidentiality as part of Employment Agreement with appropriate provisions; third parties and business contacts sign NDAs
- Mark any written material pertaining to the trade secret as confidential and proprietary and/or follow-up in writing if verbal disclosure

Risks of Losing Trade Secret Protection

- When are your trade secrets at greatest risk?
  - Departing employees
  - Failed business dealings
  - Corporate espionage
  - Estimated that over 85% of trade secret thefts are by someone known to the trade secret owner (*e.g.*, insiders, employees, business partners, etc.)*

*** D. Almeling *et al.*, *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 Gonz. L. Rev. 291, 295 (2010)**

Components of an Effective Trade Secret Program

- Identify, assess, and manage trade secret assets and any risks of trade secret theft
- Appoint the right people to develop procedures and include people responsible for information management/IT
- Conduct 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)
- Make sure internal and third party agreements are in place
- Develop and implement the procedures, including monitoring, auditing, and taking of corrective actions as needed
- Extend physical and network/computer security
- Educate and train employees, contractors, and consultants
- Enforce it (*e.g.*, have enforcement/response plans, incorporate procedures in employee code of conduct, and have consistent enforcement)

Identify And Assess Your IP Assets & Risks

- Document your IP assets in the event there is a later dispute
  - Ownership
  - Development
  - Value
- Consider multiple forms of IP protection for key IP assets
  - Federally registered IP rights
  - Trade Secrets
- Review possible avenues of unauthorized access to your IP
  - Documents and filing systems
  - Facilities such as offices, manufacturing plants
  - Computer systems and Email
  - Employees
  - Third Parties–business partners, contractors, consultants, vendors, visitors

Reasonable Safeguards—General

- Overall Corporate Policy
  - ***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)
- Business Dependent
  - Smaller company may meet 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.")

Reasonable Safeguards—General

- Proprietary information, systems, technologies or documents may warrant individual protections
  - Restricted Physical Access
    - Locked doors, building security guards, electronic sensors, cameras, access passes
    - ***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)
  - Providing access only to discrete parts, not the whole or use of "Black Box" procedures
    - ***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)
  - No copies or restricted copies
    - Mark confidential, proprietary
  - Documents and technology do not leave premises
  - Manufacture and maintain secret components internally
  - Employee and third party confidentiality agreements

Reasonable Safeguards—Employees

- Issue ID badges to employees and contractors
- Employee, Confidentiality and Non-compete Agreements
  - Alert employees and contractors of what information company considers confidential/trade secrets and how the information should be treated
  - Have employee and independent contractor also sign an invention assignment agreement. Employer can consider additional consideration to sign any invention assignment agreement for employees who are not at will.
  - ***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)

Reasonable Safeguards—Employees (cont'd)

- Entrance Interview
  - Importance of IP to company
  - Respect IP of others and instruct employee not to bring information or material belonging to another company (*e.g.*, consider having employee sign a statement to that effect)
- Exit Interview
  - Documented reminder regarding confidentiality and any non-compete agreements
  - Return of all company issued/owned devices and files–paper, electronic, USB drives
    - ***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")
    - *See also* ***PatientPoint Network Solutions****, infra*
  - Deletion of all company documents, emails and personal copies
  - Audit employee activities, including prior trade secret access–file access, email

Employee Education

- All employees
  - Employees cannot adhere to IP protection strategy unless they are made aware of it
  - Can be tailored based on level of access to confidential information
  - Give periodic reminders as appropriate, particularly during any merger, acquisition, or sale talks
- Recurring
  - Should be reinforced on a regular basis
- Reinforce importance of IP to the company
  - Company's IP
  - Respect other's IP

Reasonable Safeguards—Computer Systems

- Most companies have numerous systems:
  - File Servers
  - Email Servers
  - Desktops
  - Laptops
  - Portable Electronic Devices
  - Portable Drives and Media (*e.g.*, thumb drives, CDs)
- Each system must be part of an IP protection strategy
  - Balance between ease of operation and security
  - Need Social Media policy that is also consistent with IP protection strategy

