SEYFARTH SHAW

The Growing Importance of Trade Secrets in Protecting Emerging Technology

Presented by:
Robert B. Milligan

What Will Be Covered.

01 Increasing Reliance on Trade Secrets to Protect Cutting Edge Technologies

02 *Waymo v. Uber* and Other Key Cases: Lessons Learned

03 How the New U.S. Federal Trade Secrets Law Helps Trade Secret Owners

04 Best Practices: Avoiding “Bet-the-Company” Trade Secret Litigation, Managing Onboarding and Offboarding with Continual Training Component

Increasing Reliance on Trade Secret Protection

Patent vs. Trade Secret Protection

- Patent vs. trade secret for cutting edge technologies
- Patents: popular because they give holders a monopoly

  - Patents may be available for compounds, products, methods of manufacture, commercial applications of product candidates, and even packaging
  - BUT patents often focus on end product, and leave out highly useful information
    - As a result, companies may lose out on opportunities to produce new IP

Why Trade Secret Protection?

- Trade secrets: more prevalent in recent disputes
  - A good option when the secret is not patentable, e.g. background scientific information
    - Patents are only available for certain types of truly novel inventions
  - Applicable to cutting edge technology where obsolescence will precede the issuance of a patent, and competitiveness depends on reaching the market first
    - Trade secret protection may continue indefinitely
      - … as long as the protected material meets the definition of a “trade secret”

Why Trade Secret Protection?

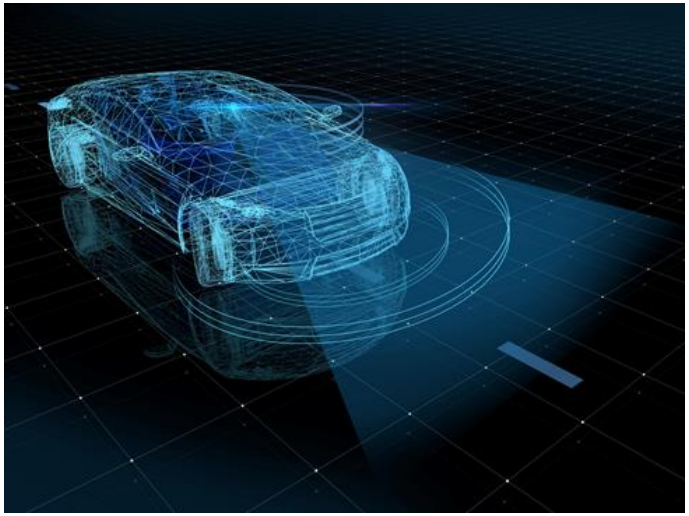
- Cheaper than other forms of IP that require formal registration
  - Trade secret owners need only incur the costs of keeping the information secret (e.g. securing facilities and nondisclosure agreements is enough)
  - Patents are significantly more expensive

- Covers any information that derives value from not being generally known; use or knowledge by others does not necessarily preclude protection

- International “open innovation” trade secret laws may be advantageous to smaller firms and individual inventors, allowing them to protect shared information and partner with larger companies and SMEs

Waymo v. Uber: Lessons Learned

- High-level employee developing self-driving car tech at Waymo
- Employee left, created his own self-driving truck company, and sold it to Uber
- Waymo sued and got an **injunction** against employee working on self-driving technology and essentially, for Uber to fire him
- There was also a federal criminal referral



Waymo v. Uber: Lessons Learned

- Why spend over $500M without knowing whether Waymo trade secrets were involved?
  – Did Uber really look at what came up in the third party "due diligence room"?

