Course #900:
Protection of Intellectual Property with a Focus on Trade Secrets for the Non-Specialist

Part 1: Defining Trade Secrets

What is Intellectual Property?

- Trademarks
- Copyrights
- Patents
- Trade Secrets

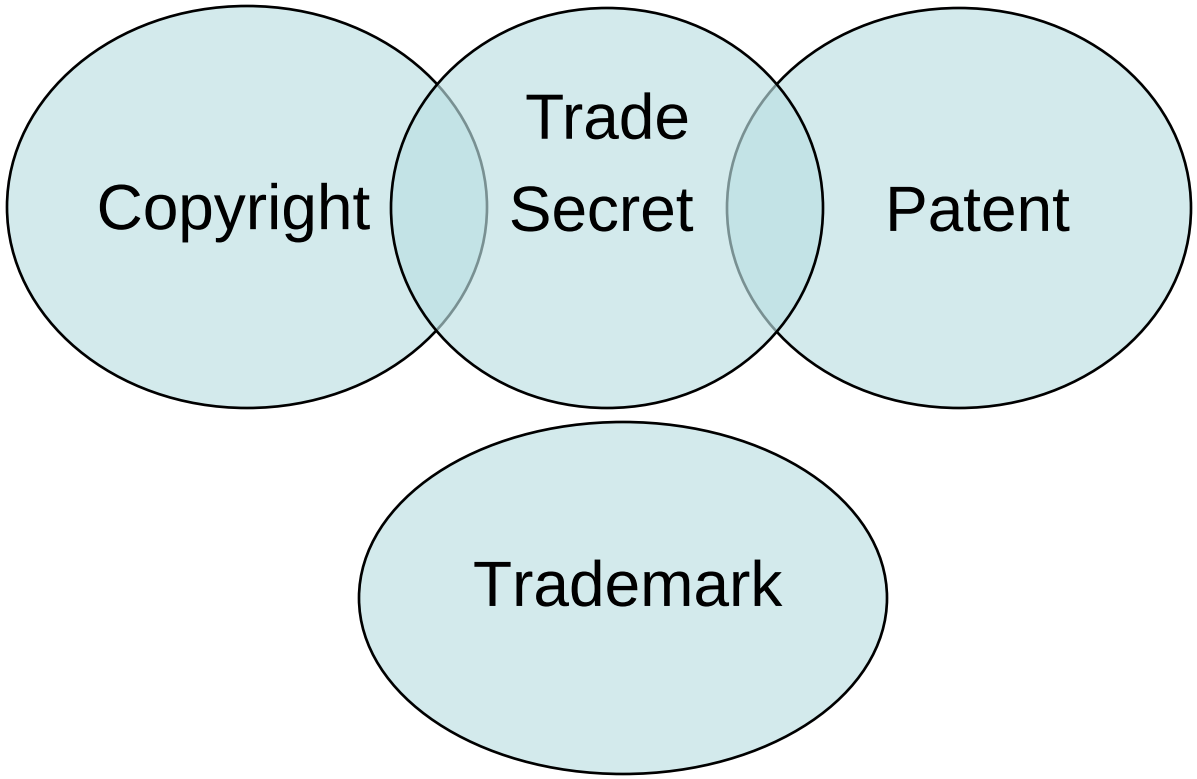
Trade Secrets

- The oldest form of IP protection
- A trade secret is information that has economic value from not being known or readily ascertainable and which is subject to security measures
  - Specific definition varies
  - Generally state based
  - There is no uniform federal law but some statutes apply

Trade Secrets

- Trade secret law is unique in that it does not grant a set of exclusive rights like other IP laws
- Trade secret law protects against wrongful access to (and subsequent use of) information, not controlling the use of that information (like patents, copyrights, trademarks)

Overlapping rights



Trade Secrets vs. Patents vs. Copyrights

Factors to Consider:

