Trade Secrets on the Internet and in Cyberspace
The Law of the Internet in California Seminar
National Business Institute - May 31, 2001

Jack Russo, Michael Risch, and Mary E. Mullarkey/ Russo & Hale LLP
computerlaw.com℠

I. Introduction & Overview

New millennium business trends in the high tech arena -- more specifically the Internet and new communications standards -- are shifting toward a greater emphasis on trade secrecy, discreet handling of proprietary information, and a greater willingness to communicate on the Internet.

However, the Internet has created a variety of tensions as well:

1. **Downsizing** - and Individual Loyalty
2. **Outsourcing** - and . Proprietary Information
3. **Re-engineering** - and Knowledge Workers
4. **Knowledge Capital** - and determining who Owns it
5. **Electronic Commerce** - and the Controls necessary to acheive it
6. **Virtual Organizations** - and the Value Added they bring
7. **Internet** - and the potential nearly unlimited Access that goes with it

These new business trends lead to several key questions:

➢Can trade secrecy co-exist with the 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?

The following topics discussed here will answer some of these questions:

- ➢ Overview of 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?

II. Relevant Trade Secret Law

There are several sources of trade secret law:

A. Restatement (Second) of Torts

A trade secret is a 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).

B. Uniform Trade Secret Act

A trade secret is 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).

C. California Uniform Trade Secret Act

A trade secret is 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).

D. Federal Economic Espionage Act of 1996

A trade secret is 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).

E. Digital Millennium Copyright Act

This is the future of protection on the Internet - 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.

F. Summary of Requirements

The following is a summary of California state and federal trade secret laws:

- ➢Trade Secrets Are Protected (vs. Patents, Copyrights, or Trademarks)
- ➢No Statutory Registration
- ➢No Examination Process
- ➢No Writing Required (Intangible)
- ➢Potential Perpetual Existence
- ➢Generally State Court Enforcement
- ➢Ideas Alone, if Secret, Are Protectible
- ➢Protection Requires Secrecy Efforts

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

The following table sums up a comparison between the different protection schemes:

	Restate-ment	**"Uniform" UTSA**	**California UTSA**	**Economic Espionage**	**Federal DMCA**
Subject	formula, pattern, complila tion	information, including formula or process	information including formula or process	all tangible or intangible informatio n	any information, if some is copyrightable
Value	used for advant-age	actual or potential independent value	actual or potential independent value	actual or potential independ-ent 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 ascertain-able	none
Program	none	reasonable efforts to maintain secrecy	reasonable efforts to maintain secrecy	reasonable efforts to maintain secrecy	digital lock

III. Trade Secret Plan Requirements v. Internet and Cyberspace Facts

Any solid Trade Secret protection plan should be comprised of the **five C's**: **Control**, **Centralization**, **Certainty**, **Confirmation**, and **Censorship**. However, information and knowledge on the Internet and in Cyberspace often highlight **Convenience**, **Decentralization**, **Uncertainty**, **Anonymity**, and **Freedom**– conditions that can make developing and maintaining the integrity of trade secrets problematic at best.

There is a real tension between the secrecy plan required by the trade secret laws and the norms of the Internet.

Trade Secret Plan Requirements	**Internet and Cyberspace Facts**
Control • Written agreements Both contractors and employees • Written acknowledgments • Exit interviews & certificates • Internal security measures • External security measures **Attitude:** Corporate Ownership & Control	**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
Centralization •"Need to Know" Limits • File Centralization • Remote Access Limits • Diskette-less CPUs • Copier, Fax and Site Management **Attitude:** Information = Valuable	**Decentralization** • Providing Laptop Computers = Productivity • Allowing Remote Access = Efficiency • Email/Fax/Data Distribution = Communication • Copying of Email/Voicemail = Teamwork • Communication + Teamwork = Knowledge **Attitude:** Information = Commodity
Certainty • Identification • Security • Encryption • Shredding • Audits **Attitude:** Surprises destroy	**Uncertainty** • Transformation • Obsolescence • Convenience • Burdensome (& Distracting) • Expensive (& Boring) **Attitude**: "Go with the flow"

Confirmation • Proprietary Notices • Proprietary Legends • Proprietary Information • Employee Exit Interviews • Accountability & Responsibility • Other Required Procedures **Attitude**: Accountability	**Anonymity** • Unknown • Unsigned • Unidentified • Unidentifiable • Unaccountable **Attitude**: Freedom
Censorship • Papers • Speeches • Spam • Chat (& News) Groups • File Download • Other WWW Access • Review Committees **Attitude**: Silence	**Freedom** • First Amendment Rights • Federal Rights of Privacy • California Rights of Privacy • California Labor Code §2870 • California Business & Profession Code §16600 (& Anti-SLAPP) **Attitude**: Learning

IV. <u>Current Hot Topics - State Law</u>

There are several hot topics in the area of trade secrets and the Internet. The wealth offered to individuals who are mobile have really raised the level of concerns in companies with departing employees.