Protections of Computer Systems

- Limited Access
  - Usernames and passwords
    - Complexity of password
    - Periodic changes in password
    - ***Cellular Accessories for Less Inc., v. Trinitas LLC***, 2014 U.S. Dist. LEXIS 130518 (C.D. Cal. Sept. 16, 2014) (court denied defendant's MSJ 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)
  - Restricted Permissions
    - Disable copy and printing functions
    - Disable ability to install programs and applications
    - Access to internet mail, ftp and public ports
    - Segregate access to sensitive information
  - Logs of computer activity
- Updated virus protection suite and spam filters

Laptops and Portable Drives

- Policy against files being transferred to personal computers
  - Remote desktop, Citrix™, or other service to access files remotely
  - Use of company-issued laptops only
- Restrict use of Portable drives
  - Highly problematic because high capacity and very small
  - Review logs of portable drives being mounted and files being copied–ensure that all copies of the files are accounted for

Portable Electronic Devices

- Smartphones and Tablets
  - Company issued vs. personal devices—necessary to have defined BYOD (Bring Your Own Device) policy
  - Managing copies of files
  - Managing email access
  - Requiring security measures be implemented
    - Passwords
    - Tracking if lost
    - Remote deletion
  - Return and/or forensic examination upon employee departure

Audits

- IP protection strategy is only effective if adhered to
- Routine
  - Scheduled and systematic review of all aspects of IP protection strategy
- Ensure insider and third party compliance

Enforcement

- Prompt enforcement actions
  - Letter to former employee and new employer
  - Need to act quickly and not sit on hands
  - Lawsuit
  - Report criminal activities to the authorities

At the end of the day . . .

- The law requires reasonable precautions, not extraordinary precautions, nor absolute secrecy
- Not reasonable if unduly hampers operations of the business
  - But risk increases as standards are lowered
- Your 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

Recent Decisions In Trade Secret Protection

- ***Tucson Embedded Sys., Inc. v. Turbine Powered Tech. LLC,*** 2016 U.S. Dist. LEXIS 44696 (D. Az. Mar. 31, 2016) (court granted defendant's MSJ 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)
- ***Zylon Corp. v. Medtronic, Inc..,*** *2016 N.Y. App. Div. LEXIS 1564* (N.Y. Mar. 3, 2016) (triable issue of fact raised as to existence of a trade secret where agreement was in place and evidence that trade secret was provided under "duty of confidence" and where defendant gave "assurances")
- ***Orthofix, Inc. v. Hunter,*** 2015 U.S. App. LEXIS 20111 (6th Cir. Nov. 17, 2015) (Reversed DCT's ruling on Orthofix' contract (non-disclosure/non-compete) claim finding that Hunter breached agreement by using and disclosing confidential information that did not necessarily qualify as a trade secret; contract claim under Texas law did not require finding that information was a trade secret in order for Orthofix to prevail)
- ***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 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)

Recent Decisions—cont'd

- ***InnoSys, Inc. v. Mercer,*** 2015 Utah LEXIS 226 (Utah Aug. 28, 2015) (court reversed SJ in favor of Mercer where undisputed that trade secrets were disclosed in connection with unemployment benefits claim and to her personal unsecure gmail account and that Mercer had signed NDA; court disagreed with lower court finding that such disclosures (and any future disclosures) created no presumption of irreparable harm to InnoSys even where Mercer had deleted the trade secret information; also reversed grant of attorneys' fees to Mercer)
- ***CDM Media USA, Inc. v. Simms,*** 2015 U.S. Dist. LEXIS 37458 (N.D. Ill. Mar. 25, 2015) (court denied in part defendant's MTD, 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; case may be cited in future instances where companies argue substantial investment of resources and value in business development through social media)
- ***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)