- Duration
- Date of invention/creation
- Patentability
- Cost of obtaining
- Cost of litigation/enforcement
- Roadmap effect/secrecy
- Licensing potential
- Time to market
- Presumption of validity

One is Good, Two is Better

- Multiple methods of IP protection are preferable
  - Cover more subject matter than a single method
  - Strengthen exclusivity
  - Provide additional remedies
  - Backup in case primary IP is invalidated
  - Exploit IP overlap
  - Build a complete IP portfolio
  - Overprotect
  - Create a minefield

Trade Secrets - UTSA

- The Uniform Trade Secrets Act, in various forms, has been adopted by 46 states
- Massachusetts, New Jersey, New York and Texas have not adopted
- The UTSA is a model act so even in states that have adopted the UTSA some variations may occur

Trade Secrets - UTSA

Trade secrets are defined as information, including a formula, pattern, compilation, program, device, method, technique or process that:

(i) derives independent economic value, actual or potential, from not being generally known to, and not being ready ascertainable by proper means by other persons who can obtain economic value from its disclosure or use, and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. UTSA § 1(4)

Trade Secrets - UTSA

- Trade secrets are information….
- The UTSA give a nonexclusive list of potential trade secrets:
  - Formula (e.g. a chemical formula or recipe)
  - Pattern (e.g. manufacturing drawings)
  - Compilation (e.g., customer lists, marketing data)
  - Program (e.g., computer programs)
  - Device (e.g., the design of a machine)
  - Method, Technique or Process (e.g. “know-how”, the knowledge of a way to do things)

Trade Secrets - UTSA

- … derives independent economic value….
- Economic value can be proved in a number of ways
  - Value to business
  - Expert testimony
  - Cost to develop the information
  - Licensing by others
  - Cost of security
  - Fact of improper acquisition

Trade Secrets - UTSA

- … economic value, actual or potential….
- Not required that you prove it actually provides economic advantage, just that it could
- Compare to the narrower Restatement (First) of Torts § 757 which provides that information must be "in use in business" and must provide an "advantage over competitors who do not know it or use it"

Trade Secrets - UTSA

- … economic value … from not being generally known….
- Absolute secrecy is not required so long as it is not "generally known"
- Economic benefit is the touchstone - can the other parties who know the information economically benefit?
- Don't rely on the absolute secrecy exception - if the information is known by others at all, the owner's burden will be high

Trade Secrets - UTSA

- … and not be readily ascertainable….
- Information that can be discovered easily and relatively cheaply won't be protected
- Information learned by examining a product is not protectable
- It is not "readily ascertainable" if improper means are required to discover the information
- Comparatively more restrictive than the Restatement which requires actual knowledge

Trade Secrets - UTSA

- … subject of efforts… to maintain secrecy….
- Information must be subject to reasonable security measures, not absolute secrecy
- Industry standards and the cost of security are relevant
- Examples of reasonable security include
  - Advising employees of the existence of a trade secret
  - Limiting access to the trade secrets on a “need to know” basis
  - Securing the location of the trade secrets
  - Keeping records of access to the trade secrets

Non Disclosure Agreements

- What's the difference between Trade Secrets and Confidential Information?
- What clause should always be in your NDA?

Trade Secrets – Non UTSA States

- Massachusetts
  - Mass. Gen. Law 266 § 30
- New Jersey
  - Based solely on common law, largely following the Restatement
- New York
  - Based solely on common law, largely following the Restatement
- Texas
  - Based solely on common law, largely following the Restatement
  - Also has criminal provisions (Tex. Penal Code Ann § 12.34)
- These states have significant economic impact (20%+ of US GDP)

Select Federal Statutes

- 18 USC § 1030: Computer Fraud and Abuse Act
- 18 USC § 1831 *et seq.*: Economic Espionage and Trade Secret Theft
- 18 USC § 1905: Unauthorized Disclosure of Government Information by a Government Employee
- 22 USC § 2278: Arms Export Control Act and the International Traffic in Arms Regulation
- 18 USC § 1341: Mail/Wire Fraud
- 18 USC § 2311 *et seq.*: Foreign/Interstate Transportation of Stolen Property

