Trade Secrets on the Internet and in Cyberspace

RUSSO & HALE LLP

Palo Alto, California

New Millennium Business Trends

- Downsizing (and Individual Loyalty)
- Outsourcing (and Proprietary Information)
- Re-engineering (and Knowledge Workers)
- Knowledge Capital (and Who Owns It)
- Electronic Commerce (and Controls)
- Virtual Organizations (and Value Added)
- Worldwide Global Network (and Access)

Key Questions

- Can Trade Secrecy Co-Exist with the Worldwide Global Network (INTERNET)?
- Is the soul of the INTERNET: individual freedom or corporate property?
- Will Trade Secrets Become Obsolete or More Crucial in the Next 10 Years?
- What Should Companies (and their Lawyers) Do in the Meantime?

Today's Topics for Discussion

- Overview on Trade Secret Law
- Trends in Nationwide Trade Secret Law
- Trends in California Trade Secret Practice
- What Must Our Supreme Court Decide?
- What Recommendations Should Counsel Make to Their Clients in Light of Trends?

Trade Secret Law

- Restatement (Second) of Torts
- Uniform Trade Secret Act
- California Uniform Trade Secret Act
- Federal Economic Espionage Act
- Digital Millennium Copyright Act
- Other Federal and State Laws

Restatement (Second) of Torts

- Formula, pattern . . . compilation of information (SUBJECT requirement)
- used in one's business (ACTUAL USE requirement?)
- gives competitive advantage (ADVANTAGE requirement)
- over those who do not know or use it (SECRECY requirement)

Uniform Trade Secret Act

- information including a formula . . .or process (SUBJECT requirement)
- derives independent economic value, actual or potential (VALUE requirement)
- from not being generally known and not being readily ascertainable (SECRECY)
- and is subject of reasonable efforts to maintain secrecy (SECRECY PROGRAM)

California Uniform Trade Secrets Act

- information including a formula . . . or process (SUBJECT requirement)
- derives independent economic value, actual or potential (VALUE requirement)
- from not being generally known (SECRECY) [deletes "readily ascertainable"]
- and is subject of reasonable efforts to maintain secret (SECRECY PROGRAM)

Federal Economic Espionage Act of 1996

- all forms . . . of . . . information . . . tangible or intangible (**SUBJECT**)
- derives independent economic value, actual or potential (**VALUE** requirement)
- from not being generally known and not being readily ascertainable (**SECRECY**)
- and is subject of reasonable efforts to maintain secrecy (**SECRECY PROGRAM**)

The Digital Millennium Copyright Act 1998 (DMCA)

- Future of Cyberspace - Protection by Digital Lock, e.g. ,web page password
- Prohibits "breaking and entering" through a technological measure that effectively controls access (**SECRECY PROGRAM**) to any copyrighted work, even if the information taken is not copyrighted (**SECRECY**)
- The DMCA may be used to provide a type of potential federal protection for trade secrets

State and Federal Trade Secret Law: Summary of Requirements

	Restate-ment	"Uniform" UTSA	California UTSA	Economic Espionage	Federal DMCA
Subject	formula, pattern, compilation	information, including formula or process	information, including formula or process	all tangible or intangible information	any information, if some is copyrightable
Value	used for advantage	actual or potential independent value	actual or potential independent value	actual or potential independent value	none
Secrecy	others do not know	not generally known and not readily ascertainable	not generally known and not readily ascertainable	not generally known and not readily ascertainable	none
Program	None	reasonable efforts to maintain secrecy	reasonable efforts to maintain secrecy	reasonable efforts to maintain secrecy	digital lock

Summary of Law

- Uniform Act definition is broader than Restatement definition
- Federal Economic Espionage Act definition is broader than Uniform Act
- California Act is potentially even broader than both the Uniform and Espionage Acts
- DMCA made be the broadest of all:
  - "Digital Lock" approach with broad remedies, nationwide jurisdiction, and potentially broad criminal exposure (e.g., attempts)

Trade Secret Plan Requirements v. Internet and Cyberspace Facts

- Control
- Centralization
- Certainty
- Confirmation
- Censorship

- Convenience
- Decentralization
- Uncertainty
- Anonymity
- Freedom

Trade Secret Program - Control

- Written agreements
  - Both contractors and employees
- Written acknowledgments
- Exit interviews & termination certificates
- Internal security measures
- External security measures
- Attitude: Corporate Ownership & Control

Cyberspace - Convenience

- Time is most valuable
- Time saved is time owned
- Time is individually owned
- Time is saved when information is free
- Attitude: Personal Ownership & Control

