Trade Secrets for Patent Lawyers

Implementing an Effective Trade Secret Strategy to Maximize the Value of Your IP Portfolio

WSPLA | March 20, 2024

Amelia L.B. Sargent

Partner, *Willenken LLP*

Stanford Law School, J.D.

University of California, Berkeley, Ph.D.

Georgetown University, B.A.

- 13 years' experience in complex commercial litigation, with focus on trade secrets.
- First-chair trial and arbitration experience, appellate briefing and argument before the Ninth Circuit, and primary drafter of three Supreme Court *amicus* briefs.

Ashley L. Kirk

Of Counsel, *Willenken LLP*

University of Illinois College of Law, J.D.

Baylor University, B.S.E.

- Represents clients before the U.S. Patent and Trademark Office (USPTO), various U.S. District Courts, and at the appellate level. Experienced in all aspects of intellectual property procurement, monetization, and enforcement strategies.
- Participated in the prosecution of over 750 patent applications and hundreds of trademark applications in the U.S. and abroad.
- Focuses on patent re-examination proceedings, defensive invalidity and non-infringement opinions, drafting and reviewing of pleadings, claim construction and invalidity contentions, participating in witness depositions and trial, and negotiating intellectual property-related settlement agreements.

1. The What: Definition of a Trade Secret
2. The Why: Why Incorporate Trade Secrets Into Your Strategy?
3. The How: How to Incorporate Trade Secrets Into Your IP Strategy
4. Tips & Takeaways