Recent Decisions—cont'd

- ***Texas Advanced Optoelectronic Solutions, Inc. v. Intersil,*** No. 4:08-cv-451 (E.D. Tex. Mar. 6, 2015) (case involved failed merger talks in light sensor market and illustrates necessity of using confidentiality agreements in preliminary business negotiations where trade secrets are at stake; jury awarded $48.7M to TAOS on trade secrets claim (disgorgement of defendant's profits) and also found defendant willfully infringed TAOS patent; in a subsequent April 22, 2016 Order, the court denied TAOS' request for permanent injunction but did order parties to negotiate reasonable royalty on TAOS' patent claim, not trade secrets claim, since damages award at trial compensated TAOS on the trade secrets claim)
- ***NanoMech, Inc. v. Suresh,*** No. 13-3671 (8th Cir. Feb. 6, 2015) (aff'd DCT where non-compete was overbroad given broad restriction on activities (*e.g.*, that would prevent employee from working in any capacity for any nanotechnology company in the world) and lack of geographic limitations)
- ***ABB Turbo Systems, AG v. TurboUSA, Inc.,*** 774 F. 3d 979 (Fed. Cir. 2014) (reversed DCT'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)
- ***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; court also found intent to reap economic benefit from trade secret misappropriation sufficient to sustain criminal conviction under 18 U.S.C. § 1832)

Recent Decisions—cont'd

- ***nClosures Inc. v. Block & Co., Inc.,*** No. 13-3906 (7th Cir. Oct. 22, 2014) (aff'd DCT 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, the court found that nClosures did not engage in "reasonable steps" to protect the confidentiality of its designs)
- ***Cellular Accessories for Less Inc., v. Trinitas LLC,*** 2014 U.S. Dist. LEXIS 130518 (C.D. Cal. Sept. 16, 2014) (whether and to what extent LinkedIn contacts are trade secrets; denied summary judgment on issue of trade secret misappropriation under California Uniform Trade Secrets Act where material facts in dispute)
- ***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 termination; other employees with trade secret access did not sign confidentiality agreements; no written request to employee to return company issued laptop/iPad or other company trade secret information; TRO was denied despite extensive forensic evidence showing employee had repeatedly downloaded trade secrets on flash drives after termination)

Patent vs. Trade Secret?

- Shelf-life of innovation? Will the innovation be useful beyond twenty years, or less than two?
- Is it possible for the innovation to be reverse-engineered?
- Is the innovation detectable and embedded in a product, or is innovation a part of an internal manufacturing/testing process?
- Is the innovation likely soon to be independently discovered?
- Does company have a high turnover among its employees?
- Are confidentiality procedures or other security measures difficult to implement?
- Is the innovation a business method or computer software implemented invention?

Advantages of Patent Protection

- **Patents avoid the need to maintain complete security for innovations that would otherwise be required for trade secret protection.**
- Patents deter competitors from implementing claimed features within their products.
- Patents allow for relief if others independently develop the same innovation—along with broader scope of protection.
- Patents can deter competitors from filing patent infringement suits, and also can be used in cross-licensing (*e.g.*, for settlement or other negotiations).

Advantages of Trade Secret Protection

- Unlimited duration—trade secrets could potentially last longer than patents (20 years) and copyrights
- Protection is theoretically worldwide
- "Absolute Bar" to protecting outside U.S.
- No application required
- No registration costs
- No public disclosure or registration with government agency
- **Effective immediately**
- Value of lead time/avoidance of early publication
- No *Alice v. CLS Bank*, 134 S. Ct. 2347 (2014) concern or risk of parallel PTAB proceeding

Questions?

JEANNE M. GILLS, PARTNER

VICE CHAIR, INTELLECTUAL PROPERTY DEPARTMENT

FOLEY & LARDNER LLP

321 North Clark, Suite 2800

Chicago, Illinois 60654

(312) 832-4583 / jmgills@foley.com