Trade Secrets: Fundamentals, Statistics and Litigation Strategy

By

Aaron Myers

Friday, March 26, 2010

HOWREY LLP

Antitrust Global Litigation Intellectual Property

Types of IP

- **Patents** – protect a thing, an idea, or a method
- **Copyright** – protects literal expression (e.g., the words of a book, song lyrics, software code, product brochures). Does NOT protect underlying ideas
- **Trademarks** – protect names (e.g., product names or service names) to indicate source of origin
- **Trade Secrets** – protect information that is kept secret and that is commercially valuable

Patent Examples

- To protect a physical device such as a sensor cable:

(12) **United States Patent**
McCoy et al.

(10) **Patent No.: US 6,777,947 B2**
(45) **Date of Patent: Aug. 17, 2004**

(54) **SENSOR CABLE**

(75) Inventors: **Kenneth Ferrell McCoy**, Redwood City, CA (US); **Robert Stephen Wasley**, San Carlos, CA (US)

(73) Assignee: **Tyco Thermal Controls LLC.**, Redwood City, CA (US)

4,922,183	A	5/1990	Kamas	324/694
4,926,129	A	5/1990	Wasley et al.	324/555
4,926,165	A	5/1990	Lahlouh et al.	340/603
4,931,741	A	6/1990	Koppitsch et al.	324/525
5,015,958	A	5/1991	Masia et al.	324/522
5,177,996	A	1/1993	Sahakian	73/40
5,191,292	A	3/1993	Klotz et al.	324/446
5,203,202	A	4/1993	Spencer	73/40.5 R
5,235,286	A	8/1993	Masia et al.	324/522
5,313,823	A	5/1994	Berkman et al.	73/40

HOWREY LLP

Patent Examples (cont'd)

- To protect a method:


US007322415B2

(12) **United States Patent**
de St. Remey

(10) **Patent No.: US 7,322,415 B2**
(45) **Date of Patent: Jan. 29, 2008**

(54) **SUBTERRANEAN ELECTRO-THERMAL HEATING SYSTEM AND METHOD**

(75) Inventor: **Edward Everett de St. Remey**, Anchorage, AK (US)

(73) Assignee: **Tyco Thermal Controls LLC**, Redwood City, CA (US)

4,214,147 A * 7/1980 Kraver 392/468
4,284,841 A 8/1981 Tijunelis et al. 174/103
4,303,826 A 12/1981 Ando 219/301
4,490,577 A 12/1984 Neuroth 174/103
4,538,682 A 9/1985 McManus et al. 166/255
4,572,299 A 2/1986 Vanegmond et al. 166/385
4,694,907 A 9/1987 Stahl et al. 166/303
4,707,568 A 11/1987 Hoffman et al. 174/103
5.070.533 A * 12/1991 Bridges et al. 392/301

43. A method of configuring a subterranean heating system for delivering thermal input to localized areas in a subterranean environment, said method comprising:

defining a pattern of at least one heat target region and at least one non-target region within said subterranean environment;

interconnecting at least one cold lead cable section with at least one heater cable section; and

positioning said cold lead section and said heated cable section in said subterranean environment such that said heater cable section extends into an associated one of said heat target regions and adjacent and outside of an oil production tube at least partially disposed with said heat target region for providing a heater cable thermal output to said associated heat target region for heating oil in said oil production tube and such that said cold lead section passes through an associated one of said non-target regions for providing an associated cold lead thermal output less than said heater cable thermal output.

HOWREY LLP

Copyright Example

- To protect creative works including writings, music, pictures and movies:

HOWREY LLP

Copyright (cont'd)

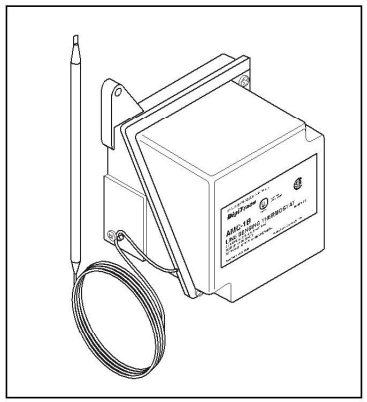
- To protect instructions, manuals, and datasheets:

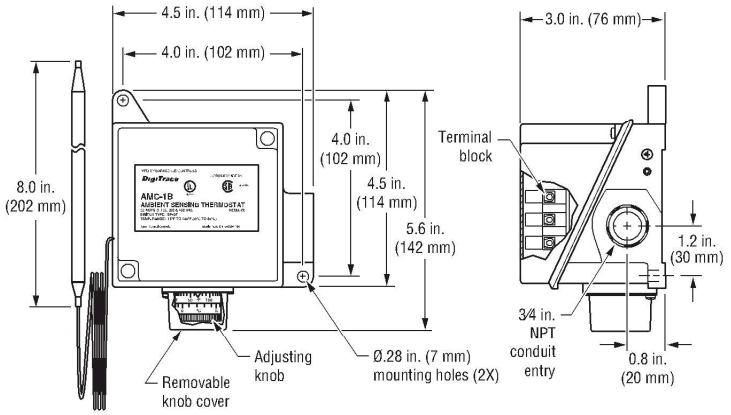
DigiTrace

AMC-1B

Line-sensing thermostat for nonhazardous locations

Installation Instructions





Description

The AMC-1B thermostat is designed for controlling heat-tracing systems in nonhazardous locations. The AMC-1B can be used to control heat-tracing circuits in a pipe-sensing mode (see Figure 1 on back), to indicate low-temperature (Figure 2) or high temperature (Figure 3) alarm conditions, or to control the coil on a contactor (Figure 4).

HOWREY LLP

Trademarks

- To protect product or service names that customers come to associate with the source of origin:

Trade Secrets

- To protect information (e.g., chemical formulas, internal pricing or marketing strategy, business plans, software source code) that is maintained in secret and that is commercially valuable.

Important Differences in Protection

- Patents protect against anyone else using the patented thing or method.
  - "Innocent" infringers just as liable as intentional copiers.
  - Protection lasts roughly 20 years.
- Trade Secret protects only against theft of information.
  - Independent development of information (e.g., reverse engineering) is not protected.

Important Differences (cont'd)

- Trademarks protect against anyone else using your product or service names.
  - Also protect against competitors using names that are not identical but are so close as to cause a "likelihood of confusion" on the part of your customers.
- Copyrights protect only against literal copying.
  - Is a limited form or protection, but is very easy to obtain (no registration process).

Trade Secrets Theft

- The theft of trade secrets
  - is more common than many realize
  - can wreak havoc with a company's business
  - leads to the loss of substantial amounts of money
  - significant impact on employee morale

Trade Secrets Theft (cont'd)

- Exponential Growth
- According to a just-released study *(A Statistical Analysis of Trade Secret Litigation in Federal Courts, Gorgonzola L.R. (2010)*:
  - 1988 – 1995: Doubled.
  - 1995 – 2004: Doubled.
  - At the current rate, will double again by 2017

Trade Secrets Theft (cont'd)

- Companies surveyed each lost on average $4.6 million worth of intellectual property in 2008 due to security breaches. *Unsecured Economies: Protecting Vital Information*, McAfee, Inc. (2009).
  - Based on extrapolation from survey sample, 2008 losses were roughly $1 trillion in aggregate (including value of stolen data and cost of repairing breaches)

Trade Secrets Theft (cont'd)

- Who is stealing?
  - In 85% of cases, someone the trade secret owner knew
  - In 50-60% of cases, employees
  - In 30-40% of cases, business partners
- What is stolen?
  - In 50% of cases, a customer list or other internal business information
  - In 50% of cases, technical information or know-how, such as formulas or software

Trade Secrets Theft (cont'd)

- Nearly 60% of employees who quit a job or are asked to leave are stealing company data. *Data Theft Common By Departing Employees*, Washington Post, Brian Krebs (Feb. 26, 2009) (discussing report by Ponemon Institute).
- Former Intel engineer indicted in November 2008 for stealing Intel trade secrets worth over $1 billion in R&D costs

Why Is This a Growing Problem?

- Increased use of contractors, temporary workers, out-sourcing
- More-frequent job changes
- Organized efforts: there's money to be made in stealing IP
- Data storage devices, *e.g.*, DVDs, portable hard drives, thumb drives
- Internet/Web access and the expanding use of wireless technology
- Globalization: subsidiaries, affiliates and partners in countries with corruption problems or different laws/policies/cultural attitudes toward intellectual property and information security

Examples of Trade Secret Theft

- Burglaries by professional criminals targeting specific technology
- Network attacks (hacking)
- Laptop computer theft
- Employees
  - According to the Ponemon Institute report, among those who took data from their former employer,
    - email was the most frequently stolen (65%), followed by
    - non-financial business information (45%),
    - customer contact lists (39%),
    - employee records (35%) and
    - financial information (16%).