What Is a Trade Secret

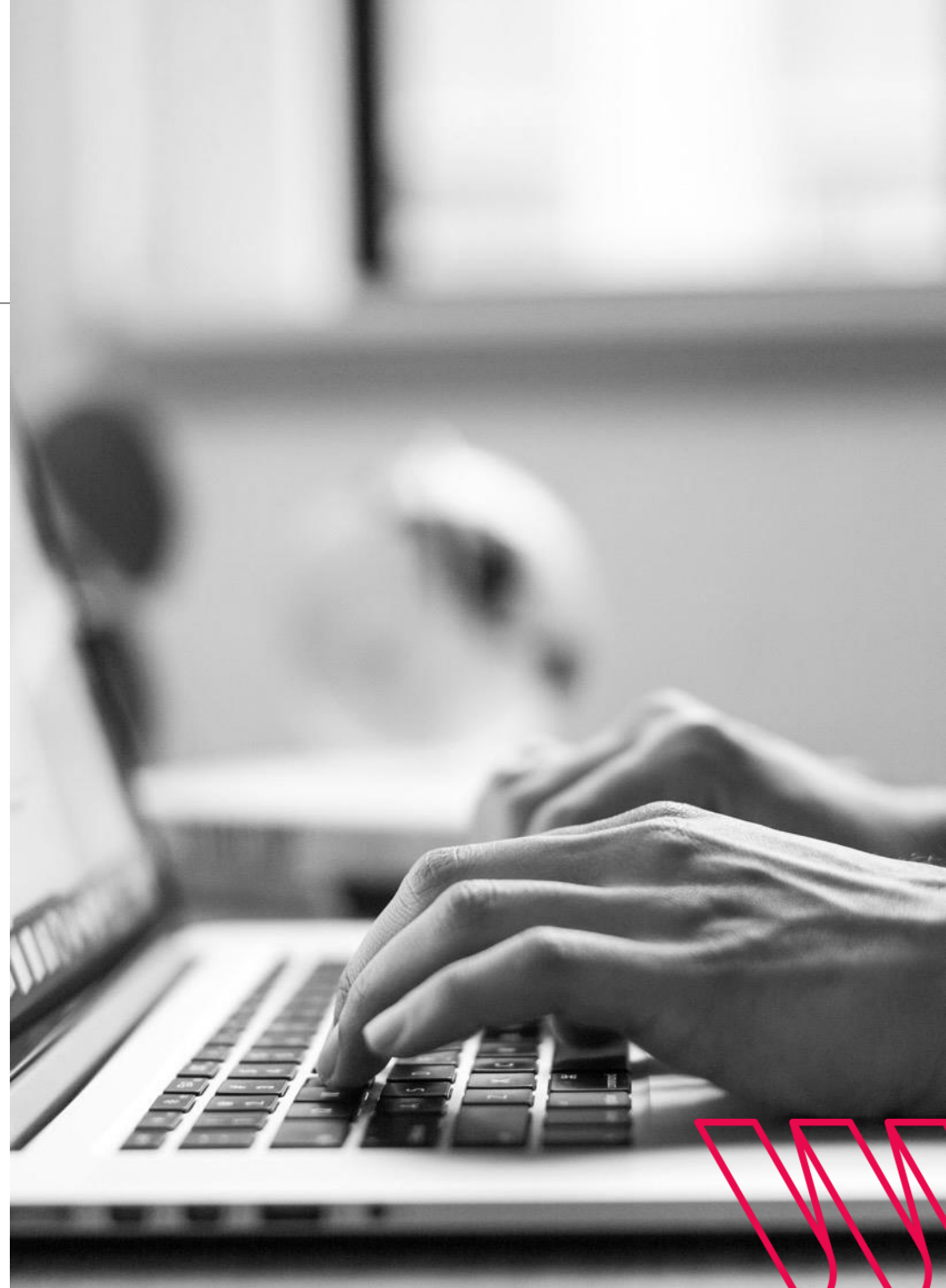
Examples of Trade Secrets: The Classics

Trade Secret Protection

- State Law:
  - Uniform Trade Secrets Act (UTSA) (48 states + DC, PR, VI)
  - NC Trade Secrets Protection Act, or
  - common law (NY)
- Federal Law: Defend Trade Secrets Act of 2016 (DTSA)
  - 18 U.S.C. § 1831 et seq.
  - Amends Economic Espionage Act to create federal private civil remedy for unauthorized use of trade secrets.

What is a Trade Secret

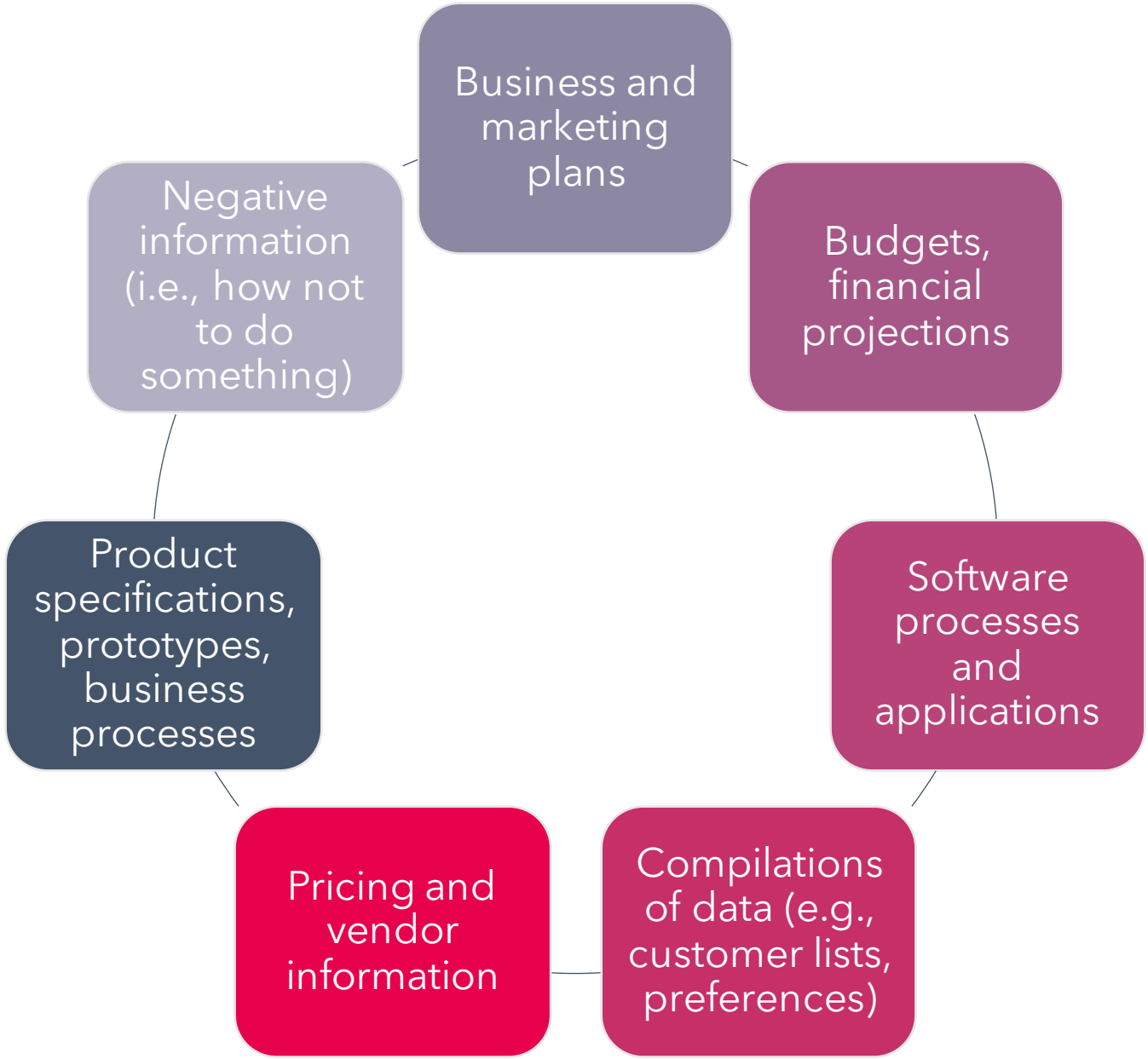
- Trade Secret protectable information can include all kinds of information in all kinds of forms.
- WUTSA specifies it can be “a formula, pattern, compilation, program, device, method, technique, or process.”