International Aspects

- While this presentation is focused on US law, GATT, TRIPS, NAFTA and other international treaties require protection of trade secrets as well
- TRIPS doesn't use the term "Trade Secrets" but does track the language of the UTSA
- Signatories to the treaties are obligated to enact legislation to protect trade secrets using these principles

Part 2: Legal Claims and Remedies

Typical Civil Claims

- Misappropriation of trade secrets claim under the Uniform Trade Secrets Act (UTSA)
- Breach of Contract (Confidentiality, Non-Compete, Non-Solicitation)
- Other common law torts, *e.g.,* tortious interference with contract claims
- Breach of fiduciary duty/aiding and abetting
- Civil conspiracy (RICO)
- Violations of the Computer Fraud and Abuse Act, *e.g.*, unauthorized access to a protected computer

Pursuing Remedies

- Reasons to pursue or not pursue remedies
  - Effect on relationships with customers, vendors, competitors and employees
  - Willingness to sue
  - Making an example
  - How much willing to spend
  - New employer - Deep pockets? Competitor? Do they know that they have trade secrets?
  - Size and location of entity
  - Enforcement outside of the U.S.

Pursuing Remedies

- Effect of not taking action
  - Information may cease to be a secret and lose status as a trade secret
  - Potential defenses against future actions such as waiver, acquiescence, estoppel and laches

Types of Civil Remedies Generally Available

- Injunctive Relief
- Money Damages
- Unjust Enrichment/Restitution
- Punitive Damages
- Attorney Fees

Injunctive Relief Generally

- Preliminary Injunction Factors
  - Likelihood of success on merits
  - Irreparable harm
  - Harm caused to third parties
  - Public interest
- Permanent Injunction Factors
  - Irreparable harm
  - No adequate remedy at law
  - Balance of hardships between the parties
  - Public interest

Injunctive Relief Generally

- Mandatory Bond (FRCP 65(c)) – Required but amount discretionary
- Scope of Injunction – Discretionary but typically narrow

Remedies Available Under UTSA

- Injunctive relief
- Compensatory damages (actual loss and unjust enrichment)
- Willful and malicious = Exemplary damages
  - 2 x compensatory damages
  - Attorney Fees

Injunctive Relief under UTSA

- Available for *threatened* or actual misappropriation
- Generally terminated when information ceases to be a trade secret
- May be continued for an additional reasonable time to eliminate commercial advantage that would otherwise be derived from the misappropriation

Injunctive Relief under UTSA

- Royalty in Exceptional Circumstances
  - If the Court determines that it would be unreasonable to prohibit future use of trade secrets, an injunction may condition future use upon payment of a reasonable royalty
  - The royalty is only for the period of time that the use of the trade secret could have been prohibited

Injunctive Relief under UTSA

- Other Injunctive Relief
  - Affirmative acts to protect a trade secret may be compelled by a court, *e.g.*, destruction of documents containing trade secret information

Damages under UTSA

- Common methodologies used to calculate damages:
  - Unlawful gains, profits or benefits, by defendants;
  - Value to plaintiff of any of plaintiff's confidential and trade secret information; or
  - Reasonable royalty for any improper use of trade secrets

Inevitable Disclosure Doctrine

- In some jurisdictions, an employer may obtain an injunction preventing a former employee from working for a competitor because it is "inevitable" that the former employee will rely upon the employer's trade secrets in the new position with the competitor
- Application of the doctrine has the effect of a non-compete agreement
- *E.g. Bimbo Bakeries USA, Inc. v. Botticella*, 613 F.3d 102 (3rd Cir. 2010)