Trade Secret Program - Centralization

- "Need to Know" Limits
- File Centralization
- Remote Access Limits
- Diskette-less CPUs
- Copier, Fax and Site Management
- Attitude: Data & Information = Valuable

Cyberspace - Decentralization

- Providing Laptop Computers = Productivity
- Allowing Remote Access = Efficiency
- Email/Fax/Data Distribution = Communication
- Copying of Email/Voicemail = Teamwork
- Communication + Teamwork = Knowledge
- Attitude: Data & Information = “Commodities”

Trade Secret Program - Certainty

- Identification
- Security
- Encryption
- Shredding
- Audits

Cyberspace - Uncertainty

- Transformation
- Obsolescence
- Convenience
- Burdensome (& Distracting)
- Expensive (& Boring)

Trade Secret Program - Confirmation

- Proprietary Notices
- Proprietary Legends
- Proprietary Information
- Employee Exit Interviews
- Accountability & Responsibility
- Other Required Procedures

Cyberspace - Anonymity

- Unknown
- Unsigned
- Unidentified
- Unidentifiable
- Unaccountable

Trade Secret Program - Censorship

- Papers
- Speeches
- Spam
- Chat (& News) Groups
- File Download
- Other WWW Access
- Review Committees

Cyberspace - Freedom

- First Amendment Rights*
- Federal Rights of Privacy
- California Rights of Privacy
- California Labor Code Section 2870
- California Business & Profession Code Section 16600 (*& Anti-SLAPP Law)

Current Hot Topics- State Law

- Misappropriation v. "Inevitable Disclosure"
  - Threatened misappropriation
  - Effect of Bus. & Prof. Section 16600
  - Effect of trade secret descriptions
  - Competition v. Post-Agreement Restraints

"Threatened" Misappropriation

- What Constitutes "Threatened" or "Inevitable" Misappropriation? Pepsico, 54 F.3d 1262 (7th Cir. 1995)
- Not sufficient to allege that a defendants "could" misuse trade secrets, and/or plaintiff fears they will. Plaintiff must allege at least three elements, namely:
  - That Defendant intends to use the trade secrets,
  - That Defendant is in bad faith or is untrustworthy,
  - That Defendant cannot realistically operate without disclosure and/or use of the trade secrets

“Threatened” Misappropriation - PepsiCo’s Cases Are Minimal Support

- Case 1 - Teradyne Inc., 707 F. Supp. 353 (N.D. Ill. 1989)
  - observed that "[t]hreatened misappropriation can be enjoined under Illinois law" where there is a "high degree of probability of inevitable and immediate . . . use of . . . trade secrets.”
  - Teradyne's complaint failed to state a claim because Teradyne did not allege "that defendants have in fact threatened to use Teradyne's secrets or that they will inevitably do so."

“Threatened” Misappropriation

- Case 2 - AMP Inc., 823 F.2d 1199 (7th Cir. 1987)
  - affirmed the denial of a preliminary injunction on the grounds that the plaintiff AMP had failed to show either the existence of any trade secrets or the likelihood that defendant, a former AMP employee, would compromise those secrets or any other confidential business information.
  - The mere fact that a person assumed a similar position at a competitor does not, without more, make it "inevitable that he will use or disclose . . . trade secret information" so as to "demonstrate irreparable injury."

"Threatened" Misappropriation - Multiple Relevant Factors to Consider

- New Employer's or Departing Employee's Bad Faith, or Underhanded Dealing
- New Employer's or Departing Employee's Good Faith Efforts to Safeguard Trade Secrets of Previous Employer
- New Employer's Product or Service Competes with that of Plaintiff (or present lack of technology, but movement in that direction)
- Departing Employee holds Similar or Identical Responsibilities with New Employer

Importance of Trade Secret Descriptions (and Acknowledgments)

- In a misappropriation action, California Code of Civil Procedure Section 2019(d) requires specific identification of the trade secrets with "reasonable particularity."
  - This is California substantive law - Computer Economics v. Gartner Group, 50 F.Supp.2d 980 (1999)
- In California, without sufficient descriptions of trade secrets, likelihood of injunctive relief is reduced and discovery should not move forward if Protective Order is sought.
- Without this requirement, Trade Secret Misappropriation Allegations can become Instruments for Harassment.