What is Trade Secret Protectable Information?

- The federal DTSA specifies more types of information:
  - "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 . . . "

Examples of Potential Trade Secrets



Two Requirements for Trade Secret Protection

- Trade Secret means any information that
  - Derives independent economic value from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and
  - Is subject to efforts that are reasonable under the circumstances to maintain its secrecy.

Two Requirements for Trade Secret Protection

- Trade Secret means any information that
  - Derives independent economic value from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and
  - Is subject to efforts that are reasonable under the circumstances to maintain its secrecy.

What Are "Reasonable" Efforts?

- "Reasonable efforts" mean companies need to use the tools available to them to protect their trade secrets. Reasonable efforts vary depending on a number of factors, including:
  - The size and maturity of the enterprise
  - The location of the enterprise
  - The value of the trade secret
  - The extent and cost of the measures taken
  - The rationale for selection of measures taken and not taken
- Resource: The Sedona Conference Commentary on the Governance and Management of Trade Secrets (July 2023): https://thesedonaconference.org/publication/Commentary_on_Governance_and_Management_of_Trade_Secrets

How Does the Law Protect Trade Secrets?

- Trade Secret law prohibits “misappropriation” of the trade secret—i.e., theft:
  - Acquisition, disclosure or use
    - by improper means
      - Theft, bribery, misrepresentation, espionage/hacking
    - in violation of a duty to keep information secret
      - Fiduciary duties, duty of loyalty, contractual NDA, license, or employment contract or policy

How Does the Law Protect Trade Secrets?

- Trade Secret law does not exclude others from using the trade secret information if it was lawfully acquired:
  - Reverse engineering is not an "improper means"
    - Must be "clean"! No violation of contractual duty and reverse engineering should not be done by person who had contact with the trade secret.
  - Independent Derivation is not an "improper means"
    - Published or public sources, independent experimentation & development, the "flash of genius"
    - There is also a defense if the trade secret was "readily ascertainable"—that is, the defendant *could have* independently derived it.

Trade Secret Remedies

- Injunction
- Ex Parte Civil Seizure
- Damages:
  - Actual Damages (lost sales, etc.)
  - Unjust Enrichment/“Head Start” damages
  - Reasonable royalties

Why Incorporate Trade Secrets Into Your IP Strategy?

Protecting Innovation with Trade Secrets? Controversy Amongst IP Practitioners

The trade secrets process is “full of potential traps for unwary litigants”.

Trade secrets management requires extensive training and robust management that might be impractical.

“[E]mployees are increasingly mobile”, which could compromise confidentiality.

Trade secrets can have “huge economic advantages under the right conditions”.

Trade secrets offer better protection when patent laws are hostile to the innovation – software, AI and certain biotech technologies.

Trade Secrets and Innovation – Why?

- According to Ocean Tomo, intangible assets (primarily intellectual property) now account for over 90% of the S&P500 market value.
- Almost all technology can be protected with a combination of patents and trade secrets to enhance portfolio value and extend the company's monopoly
  - Patent the preferred embodiment, but protect innovation specifics with trade secrets:
    - Source code, Dimensions, Materials, Interoperability, Method of Manufacture
- Reclaim Public Subject Matter
  - Specificity can Transform the Obvious into a Protectable Trade Secret

But, MUST BE ADEQUATELY DEFINED?

Trade Secrets and Innovation – When?
ALMOST ALWAYS IN SOME FORM

- In Combination with other IP
- Specialized Products or Customers
- Shared Technology
  - Prevent reverse engineering by partners and customers
- Greater Economic Value From the Innovation Remaining Secret
  - Internal Process?
  - Specialized Formula?
  - Economic Value of the Innovation over its Lifetime?
- Nascent Technology
- Unfavorable Status of Technology under Current Patent Laws
- Unpatentable Subject Matter or Combination

Protecting Software as a Trade Secret

- Supreme Court decisions have made software patents easier to invalidate under
  - *Alice* & progeny
- Protects Source Code or backend functionality only?
- Requires Robust Terms of Service and Licenses

Protecting Biotechnology as a Trade Secret

- Genomic sequences
  - Seeds
  - botulinum toxins
- Biologics
- Combinations of Known Elements
  - Precise dimensions, materials, for e.g., a heart valve
- Compatibility of Equipment Components
  - Probes in ablation equipment

AI-Generated Content – Only a Trade Secret

- Information or content generated by AI is not subject to Patent or Copyright.
  - Patents require an “inventor” and Copyright requires an “author”. Courts interpret these to mean a human creator.
- Trade secret law can protect all kinds of information, regardless of how it was created, as long as it is
  - *(Valuable because) Secret & Safe!*

What are the Risks?
MANAGEABLE

- *Reverse Engineering*
- *Independent Discovery and Patent Infringement Claim*
- *Inadvertent Disclosure*
- *Difficulty in Pleading a Claim*

Trade Secrets and Innovation: **Risk** of Reverse Engineering

Card Isle Corp. v. Farid, No. 1:21-CV-1971-TWT, 2023 WL 5618246 (N.D. Ga. Aug. 30, 2023).