Waymo v. Uber: Lessons Learned

- Who can fall prey to trade secret theft? Any employer, even the most sophisticated of companies

- In California, anything goes? Not!
  - Trade secret owners can get **injunctions**
    - Combat data theft with the ability

    to get a more robust injunction

Loop AI Labs: When the CEO Leaves

- CEO/President at artificial intelligence startup was fired
- CEO (allegedly) provided proprietary information through “advisory services” for competing startups during her employment
- CEO (allegedly) took a concurrent CEO position at Almawave USA, a competing artificial intelligence company

Meta v. Zhong: Theft of Augmented Reality Technology

- Employee heavily involved in developing VR headset at Meta
- Employee left Meta and founded DreamWorld
- Dreamworld announced its first product, a VR headset
- Meta sued for theft of trade secrets

Agilent: Theft of DNA Synthesis Technology

- Employee resigned from Agilent in 2013
- That year, rival company Twist received $4.7M in funding and applied for patents for a device to synthesize DNA using inkjet technology
  - Did Twist create the technology between the time of its founding and the time of filing?
- Recent ruling: trade secret claims do *not* preempt breach of loyalty claims under the California Uniform Trade Secrets Act ("CUTSA")

Zhang: Code Theft from Global Financial Services Firm

- Computer engineer was charged with stealing proprietary algorithms for trading models
  - Employer protected source code with encryption keys
  - Employee had access to the company computer system
  - Employee accessed parts of the system without authorization

- Employer alerted law enforcement
  - Maximum sentence of 10 years
  - Maximum fine of $250,000 or twice the gross gain/loss from the offense

A Note about IP in the Gaming Industry

- In 2016, the global computer game market reached over $100B and the industry is on track to continue growing
- IP protection is crucial for game companies of all sizes
- Options:
  - Copyright can protect the literal source code and object code, and aspects of the structure, sequence, and organization of the software
    - **BUT: many aspects are not protectable, risks when hiring programmers**
  - Trademark can protect the game's name and promotional materials
    - **BUT: take care not to infringe other marks in the process**
  - Patent can protect the underlying technology used in software engines and tool kits, as well as hardware and distribution platforms
    - **BUT: significant expense involved, infringement may be hard to detect**
  - Trade secrets can protect other key components or methods involved

How the New U.S. Federal Trade Secrets Law Helps Trade Secret Owners

- Before the DTSA:
  - No federal civil cause of action available to private litigants for trade secrets misappropriation
  - No basis for federal court jurisdiction in civil actions without diversity jurisdiction or some other hook
  - Inconsistencies and differences between state laws

The Defend Trade Secrets Act of 2016

- Amendment to the Economic Espionage Act ("EEA")
- Uses the existing definition of "trade secret" in the EEA, uses similar or exact language of other provisions from UTSA
- Creates a civil cause of action
  - "[a]n owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce"

The Defend Trade Secrets Act of 2016

- **"trade secret"** includes
  - "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
    a) the owner thereof has taken **reasonable measures** to keep such information secret; and
    b) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public
- **"reasonable measures,"** or efforts to maintain secrecy, are *built in*

The Defend Trade Secrets Act of 2016

- The new federal law is significant for trade secret owners because it provides:
  - a new *property right*
  - a way into *federal* court, rather than the mercy of a state court
    - more comparable to patent protection
    - BUT:
      - federal court requires a unanimous jury
      - no inevitable disclosure under the DTSA
      - heightened threat of declaratory judgments in federal court
      - defense of reverse engineering still available
      - possible preemption, jurisdiction issues

The DTSA vs. UTSA

- **UTSA**

Attorneys' Fees	Bad faith claims, motion made or "resisted in bad faith," or willful and malicious misappropriation
***Ex Parte* Seizure**	Not authorized
Injunctions	Actual or threatened misappropriation may be enjoined
Royalties	In exceptional circumstances, an injunction may condition future use upon payment of a reasonable royalty for no longer than the period of time for which use could have been prohibited
Compensatory Damages	Damages for actual loss and for unjust enrichment or reasonable royalty for unauthorized use or disclosure
Exemplary Damages	Exemplary damages of two times actual damages permitted for willful or malicious misappropriation
Statute of Limitations	Typically three years
Whistleblower Immunity Provisions	None