  Data Theft Common By Departing Employees, Washington Post, Brian Krebs (Feb. 26, 2009).

Case Study

Coca-Cola®

Coca-Cola®

- **Type**
  - Criminal
- **Content**
  - Sample of new product
  - Confidential marketing documents
- **Method**
  - Reviewed hard-copy documents, placed into personal bag
  - Placed new product sample into personal bag
  - Downloaded data onto memory stick
- **Proceedings**
  - Convicted and sentenced for conspiracy to commit theft of trade secrets, in violation of 18 U.S.C. § 1832(a)(1), (3), and (5) (Economic Espionage Act of 1996)
  - 8-year sentence for secretary, $40,000 in restitution
  - 5-year sentence to non-cooperating co-defendant, $40,000 in restitution
  - 2-year sentence to cooperating co-defendant
  - 3/20/08: 11th Circuit affirmed convictions of secretary and co-defendant

Coca-Cola® CEO Memo to Employees

07/05/06
Memo from Chairman and CEO Neville Isdell to All Employees Worldwide Regarding Trade Secrets Investigation

EXECUTIVE OFFICE MEMORANDUM
Atlanta, GA
July 5, 2006
TO: ALL EMPLOYEES WORLDWIDE

Today, the Federal Bureau of Investigation and the United States Attorney's Office of the Northern District of Georgia successfully concluded an undercover operation that thwarted an attempt to steal and sell Coca-Cola trade secrets. The Company contacted the FBI after we were alerted that individuals were offering to sell our confidential information on the open market.

I am pleased to report that the individuals responsible for this crime have now been apprehended. The Company is cooperating fully with the government's investigation and prosecution of this matter. As this is an ongoing criminal matter, we are limited in what we can communicate. However, it should be noted that no personal employee information was ever at risk.

Sadly, today's arrests include an individual within our Company. While this breach of trust is difficult for all of us to accept, it underscores the responsibility we each have to be vigilant in protecting our trade secrets. Information is the lifeblood of the Company. As the health of our enterprise continues to strengthen and the breadth of our innovation pipeline continues to grow, our ideas and our competitive data carry increasing interest to those outside our business. Accordingly, I have directed a thorough review of our information protection policies, procedures and practices to ensure that we continue to rigorously safeguard our intellectual capital.

I would like to thank our Security and Legal teams for the manner in which they assisted law enforcement in this unfortunate situation. I would also like to express our sincere appreciation to PepsiCo for alerting us to this attack.

Let me end by emphasizing our shared responsibility to protect the intellectual capital of our Company and by encouraging us to continue working together in moving our business forward.

NEVILLE ISDELL

Outline of This Presentation

- Statutory definition of trade secret (civil)
- Plain English definition
- Examples of trade secrets
- The three main factors
  - Secret
  - Commercial value
  - Reasonable efforts
- Examples of reasonable efforts

The U.S. Statutory Definition of a Trade Secret (Civil)

"Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and

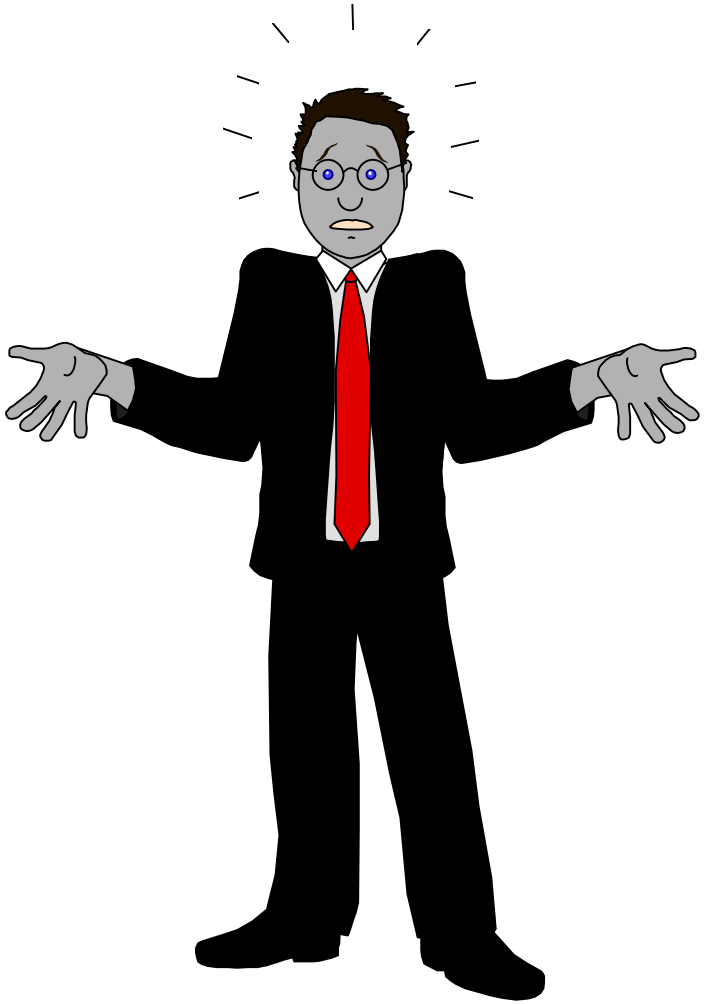
(2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Cal. Civil Code §3426.1(d) (California Uniform Trade Secrets Act).

Plain English, Please . . .

There are three principal legal requirements for a trade secret:

1. The information must be secret.
2. The information must have actual or potential commercial value because it's secret.
3. The owner must have made reasonable efforts to keep the information secret.



Ah, So a Trade Secret Is . . .

In the U.S., Trade Secret Theft Is Also a Crime

- Second-highest priority of the U.S. Department of Justice after terrorism
- The Economic Espionage Act of 1996 criminalizes trade secret theft
  - involving interstate commerce with knowledge or intent to injure trade secret owner

– or –

  - with knowledge or intent that theft will benefit a foreign power

Examples of Trade Secrets

- New product names
- Algorithms, formulas, data flow charts and specific procedures implemented in software
- Technical data about product performance
- Business plans & strategies

Examples of Trade Secrets (cont'd)

- Financial projections
- Marketing plans, unpublished promotional material
- Cost & pricing information
- Sales data
- Customer lists
- Info re: new business opportunities
- Personnel performance

Case study

Google

1. Secret

- "Not generally known among or easily accessible to persons within the circles that normally deal with this kind of information"
- So a trade secret will not include, for example:
  - Matters of common knowledge
  - Information you find at library, online database, trade journals etc.
  - Published price lists
- Not required that it be known only by one person
  - *e.g.*, may be based on supplier relationship, joint development agreement, due diligence investigation etc.

2. Commercial Value

- Must confer some economic benefit on the holder
- This benefit must derive *specifically* from the fact that it is not generally known – not just from the value of the information itself
- Ways to demonstrate:
  - benefits derived from use
  - costs of developing the trade secret
  - licensing offers
- May be actual or potential

3. Reasonable Efforts

- "Reasonable" → case by case
  - reasonable security procedures
  - non-disclosure agreements (NDAs)
  - such that the information could be obtained by others only through improper means
- Importance of proper trade secret management program
- (More on this in a few minutes . . .)

Case Study

Intel

Intel

- **Type**
  - Criminal
- **Content**
  - Design details on Intel's newest chips
  - Instructions on how encrypted documents could be reviewed when not connected to Intel's network
- **Method**
  - Resigned as of date 1-1/2 weeks in the future, remained on payroll while using accrued vacation time and under Intel procedures retained access to Intel network
  - Lied during exit interview and kept Intel-issued laptop
  - Remotely accessed network and downloaded documents
- **Proceedings**
  - Indicted in November 2008 on 1 count of trade secret theft, 4 counts of wire fraud
  - Facing up to 10 years of imprisonment on the trade secret charge, and an additional 20 years on each of the wire fraud counts, 3 years of supervised release per count, a fine on each count of $250,000 or twice the gain or loss, restitution to Intel, and forfeiture

Case Study

HP

HP

- **Type**
  - Criminal
- **Content**
  - Information re IBM product costs and materials re management of printers and other output devices
- **Method**
  - Requested and obtained documents marked “IBM Confidential” from IBM Pricing Coordinator who directed Malhotra “given the sensitive nature of the material please do not distribute.”
- **Proceedings**
  - June 27, 2008 charged by criminal information with trade secret theft in violation of 18 U.S.C. § 1832(a)(2) (Economic Espionage Act of 1996)
  - July 2008 pleaded guilty to one count of stealing trade secrets, faces maximum sentence of ten years imprisonment and $250,000 fine.
  - December 18, 2008 sentenced to 5 months prison on count 1 of the Information; 3 years supervised release; $100.00 special assessment; and $3,000.00 fine.