Facts: Card Isle supplied retailers like Edible Arrangements with coding systems, infrastructure, and support to sell personalized greeting cards on their websites under an agreement that the customers could not reverse engineer the software. Edible Arrangements did. An action was brought alleging theft of trade secrets under Georgia Trade Secrets Act or Federal Defend Trade Secrets Act, and Breach of Contract.

Holding: Customer's agreement to not directly or indirectly, "**reverse engineer**, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas, know-how or algorithms relevant to" technology company's services or software **was valid and enforceable**.

TAKEAWAY – The defense of "reverse engineering" may be admission to a breach of contract.

Trade Secrets and Innovation: …**Risk** of Reverse Engineering

Faiveley Transp. Malmo AB v. Wabtec Corp., 559 F.3d 110, 117 (2d Cir. 2009).

Facts: Swedish company manufacturing company brought trade secret misappropriation action against American company, with which it had a licensing agreement, for the "know-how" in manufacturing braking systems for trains. Wabtec "reverse engineered" the braking system and won a sole source contract from the NY Transit Authority.

Holding: "To succeed on a claim for the misappropriation of trade secrets under New York law, a part must demonstrate: (1) that it possessed a trade secret, and (2) that the defendants **used that trade secret in breach of an agreement, confidential relationship or duty**, or as a result of discovery by improper means." And, Wabtec Corp. employees were sufficiently tainted by the disclosure of Plaintiff's trade secrets that its reverse engineering defense was not viable.

TAKEAWAY – While reverse engineering is a defense to a claim, practically it is difficult to prove that reverse engineering occurred without the use of protected disclosures.

Trade Secrets and Innovation: …Risk of Reverse Engineering

Pauwels v. Deloitte LLP, 83 F.4th 171, 178 (2d Cir. 2023).

FACTS: Pauwels was engaged by his employer BNYM to evaluate a potential investment in the alternative energy sector. He developed the so-called "Pauwels Model," a "proprietary model to value BNYM's proposed energy sector investments." BNYM, seeking to replace Pauwels with Deloitte, shared spreadsheets output from the model with a Deloitte employee without Pauwels knowledge or consent.

HOLDING: Deloitte's reverse engineering of the Pauwels Model was not trade secret misappropriation because Pauwels did not take adequate precautions to keep his model, or its output, confidential.

TAKEAWAY – Reverse engineering is always a defense, and it is a stronger defense where there are no contractual obligations to regarding the confidentiality of the material used.

Trade Secrets and Innovation: **Risk** of Patent Infringement Suit

BASF Corp. v. SNF Holding Co., 955 F.3d 958, 968 (Fed. Cir. 2020).

"Congress has considered the implications of patenting secret processes, which prior innovators might often choose to conceal **as trade secrets**, and addressed the issue. . . . Congress revised **35 U.S.C. § 273** to create **a prior-use defense for a defendant that "commercially used" a claimed "process" or "machine, manufacture, or composition of matter used in a manufacturing or other commercial process" "at least 1 year" before the earlier of the effective filing date** of the claimed invention or a previous disclosure thereof."

TAKEAWAY – Trade Secrets can be used to defend against patent infringement suits.

Trade Secrets and Innovation: …**Risk** of Patent Infringement Suit

Pelican Int'l, Inc. v. Hobie Cat Co., No. 320CV02390RSHMSB, 2023 WL 2127994, at *19 (S.D. Cal. Feb. 10, 2023).

FACTS: Pelican sued Hobie Cat alleging infringement of its patented interface for a propulsion mechanism on a kayak. The claims included a "watercraft" with a "rigid body". Hobie Cat has previously proto-typed such an interface and claimed a prior use defense under 273(a).

Holding: "When Section 273 uses the term "**claimed invention**," it describes it as the "claimed invention being asserted against the person" that the person "would otherwise infringe. . . .an infringement analysis is performed on a claim-by-claim basis. . . . Thus, a person can only "otherwise infringe" a particular claimed invention if the person's **accused product or act meets each and every limitation in a particular claim or claims asserted against it**. . . Accordingly, the Court rejects Hobie's argument that a Section 273(a) analysis is not tied to the specific claims asserted in the action."