The DTSA vs. UTSA

- **DTSA**

Attorneys' Fees	Bad faith claims, motion made or "resisted in bad faith," or willful and malicious misappropriation
***Ex Parte* Seizure**	Application can be brought by a plaintiff without any notice to the adverse party, subject to limitations
Injunctions	Actual or threatened misappropriation may be enjoined, provided the order does not (I) prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows; or (II) otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business
Royalties	In exceptional circumstances, an injunction may condition future use upon payment of a reasonable royalty for no longer than the period of time for which use could have been prohibited
Compensatory Damages	Damages for actual loss and for unjust enrichment or reasonable royalty for unauthorized use or disclosure
Exemplary Damages	Exemplary damages of two times actual damages permitted for willful or malicious misappropriation
Statute of Limitations	Three years
Whistleblower Immunity Provisions	Protects individuals from criminal or civil liability for disclosing a trade secret if (I) it is made in confidence to a government official or to an attorney for the purpose of reporting a violation of law, or (II) is disclosed to an attorney or used in court (subject to limitations) by an individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law; requires that employers include notice of such immunity in any agreement with an employee, contractor, or consultant that governs the use of the trade

Best Practices: Avoiding “Bet-the-Company” Trade Secret Litigation

- Companies have to be more on the ball in evaluating trade secrets and bringing new talent

1) **Update**

   a) Update standard agreements and non-disclosure agreements with new employees, contractors, and consultants

      - Must contain **whistleblower immunity provision** and **disclosure** language, or forfeit the remedies available under the DTSA

   b) Update IT and security policies to ensure the safety of sensitive documents and information

2) **Review**

   a) Review policies and agreements to ensure DTSA requirements are met

      - Take steps to discourage employees from bringing information from other companies

   b) Clear definitions of your company's trade secrets

      - Must not be vague or overbroad

3) Protect

a) Identify valuable, protectable information

b) Ensure your proprietary information meets “trade secret” definition under the EEA and DTSA

4) Prepare

a) Be mindful of state-specific factors that may make trade secret litigation more likely

- Reminder: the DTSA cuts both ways; your company may be sued under the DTSA

b) Prepare for employee entrances and exits by maintaining appropriate onboarding and offboarding procedures

- When hiring, assume *everything* is subject to discovery

c) Monitor relationships with third-party affiliates and partners

5) Managing Onboarding and Offboarding with Continual Training Component: Onboarding

a) Ensure agreements are provided to and signed by prospective employees at the appropriate time pursuant to state law

b) Require that employees will not use prior employers' trade secrets and/or proprietary information, and the return of any property belonging to the prior employer

c) Ensure policies on social media and use of IT resources are consistent with NLRB rulings

d) Counsel regarding safekeeping and handling of company trade secrets; create a culture of understanding confidentiality

- Institute **continuing training** and follow up with new employees
- Have routine reminders and training
- Monitor relationships with third party affiliates

6) Managing Onboarding and Offboarding with Continual Training Component: Offboarding

a) Conduct thorough exit interviews; consider using exit interview certification

- Identify the confidential/trade secret information that employee had access to

- Ask departing employees about their reason(s) for leaving and what their next positions will be

b) Check employee's computer and work-related activities in advance of the exit interview

Managing Onboarding and Offboarding with Continual Training Component

c) Ensure return of *all* Company property, including hardware, devices, email, cloud data, social media accounts (consider an inventory list)

- Arrange to have all Company data removed from any personal devices
- Disable access to Company computer networks
- Obtain user names and passwords for all Company social media accounts

d) Inform employee and/or new employer of continuing obligations under agreements with the Company

e) Conduct post-termination investigations as appropriate

How You Can Reach Us

Robert B. Milligan
Partner

Los Angeles
rmilligan@seyfarth.com
(310) 201-1579

Visit our award-winning blog to stay current on trade secrets, non-competes, and computer fraud issues at www.tradesecretslaw.com

SEYFARTH SHAW

Thank You