Case Study

Air Canada

Air Canada

- **Type**
  - Civil
- **Content**
  - Confidential data on passenger loads, scheduling and pricing
- **Method**
  - Misuse of ex-employee's password to access Air Canada's internal booking site
- **Proceedings**
  - Lawsuit by Air Canada for $220 million in damages for lost sales and profit
  - Settlement: public apology, $15.5 million paid by WestJet

Reasonable Efforts

Trade Secrets Assessment

1. Identify Trade Secrets

- Accurate record keeping is imperative.
- Relevant factors include:
  - Is it known outside the company?
  - Is it widely known by employees and others involved within the company?
  - What measures have been taken to guard its secrecy?
  - What is the value of the information for your company?
  - What is the potential value for your competitors?
  - How much effort/money have you spent in developing it?
  - Have you kept detailed logs of research and development work?
  - How difficult would it be for others to acquire, collect or duplicate it?
- Audit as necessary

2. Develop a Protection Policy

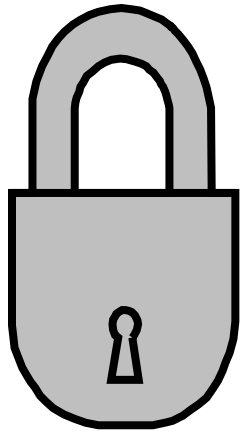
- Reduce policy to writing:
  - Provides clarity on how to identify and protect
  - Provides guidelines on how to reveal inside and outside the company
  - Demonstrates a commitment to protection → **important in litigation**
- Educate and train:
  - Clear communication and repetition
  - Make the policy readily available, *e.g.*, on your intranet
  - Make it clear that disclosure of a trade secret may result in termination and/or legal action
- Monitor compliance and prosecute violators

3. Need to Know

- Restrict access to only those persons having a need to know the information
- Limit each employee's computer access to data actually used/needed for a transaction

4. Physical Protection

- Separate locked depository
- Locked offices and drawers
- Authorization and access control
  - Access log: person, document reviewed
  - Biometric palm readers or equivalent
- Surveillance of depository/company premises
  - Guards, surveillance cameras
- Shredding
- Oversight including audit trail



5. Restrict Public Access to Facilities

- Log and visitor's pass
- Escort visitor
- NDA as necessary
- Overheard conversations
- Documents left in plain view
- Unattended waste baskets
- Visible to anyone walking through a company's premises
  - e.g., type of machinery, layout, physical handling of work in progress

6. Mark Documents

- Label as confidential any documents – hard copy and electronically stored information – that contain or reflect trade secret information
  - Helps employees recognize trade secrets, prevents inadvertent disclosure
- Uniform system of marking documents

7. Digital Protection

- Password and other access control
  - Record employee access, downloading, and viewing of confidential and proprietary documents
  - Restrict access: need to know
  - Terminate access promptly for departing employees
- Secure transactions for intranet access
- Monitor remote access to servers
- Firewalls
- Anti-virus software
- Encryption
- Physically isolate and lock computer tapes, discs, other storage media
- Prohibit/limit/disable portable storage, USB ports
- Mark confidential

8. Travel

- May/June 2008 media reports:
  - Chinese officials suspected of secretly copying the contents of a US government laptop computer during December 2007 trade talks visit by Commerce Secretary Carlos Gutierrez.
  - Copying is believed to have occurred when his laptop was “left unattended”
- Exercise caution when traveling, especially overseas – guard against loss or theft of papers, laptops, cell phones, BlackBerries etc.
  - “Sanitized” laptop
  - Disposable cell phone
  - Assume hotel rooms, offices etc. may be accessed at any time without your consent or knowledge
  - Don’t leave important data/devices unattended

9. New Employees

- Brief on protection expectations early: explain the importance of keeping proprietary information secret and the value to the company
- Cover obligations owed to former employer
- NDA/CA
- Non-compete provision

10. Departing Employees

- Limit access to data as departure date nears
- Stop access to data immediately upon notice
- Exit interview:
  - require return of trade secret materials – in fact, all company documents and materials
  - ditto for all company laptops, PDAs etc.
  - remind non-disclosure agreements/execute
- Consider how you should treat hardware and data
  - forensic image of hard drive?