TAKEAWAY – Innovative trade secrets should be adequately described in internal documents so they can be used defensively on an element-by-element claim analysis.

Trade Secrets and Innovation: **Risk** of Disclosure

Broker Genius, Inc. v. Zalta, 280 F. Supp. 3d 495 (S.D.N.Y. 2017).

Facts: Licensor of software used by ticket brokers in the secondary market filed suit against former licensees and their company, who subscribed to the software to assist in developing a competing software product.

Holding: Although there was adequate evidence of commercial value, and copying in violation of the agreements between the parties, "[b]ecause Broker Genius discloses the information that it alleges to be its trade secrets to each of its licensees as a matter of course and . . . has not shown that it required those licensees to maintain the confidentiality of user-facing elements [its] software" it cannot show it is likely to be successful on its trade secret claim.

TAKEAWAY – Leaky processes taint even the best claims.

Trade Secrets and Innovation: …Risk of Disclosure

***Pioneer Hi-Bred Int'l. v. Holden Found. Seeds, Inc.*,** 35 F.3d 1226, 1229 (8th Cir. 1994).

Facts: Parties are competing breeders of hybrid corn seed. Pioneer alleged that Holden derived its seed from a Pioneer line, and presented evidence that the genetic makeup of Holden's seed showed it was derived from Pioneer material.

Holding: "Holden's argument that Pioneer abandoned its trade secret by selling [the seed] to the Soviet Union is similarly unpersuasive. Pioneer did sell [the seed] to the Soviet Union . . . [t]his sale . . . was pursuant to an agreement which restricted use of the seed and contained a confidentiality provision. . ."

TAKEAWAY – Trade Secrets can be maintained even after a Product is Sold – it all depends on the nature of the sale and related agreements.

Trade Secrets and Innovation: **Risk** of not Pleading with Particularity

Syngenta Seeds, LLC v. Warner, et al., No. 20-cv-1428, 2021 BL 61423, at *12 (D. Minn. Feb. 22, 2021).

Facts: Syngenta Seeds claimed two former employees—Todd Warner and Joshua Sleper—took its confidential business information and trade secrets and used them to help a competitor called Farmer's Business Network ("FBN"). Syngenta claimed the employees took, e.g., information related to "data generated from pan-genomic analytics using DNA sequence data," "genetic maps," and "molecular marker (genotyping) data", with examples. However, they also claimed a breeding program plan created by Sleper, and sent to FBN during his employment, used its trade secrets.

Holding: While some claims could be maintained, Claims directed to the breeding program plan by Sleper was not pled with particularity because the document itself did not appear on its face to include Syngenta data, nor did the pleadings explain how it was derived from Syngenta data.

TAKEAWAY – To support a trade secret claim, the fact an employee created work product for a competitor is not enough. The company must identify the trade secrets that were used to create that work product.

Trade Secret Rewards: **SUBSTANTIAL**

- No need to Register.
- Protection Indefinite.
- Can still Monetize (license, etc.) the Trade Secret.
- May be able to Still Seek Patent Protection.
- Claims can be brought for Patent Infringement and Trade Secret Misappropriation.
- Jury trials in both State or Federal Court have been Awarding Large damages in Trade Secrets Cases.
  - Exemplary damages available for “willful or malicious” appropriation.

How to Incorporate Trade Secrets Into Your IP Strategy

Is the Writing on the Wall for Non-Competes?

- Many companies use non-compete clauses to protect trade secrets because workers who gain access to trade secrets and confidential information are forbidden from taking that information to a competitor, where it might be disclosed and used.
- Non-competition clauses, or non-competes, are restrictive covenants in contracts that prevent or delay individuals from working for a competing employer, or starting a competing business, after their employment ends.
- According to the U.S. Government, 1 in 5 American workers, or about 30 million people, are bound by non-competes.

FTC Proposes to Ban Non-Compete Clauses

- On January 5, 2023, the FTC proposed a draft rule to ban the use of non-compete clauses.
- The Proposed Rule would provide that it is an "unfair method of competition," and therefore a violation of Section 5 of the FTC Act, for an employer:
  - to enter or attempt to enter into a non-compete clause with a worker,
  - to maintain a worker with a non-compete clause, or
  - under certain circumstances represent to a worker that the worker is subject to a non-compete clause.

FTC's Proposed Rule

- The Proposed Rule applies to "workers," not just employees:
  - A "worker" is a person "who works, whether paid or unpaid, for an employer".
- The Proposed Rule only applies to non-compete clauses (not other restrictive covenants, such as NDAs or non-solicits) but uses a functional test to determine whether a clause is a *de facto* non-compete.

…FTC's Proposed Rule

- The Proposed Rule also:
  - requires employers to rescind existing non-competes as of the compliance date,
  - provide workers and former workers notice of rescission in an individualized communication within 45 days.
- There is an exception only between the seller and buyer of a business, when the seller/party restricted by the non-compete holds at least a 25% ownership interest in the business entity.