Inevitable Disclosure Doctrine

- Jurisdictions that have adopted the doctrine:
  - Arkansas
  - Connecticut
  - Delaware
  - Illinois
  - Indiana
  - Iowa
  - Massachusetts
  - Minnesota
  - New Jersey
  - New York
  - North Carolina
  - Ohio
  - Pennsylvania
  - Utah

Remedies Available for Breach of Contract

- Compensatory damages or expectation damages
- Injunctive relief
- Attorney fees if expressly provided for in contract
- Nominal damages

Remedies for Breach of Fiduciary Duty/Aiding & Abetting

- Injunctive relief
- Actual losses
- Restitution/Constructive trust
  - Profits are held in a constructive trust for the benefit of the beneficiary
- Punitive damages

Remedies under Computer Fraud and Abuse Act

- Remedies in civil actions
  - Injunctive relief
  - Compensatory damages
- Penalties in criminal actions
  - Imprisonment of up to twenty years, or up to life imprisonment if the offender attempts to cause or knowingly or recklessly causes death from their conduct
  - Penal fines

Remedies For Economic Espionage and Trade Secret Theft

- Both civil liability and criminal sanctions are available
- Imprisonment of up to fifteen years for economic espionage and up to ten years for trade secret theft
- Penal fines, including up to $10 million for organizations for economic espionage and up to $5 million for organizations for trade secret theft

Part 3: Protecting Trade Secrets

Goals:

- Protect Trade Secrets
- Create adequate evidence to prove Trade Secret status if stolen

An ounce of prevention is worth a pound of cure…..

- **Not all Confidential Information rises to the level of a Trade Secret so it's important to adequately protect both Trade Secrets AND Confidential Information**

- **Most (but not all) Trade Secrets and Confidential Information is stolen by employees, is electronic and is transmitted electronically**

Standard of Care: "reasonable efforts"

"…is the subject of efforts that are reasonable under the circumstances to maintain its secrecy…" (UTSA § 1(4))

"Reasonable Efforts" require both INTERNAL and EXTERNAL protections.

- What is "reasonable"?
  - varies by industry & company
- Overall plan
  - audit, compliance, improvements
- Internal Protections
  - workplace and employees
- External Protections
  - customers and business partners

Overall Plan

Identify Trade Secrets and other Confidential Information

Stakeholder Participation

Review Existing Practices

- Retention policy, how long are emails and network logs kept?

Develop and Implement Action Plan

- Single person responsible to coordinate multiple departments
- Risk assessment
- Create implementation, compliance and incident response plans (remember to include in data security and disaster planning and document retention policy)
- Implement plan
- Follow up audits
- Develop and implement plans to plug gaps and improve procedures

Internal Protections-Policies/Procedures

- **Evaluate current polices and modify if necessary**
  - Pay attention to retention and social media policies
- **Cross departmental-ALL departments including**
  - **Employment:** handbooks, NDAs, employment agreements or engagement letters, noncompete agreements if legal
  - **IT:** access to files/folders (need to know), computers/laptops, home computers, smart phones, portable drives, cameras/phones, IM messages, email use including sending to personal accounts, data preservation and retention
- **Implementation**
  - Apply consistently, audit compliance, fix/make improvements
  - Employee hotlines
  - Public companies: satisfy disclosure obligations to shareholders, government and others

Internal Protections-Physical Security

Limit access and usage (need to know)

- **Physical facilities**
  - **Building:** locks, restricted areas, cameras/phones, badges, sign in/out sheets, vaults
  - **Clean office:** erase whiteboards, clean desks, lock laptops in desk, screensavers & black screens, shred documents (prevent dumpster diving)
- **IT systems and data**
  - Smart phones and portable drives are current areas of high risk
  - Prevention: disable or limit Flash Drives, monitor access, monitor copy machines, prevent cell phone sync to company email, prevent attachments to private email, prevent VPN from home, train/educate employees, DLP system