A. Misappropriation v. "Inevitable Disclosure"

1. What Constitutes "Threatened" or "Inevitable" Misappropriation?

To bring a claim for threatened trade secret misappropriation, it is not sufficient to allege that a defendants "could" misuse trade secrets, and/or plaintiff fears they will.[1] 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

These standards, however, are relatively easy to allege and relatively difficult to disprove, giving plaintiffs an advantage in any competitive litigation.

2. "Threatened" Misappropriation: PepsiCo's Cases Are Minimal Support

The Pepsico Court relied on two cases to come to support the pro-plaintiff rule, but these cases do not support the jump to inevitable disclosure.

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

---

[1]The leading case on threatened misappropriation is Pepsi Co. v. Redmond, 54 F.3d 1262 (7th Cir. 1995). No published California decision has adopted the inevitable disclosure rule *per se*.

defendants have in fact threatened to use Teradyne's secrets or that they will inevitably do so."

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."

Neither of these cases provides clear support for the Pepsico decision. Especially given the fact that California Business and Professions Code §16600 creates a strong policy allowing for mobility in the work force. Section 16600 voids any contract provision that purports to limit a person from working in any field (including for competitors). It is difficult to (and no court to date has) reconciled the notion of inevitable disclosure with Section 16600.

3. "Threatened" Misappropriation - Multiple Factors to Consider

In situations where misappropriation is a possibility (e.g. when a crucial employee departs suddenly and begins to work elsewhere in the field immediately thereafter) a potential plaintiff should ask the following:

➢ Did the new employer's or departing employee's act or appear to act with bad faith or underhanded dealing?

➢Did the new employer or departing employee make a good faith efforts to safeguard trade secrets of previous employer?

➢Does the new employer's product or service competes with that of plaintiff (or present lack of technology, but movement in that direction)?

➢Does the departing employee holds similar or identical responsibilities with new employer?

B. 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 (C.D. Cal. 1999). In California, without sufficient descriptions of trade secrets, likelihood of injunctive relief is reduced and discovery should not move forward if a Protective Order is sought. Without this requirement, Trade Secret Misappropriation Allegations can become Instruments for Harassment.

1. Policies Behind Trade Secret Description Specificity Rules

As a means of avoiding harassment or using trade secret misappropriation claims and as a means of preventing a competitor from innovating or otherwise entering a products space, California requires a certain level of specificity in description and certainty of action before a plaintiff can proceed with a lawsuit. Legal reasons for the State's hesitance in proceeding with unsubstantiated claims are as follows:

➢**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

2. Effects of Detailed Trade Secret Description Requirement

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

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

No conflict exists between California requirement of trade secret description and Federal Rule of Civil Procedure Rule 26(c)(7) on Protective Orders. The California state rule of trade secret description is not clearly substantive, but it can be outcome determinative and should thus be considered substantive. Additionally, to not apply the California state rule would encourage 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.

V. Current Hot Topics - Federal Law

The current hot topics in federal law is the expansion of federal law into trade secrets, a traditionally state based law.

A. 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) is protected by the DMCA. The DMCA also protects non-copyrighted material that is neither copyrightable or subject to trade secret protection as long as it is included with copyright material secured by a federally protectible "digital lock."

Exceptions to DMCA "Digital Lock" Prohibitions are as follows:

- ➢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

B. Federal Economic Espionage Act

The Federal Economic Espionage Act, 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.

Criminal charges of "attempt" and "conspiracy" do not require proof of the existence of an actual trade secret, but only proof of one's attempt with intent to steal a trade secret. 18 U.S.C. § 1832(a). **Attempt liability attaches even if the subject matter of attempt is not secret**! In United States v. Hsu and Ho, 155 F.3d 189 (9th Cir. 1999), the court ruled that "Legal Impossibility" is not a defense to attempt of trade secret theft under the EEA. Also, a charge of "attempt" under the EEA requires proof of the same elements used in other modern attempt statutes, including the Model Penal Code. For example, 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.

VI. Conclusion: Pushing the Limits of Trade Secret Law

Companies are using novel uses of trade secret law to attempt more general intellectual property protection when other federal and state laws are insufficient.

This generates even further questions:

➢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?

➢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?