Current Status of FTC Ban and Other Developments

- The FTC received 26,813 comments on the Proposed Rule before comment period ended in April 2023 and is now reviewing those comments.
- Bloomberg Law reports that the FTC will vote in April 2024 on the final version of the proposal.
- Since then, in May 2023, Minnesota joined the ranks of states that ban most non-competes.
- New York's legislature also passed a ban, but on Dec. 4, 2023, Gov. Hochul stated she will not sign it without modifications—but NYC has introduced its own noncompete ban last month.
- California enacted two further bills restricting noncompetes (& more!).

New California §16600 Amendments

- Effective Jan. 1, 2024, two new amendments to California Bus. & Prof. Code §16600 may have outsized impacts restricting non-competes and other restrictive covenants
  - §16600(c): Not limited to Ks where person being restrained from engaging in a lawful profession, trade, or business is a party to the K → Non-solicits? No poach contracts?
  - §16600.5: Reaches Ks "regardless of when and where the contract was signed" and "regardless of whether the K was signed and the employment maintained outside of California" → people subject to non-competes moving into CA for a new job; remote workers?
  - §16600(b): Codifies CA Caselaw on noncompetes and "de facto" noncompetes

What Is a De Facto Non-Compete?

- Overbroad confidentiality provisions that would have effect of restricting employee's ability to practice profession
  - *Brown v. TGS Mgmt*, 57 Cal.App.5th 303 (2020)
  - Court invalidated entire confidentiality provision in employment contract
- Non-solicitation or no-recruit provisions
  - *AMN Healthcare, Inc. v. Aya Healthcare Svcs*, 28 Cal.App.5th 923 (2018)
- *California law also prohibits employers using choice of law or venue provisions to get around California substantive law (Labor Code §925(a) limited somewhat by (e).)*

What About CIAAs?

- *Whitewater West Industries, Ltd. v. Alleshouse*, 981 F.3d 1045 (Fed. Cir. 2020)
  - Former employer ("Whitewater") sued former employees/inventors of waterpark attractions that individuals may ride as if surfing, and nozzle configurations for regulating water flow re: same, for failure to assign post-employment patents "resulting from or suggested by" employee's work for company or "in any way connected to any subject matter within the existing or contemplated business of" company.
  - Federal Circuit, applying California law, invalidated CIAA purporting to mandate assignment of inventions conceived post-employment and without use of former employer's confidential information or trade secrets as void under Section 16600.

Five Ways to Protect Your Trade Secrets *Without* Non-Competes

1. Identify the Trade Secrets Up Front.
2. Create a Culture of Trade Secret Awareness.
3. Tune up HR Policies and Procedures.
4. Leverage Technology to Implement Security.
5. Prepare for Red Flag Situations.

Five Ways to Protect Your Trade Secrets

1. Identify the Trade Secrets Up Front.
2. Create a Culture of Trade Secret Awareness.
3. Tune up HR Policies and Procedures.
4. Leverage Technology to Implement Security.
5. Prepare for Red Flag Situations.