Internal Protections-Physical Security

DLP = Data Leak Prevention

- Computer and network security software
- Identifies, monitors and protects
  - Data in use (endpoint actions)
  - Data in motion (network actions)
  - Data at rest (data storage)
- Track movement of documents and “fingerprint” them
- Providers: Symantec, Websense, Palo Alto Networks, Cisco and others

Internal Protections-Employees

- **Entry/Exit Interviews**
  - Discuss and provide copies of important policies
  - NDA
    - Not want prior employer/competitor Trade Secrets and Confidential Information
    - Clear description with examples of TS and CI
    - Patent Disclosures, turnover and assignment
    - Copyright assignments and work-for hire
    - Keep confidential during and after employment
    - Return property when employment ends
    - Outside CA: narrowly tailored noncompete clause

Internal Protections-Employees

- **Training**
  - ALL employees-management, supervisors, line employees (different for each group)
  - Initial Training and Periodic Refreshers
    - Establish NO expectation of privacy in communication methods (9th Cir. *Quon* case reversed on other grounds (reasonable search) by USSC)
    - Continuing responsibility, even after leave company
    - Describe how to protect (no visitors, lock up, clean desk, etc.)
    - Remind of obligations including in NDAs, employment agreements, policies & procedures
    - Social media use

External Protections

- Clients/Customers
- Business Partners

External Protections

CLIENTS/CUSTOMERS

- **NDA is primary protection**
  - Require sign BEFORE discussions commence
  - Require return documents (query: Keep copy to ensure compliance? Backups? Destroy? Certification?)
  - Note: make sure NDA differentiates time limit of keeping Trade Secrets confidential (forever) vs. other confidential information (generally 5-10 years)
  - Hold signing party responsible for breaches by all they share with otherwise individual NDAs with each person shared are needed
  - May help disprove antitrust issues (if applicable)
  - Mark everything confidential and/or Trade Secret
    - e.g. Watermarks (multilayered chip watermark, computer code, maps, design aspects that would be copied unintentionally or without understanding)

External Protections

CLIENTS/CUSTOMERS-special situations

- **RFP/RFI responses**
- **Government Contracts (FOIA) and State Open Records Laws**
  - Often exceptions for CI/TS but varies by state and who decides what is CI/TS?
- **Protection varies by state and foreign jurisdiction**
  - English speaking countries: mostly uniform
  - France and Germany: weak trade secret, strong contract law
  - China: enforcement is a problem, but getting better
- **Lawsuits** – request in camera review of TS

External Protections

BUSINESS PARTNERS (aka vendors, contractors, consultants)

- **Choose business partners carefully** (especially overseas)
- **Due diligence** on company
  - Company reputation, audit policies and systems, if international company -> include in FCPA audit
- **NDAs**
- **Contract provisions**
  - Require they follow your policies/procedures (post or provide)
  - Termination and indemnification if breach
  - Choice of law-understand what agree to
  - What happens to data on termination?
- **Issues with "The Cloud"**
  - Take it or leave it contracts, company out of business or sold, ex-US servers, subcontractors, what happens to data on termination?

Part 4: Discovering Possible Theft of Trade Secrets

- Your company has trade secrets
- You have implemented some processes to protect against disclosure of the trade secrets
- But, eventually there will be a disclosure and possibly even theft of the trade secrets
- How will you know?

Typical Sources of Leaks and Misappropriation of Trade Secrets

- Employees, current and former
- Contractors
- Consultants
- Customers
- Vendors and Suppliers
- OEM's and Manufacturers
- Sales Representatives and Distributors
- Lawyers/Patent Attorneys
- Other Business Partners and Outsiders

Sources of Detection

- Rumors and tips
- Anonymous hotline reports
- IT detection
- Saw it for sale
- Notice from a competitor
- Clone company set up
- Law enforcement contact
- Logical deduction

Rumors and Tips

- Sources: employees, customers, suppliers or industry contacts
- Next step: investigate discreetly
- Involve IT or an outside computer forensics service company
- Save the evidence!