11. Third Parties

- Applies to suppliers, consultants, financial advisors, programmers, Web site hosting company, designers, subcontractors, joint ventures
- Confidentiality agreement, NDA
- Limit access on need-to-know basis
- Compartmentalize, *e.g.*, use different vendors to manufacture different parts of a product
- Plant tours

California Code of Civil Procedure 2019.210

In any action alleging the misappropriation of a trade secret under the Uniform Trade Secrets Act (Title 5 (commencing with Section 3426) of Part 1 of Division 4 of the Civil Code), **before commencing discovery** relating to the trade secret, the party alleging the misappropriation shall **identify the trade secret with reasonable particularity** subject to any orders that may be appropriate under Section 3426.5 of the Civil Code.

- Enacted as CCP 2019(d) in 1986, later amended
- Became 2019.210 in 2004 without additional change

The Purposes of CCP 2019.210

"The disclosure rule for trade secrets serves four purposes:

(1) to 'promote [] well-investigated claims and dissuade[ ] the filing of meritless trade secret complaints';

(2) to 'prevent [ ] plaintiffs from using the discovery process as a means to obtain the defendant's trade secrets';

(3) to 'assist [ ] the court in framing the appropriate scope of discovery and in determining whether plaintiff's discovery requests fall within that scope'; and

(4) to 'enable [ ] defendants to form complete and well-reasoned defenses, ensuring that they need not wait until the eve of trial to effectively defend against charges of trade secret misappropriation.'"

Pixion, Inc. v. Placeware, Inc., 421 F. Supp. 2d 1233, 1242 (N.D. Cal. 2005), (quoting *Computer Econs., Inc. v. Gartner Group, Inc.,* 50 F. Supp. 2d 980, 985 (S.D. Cal. 1999))

Does CCP 2019.210 Apply in Federal Court?

- *nSight, Inc. v. PeopleSoft, Inc.*, 296 Fed.Appx. 555, 560 (9th Cir. 2008) (affirming summary judgment because "nSight did not identify any trade secret with reasonable particularity. Cal. Civ. Pro. § 2019.210")

- *Applied Materials, Inc. v. Advanced Micro-Fabrication Equipment (Shanghai) Co., Ltd.*, 2008 WL 183520 (N.D. Cal. Jan. 18, 2008) (granting protective order and compelling disclosure of trade secrets under Rule 26 without deciding whether 2019.210 applies in federal court)

- *Advante Intern. Corp. v. Mintel Learning Technology*, 2006 WL 3371576 (N.D. Cal. Nov. 21, 2006) (granting defendant's motion for protective order based on plaintiff's inadequate disclosure, stating "the Court has not concluded that application of section 2019.210 is mandatory in federal court proceedings, but the statute provides an appropriate guide in the absence of specific provisions in the federal rules governing trade secret discovery")

Does CCP 2019.210 Apply in Federal Court? (cont'd)

- *Neothermia Corp. v. Rubicor Medical, Inc.*, 345 F.Supp.2d 1042, 1043-1044 (N.D. Cal. Nov. 14, 2004) (finding 2019.210 applicable in federal court not only to theft of trade secrets but also to disclosure of trade secrets in violation of a nondisclosure agreement)
- *Computer Economics, Inc. v. Gartner Group, Inc.,* 50 F.Supp.2d 980, 992 (S.D. Cal. 1999) (finding 2019.219 applicable to federal cases pursuant to the *Erie* doctrine)
- *Resonance Technology, Inc. v. Koninklijke Philips Electronics, N.V.*, 2008 WL 4330288 (C.D.Cal., Sept. 17, 2008) (denying defendant's motion for identification of trade secrets as premature; good summary of how courts have differed re 2019.210)
- *Funcat Leisure Craft, Inc. v. Johnson Outdoors, Inc.*, 2007 WL 273949 (E.D.Cal. Jan. 29, 2007) (finding 2019.210 to be a state rule of civil procedure that is inapplicable in federal court)