Identify The Trade Secrets Up Front

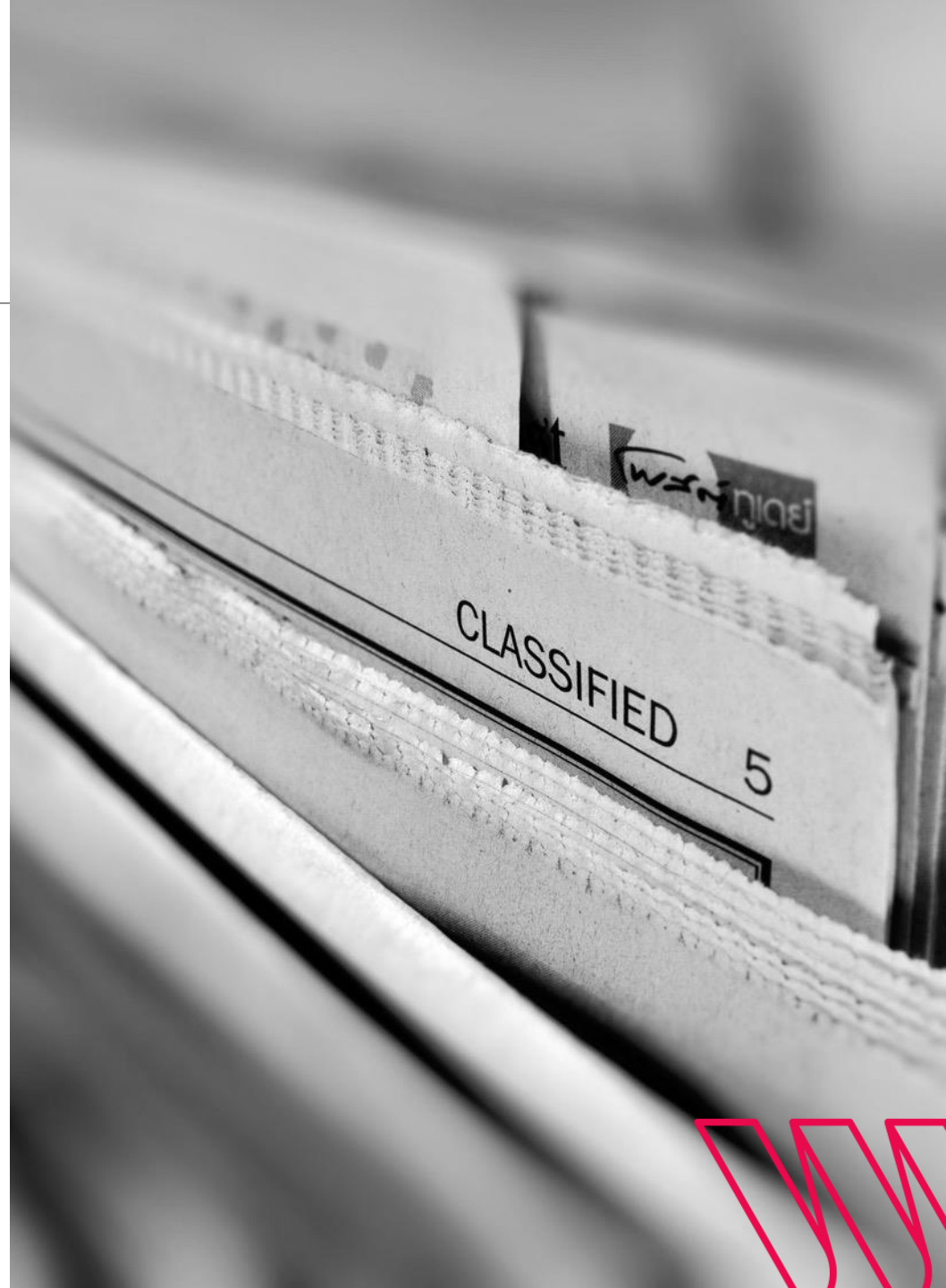
- **Goal:** Understand what the business's trade secrets are and how they are protected.
  - Articulate the value of your trade secrets to the business.
  - Consider whether Trade Secret Inventory or Trade Secret Governance Program is right for your business.
  - Identifying trade secrets up front allows the business to align valuable assets with appropriate "reasonable measures" to protect them, and to reassess at periodic intervals.

…Identify The Trade Secrets Up Front

- Interview key stakeholders across the business and ask:
  - What is the business's "secret sauce"?
  - Where and how is the information kept?
  - Who (roles/names) has access to it?
  - **For how long** is the information a "trade secret"?
    - Unless it is literally the secret recipe, information is often not "valuable because it is secret" forever:
      - Cyclical information like quarterly plans that are subsequently implemented
      - Inventions or methods that are subsequently patented
      - Strategy, plans, or projects presented at conferences or on investor calls
- Once trade secrets are identified, an assessment can be done to assess whether they are aligned with appropriate "reasonable measures"

Other Benefits to Identifying Trade Secrets

- Help workers understand and make good choices to protect trade secrets.
- Streamlines litigation:
  - Helps in-house counsel to advise on what is or is not important or worth litigating when an employee departs for a competitor.
  - Helps outside counsel identify trade secrets with reasonable particularity—stronger chances for early injunction (TRO/PI) success (or civil seizure) and streamlined discovery.



Create a Culture of Trade Secret Awareness

- Happily employed workers usually want to do the right thing – help the company grow and succeed.
  - → Don't let the employee handbook be the only explanation a valuable employee receives about what the company considers trade secret information!
- Foster a culture of transparency, trust, and accountability among your workers.
- Consider designing **a training session** to train management and workers to understand and protect the company's information:
  - Include trade secret basics, such as marking documents as confidential and not emailing documents outside the company.
  - Include explanations about what information or inventions belong to the company versus the worker.
- Engage management in encouraging and modeling good trade secret habits!

Tune up HR Policies and Procedures

- Most trade secret leaks occur when workers take trade secrets to new jobs.
- HR Policies and Procedures should both protect your company's trade secrets, and protect *against* new employees bringing in trade secrets from their former employer.
- Companies should also consider issues with contingent workers such as vendors and contractors.
- Restrictive Covenants that are *not* non-competes or *de facto* non-competes are still enforceable:
  - Employee Handbook
  - Confidentiality and Assignment Agreement
  - NDAs
  - Non-Solicits

Best Practices: Employee Onboarding

- Remind recruits not to disclose confidential information while interviewing.
- Provide and explain employee handbook and confidentiality policies, and require signed acknowledgement.
  - *Use DocuSign or Adobe E-signature functions*
- Certifications of clean arrival: Have employee certify they are not bringing confidential information from any previous employer, especially any competitor.
- Have HR or IT record and log equipment provided.