Anonymous Hotline Reports

- Public companies are SOX required to have anonymous financial concern reporting hotlines available internally
- These same hotlines can usually intake other compliance issues as well
- Advertise to employees in training sessions
- Some companies allow public access

IT Detection of Employee Misappropriation of Trade Secrets

- Monitor downloads, searches and access to documents
- Archive and review email
- Review document access log to share folders and databases like Agile
- Use a DLP System

DLP = Data Leak Prevention

Detection not just Prevention

- DLP software in your computer network
- Can automatically track “fingerprinted” documents
- Identifying the abnormal:
  - Existing data from your network
  - Movement of data in the network
  - Access to stored data

Make sure IT saves the evidence, you may need it later!

- Review your Retention Policy
- Do NOT immediately re-process computer HDs!
- Check how long back-ups of emails are kept, aim for at least two months
- How far back are network logs kept?

For Sale

- Make a “buy” of a competitor’s product
- Engineering takes it apart for a look inside
  - Besides patent infringement, is there evidence to suggest trade secret theft was involved?
  - Are there “watermarks” that prove copying?

Competitor

A competitor contacts your company about someone offering to sell your trade secrets to them (the honest competitor)

Clone Company

- Founders are former employees
- Poaching your current employees
- Terminating employees lie about why and where they are going
- Same product or services
- Worse: it's the next generation of your product!
- Launch product in impossibly short time
- They contact your customers
- They undercut your prices (no R&D costs!)

Law Enforcement

The FBI or Department of Justice contacts you about possible trade secret theft

Logical Deduction

When your engineers say it's just not possible that a competitor could have designed something the same way as there are just too many possible solutions to the same problem

Case: Lightwave Microsystems, Inc.

- Who is Policing the Policeman?:
  - In 2002, Director of IT Brent Woodard
  - Stole his employer's trade secrets in the form of computer back-up tapes in the custody of the IT department
  - Woodard tried to sell the tapes to JDSU, a competitor
  - JDSU contacted the FBI and cooperated with the investigation

Lightwave: "Joe Data"

- In 2002, Lightwave was about to go out of business
- Woodard attempted to cash in on the IP assets
- Woodard created an alias "Joe Data" and an email account: lightwavedata@yahoo.com to sell the tapes
- Woodard sent emails offering to sell the trade secrets to JDSU's Chief Technology Officer
- JDSU immediately contacted the FBI
- The FBI monitored the "Joe Data" - JDSU "sale" negotiations
- Email communications were traced back to Woodard's home address and, with a search warrant, the FBI seized Woodard's home computer and the tapes from his home

Lightwave Case Result

- In 2003 Woodard was indicted of three counts of theft of trade secrets
- In 2005, Woodard plead guilty to one count of trade secrets theft (under 18 U.S.C. § 1832) max penalty is 10 years and $250,000
- In 2006, Woodard received a $20,000 fine and was sentenced to 24 months in prison followed by 3 years of supervised release

Case: Traitors to NetLogic

- NetLogic, another Silicon Valley company, received anonymous email messages that two of their chip design engineers were stealing their trade secrets and trying to set up a new (clone) company in China to compete with them as a direct competitor
- NetLogic had computer forensics done on employee's work computers for evidence
- The FBI later seized the employee's home computers and found NetLogic's trade secrets as well as evidence of attempts to obtain venture capital funding

Traitors to NetLogic Case continued

- Evidence found by the FBI included data, emails and business plans
- At trial it turned out the anonymous tip came from one of the defendant's wives
- The Defendant tried to blame his wife that she made it up to get more time with him!
- In 2009, the jury deadlocked because it wasn't proven that what was stolen was a trade secret, DOJ said they would retry the case
- In 2010, U.S. attorney's office moved to dismiss rather than risk another loss

Conclusion

- You have discovered and confirmed trade secret theft
- The evidence has been collected and preserved, and
- The evidence has been presented to Management so they can decide whether to pursue any action

QUESTIONS?