Policies Behind Trade Secret Description Specificity Rules

- Due Process: Provides for proper notice of claims before a defendant is required to defend against those claims
- Efficiency: Protects a defendant from having to respond to discovery that may ultimately prove to be irrelevant.
- Fairness: Prevents a plaintiff from being able to enhance its settlement leverage by requesting unlimited discovery.
- Burden of Proof: Should deter plaintiff from conforming misappropriation claims to the evidence in discovery.
- Competitive Litigation: Should decrease bad faith claims and reduce likelihood of purely competitive lawsuits

Effects of Detailed Trade Secret Description Requirement

- Should promote well-investigated claims and dissuades the filing of meritless claims
- Should prevent plaintiffs from using the discovery process as a means to obtain the defendant's trade secrets
- Should assist the Court in framing the appropriate scope of discovery and in determining whether the plaintiff's discovery requests fall within that scope
- Should enable defendant to form complete & reasoned defenses
- Computer Economics v. Gartner Group, 50 F.Supp.2d 980 (1999)

Federal v. State Law: Erie Analysis Applied to State Description Rule

- No conflict between California requirement of trade secret description and Federal Rule of Civil Procedure Rule 26(c)(7) on Protective Orders.
- State rule of trade secret description is not clearly substantive; but it can be outcome determinative.
- Encourages forum-shopping, and there are no countervailing federal interests outweighing state interests in enforcing the state trade secret description requirement.
- Thus, state rule should apply in Federal Court.

Current Hot Topics- Federal Law

- Federal Expansion of Trade Secret Law
  - Digital Millennium Copyright Act
  - Federal Economic Espionage Act

Federal Protection by "Digital Lock": DMCA's Protectible Subject Matter

- The DMCA protects copyrighted material secured by a "digital lock."
- Non-copyrighted material, e.g., trade secrets included with the copyright material secured by the a digital lock, will also be protected by the DMCA.
- Even non-copyrighted material that is neither copyrightable or subject to trade secret protection may be protected by the DMCA, as long as it is included with copyright material secured by a federally protectible "digital lock."

Exceptions to DMCA "Digital Lock" Prohibitions

- Free Speech
- Fair Use
- Reverse Engineering (but "solely to achieve interoperability of an independently created computer program")
- Encryption Research (but not for purpose of theft)
- Disabling of "Cookies"
- Law Enforcement

Federal Economic Espionage Act
UNITED STATES OF AMERICA v. HSU and HO, 155 F.3d 189

- 18 U.S.C. § 1839(3) provides that a "trade secret" means:
- 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.

Federal Economic Espionage Act
UNITED STATES of America v. HSU. UNITED STATES v. HO, 155 F.3d 189

- Charges of "attempt" and "conspiracy" do not require proof of the existence of an actual trade secret
- Proof only of one's attempt with intent to steal a trade secret is criminal. 18 U.S.C. § 1832(a).
- Even if subject matter of attempt is not secret!
- Thus, Legal Impossibility is not a defense!!

Economic Espionage Act ("EEA")
UNITED STATES v. HSU and HO, 155 F.3d 189

- "Legal Impossibility" not a Defense to Attempt of Trade Secret Theft
- A charge of "attempt" under the EEA requires proof of the same elements used in other modern attempt statutes, including the Model Penal Code.
- A defendant is guilty of attempting to misappropriate trade secrets if, "acting with the kind of culpability otherwise required for commission of the crime, he ... purposely does or omits to do anything that, under the circumstances as he believes them to be, is an act or omission constituting a substantial step in a course of conduct planned to culminate in his commission of the crime." Model Penal Code § 5.01(1)(c) (1985).
- Thus, the defendant must (1) have the intent needed to commit a crime defined by the EEA, and must (2) perform an act amounting to a "substantial step" toward the commission of that crime.

Pushing The Limits of Trade Secret Law

- Novel uses of trades secret law to attempt more general intellectual property protection when other federal and state laws are insufficient.

Pushing The Limits of Trade Secret Law

- When is "reverse engineering" illegal: can a "hacked" solution violate trade secret law when the alleged "reasonable" efforts at protection are through unsigned agreements?
- When does the fact that the information is "not readily ascertainable" make a difference?
- What if the hacker had read the unsigned agreement and in fact, believed the information which he or she has now reverse-engineered to be or have been a trade secret?

Pushing The Secrets of Trade Secret Law

- What if the reverse-engineered solution is otherwise published on the web?
- How might the general UTSA have applied?
- How might the California UTSA have applied?
- How might the Digital Millennium Copyright Act have been used in the DVD encryption case?
- How might the Federal Economic Espionage Act have been used in the DVD encryption case

Key Questions (Again)

- Can Trade Secrecy Co-Exist with the Global Network (INTERNET)?
- What is the soul of the INTERNET: individual freedom or corporate property?
- Will Trade Secrets Become Obsolete or More Crucial in the Next 10 Years?
- What Should Companies (and their Lawyers) Do in the Meantime?

Recommendations

- For Employers
- For Employees
- For Entrepreneurs
- For Consultants
- For Licensees
- For Investors