Best Practices: Employee Offboarding

- Deactivate access to email and computer systems.
- Ensure employee returns all company-provided equipment (record and log returns).
- Certification of clean departure: return of all company property including information & documents.
- Remind employee of their continuing confidentiality obligations, and sign acknowledgement.

Emerging Risk Area: Dual Employment

- "Dual employment" is on the rise: Employees holding more than one job without notifying the employer.
  - Social media attention, work from home, and new technology ("mouse jigglers") create risk of employees being dual employed.
- Tune up policies on conflicts: when is a "side gig" a risk to your company?
  - Policy in employee handbook
  - Risk assessment committee

Leverage Technology to Implement Security

- Partner with IT to ensure your company is taking “reasonable efforts” to protect its trade secrets.
  - “Reasonable efforts” can be different from every company.
  - IT can protect trade secrets with passwords, restricted access by file or folder structure, read-only rights, and confidential branding.
  - Restrict access to trade secrets to those who have a need to know.
    - Use your Inventory to identify where and how trade secrets are stored, and who has access to them!
  - Companies with very sensitive trade secrets should consider monitoring and data loss prevention software to watch for unusual downloading or deletion patterns, and track access.

Types of IT Tools Available

- What Tools are Available?
  - Passwords
  - Secure cloud-based services
  - Remote desktops, VPNs
  - Videoconferencing (Zoom, Skype for Business)
  - Chat (Teams, Google hangouts)
  - Paperless Capabilities (DocuSign, Adobe)
  - Monitoring and Data Loss Prevention software
  - Encryption
  - Network segregation

Prepare for Red Flag Situations

- Red Flag situations can be any situation where trade secret information is **moving.**
  - Workers moving between competitors.
  - Workers working with trade secrets **remotely** or offsite.
  - Workers engaging in side gigs that could affect trade secrets.
  - Third-party vendors or offshoring (anything where data is moving out of the company or out of the US).
  - Pitches for funding/acquisitions where trade secret information is being disclosed.

Employee Moving to Competitor

- You'll already have identified any trade secrets this employee had access to, trained them, and can properly offboard them.
- In addition, consider whether you need to:
  - Cut the notice period and remove remote access to trade secrets immediately.
  - Arrange for immediate collection of devices and work product.
  - Preserve a forensic copy of any devices.

Access for Third Parties or Temporary Workers

- Contractors, vendors, interns, and other temporary workers may have access to sensitive information without the same sense of accountability/stewardship as employees.
- Consider principle of least privilege (PoLP) - configure devices to limit access, create specific job profiles (interns) that restrict what they can see.
- Ensure that vendor contracts are structured to protect sensitive information.

Pitches and Acquisitions

- What can you do to minimize the risk of being sued for trade secrets misappropriation, if the acquisition fails?
  - ✓NDAs.
  - ✓Clean room review or development:
    - ✓In an acquisition, segregate review team from development team.
    - ✓Document the destruction of materials received
    - ✓Consider clean-room development, where an isolated team is responsible for design of competing product.
  - ✓Consider how to adapt for remote teams.

Recap: Five Ways to Protect Your Trade Secrets

1. Identify the Trade Secrets Up Front: Consider Trade Secret Inventory or Governance Program.
2. Create a Culture of Trade Secret Awareness: Training and Reinforcement of good practices.
3. Tune up HR Policies and Procedures: Recruiting, Onboarding, Offboarding—and watch out for dual employment.
4. Leverage Technology to Implement Security: “Reasonable” measures, “Need to know,” PoLP.
5. Prepare for Red Flag Situations: Competitors, Third Parties, and Acquisitions.

Tips & Takeaways

Tips & Takeaways

1. Trade secrets can be a very valuable addition to managing your company's IP portfolio, but comes with risks and pitfalls that need careful attention.

2. Protect trade secrets by restricting the information, not the people—non-competes or other restrictive covenants that prohibit employee mobility are increasingly unenforceable.

3. Trade secret litigation is often lengthy, expensive, and fraught. Counsel your clients about the risk/benefit of pursuing litigation—when does it make sense to litigate, and when is it better to let it go?

Today's Speakers

Amelia Sargent

Willenken LLP

Partner

asargent@willenken.com

Ashley Kirk

Willenken LLP

Counsel

akirk@willenken.com

Contact: **Amelia L.B. Sargent** | amelia.sargent@willenken.com
Ashley Kirk | akirk@willenken.com

Thank you!

willenken

707 Wilshire Blvd.
Suite 3850
Los Angeles, CA 90017

TEL 213.955.9240
FAX 213.955.9250

willenken.com