A Multidisciplinary Approach To Trade Secret Protection in the Digital Age

By David C. Brezina

Law and Business

Between James Bond's brand of espionage and the emotional reaction when someone trained and trusted leaves and goes to work in competition lie most fact situations that give rise to trade secret disputes. These wrongs and their subjects overlap legal disciplines of intellectual property, employment and unfair competition.

Assume a Trade Secrets Case – How Should The Business Prepare?

There are three categories of trade secrets case. One is the tort action for the protection of the owner of a trade secret for unlawful appropriation.[1] Second is an action brought by employers against employees to prevent disclosure to others.[2] These actions are based upon either a confidential relationship or a restrictive covenant. Third is an action based on a contract involving the use of the trade secret.[3]

The Uniform Trade Secret Act (USTA) typically pre-empts other tort actions arising under trade secret facts. Winning a UTSA case is enhanced if facts surrounding events prior to the tort establish the basis for the action. The trade secret plaintiff must prove (1) the existence of a trade secret and (2) the misappropriation.[4]

These two elements are deceptively simple. The UTSA requires a "trade secret" to be: (1) sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and (2) the subject of efforts that are reasonable to maintain its secrecy or confidentiality.[5]

The Subject Must Relate To and Provide A Commercial Advantage in Business

Customer lists, manufacturing and marketing plans, financial information, manufacturing techniques and product designs, can all be protectable if the other prerequisites are met[6]. These are examples of typical business information that may give a business an advantage over competitors who do not have the information. General knowledge and skill of a worker can be transportable to a new job.[7]

"Secrets" Are Not Generally Known and Are Subject to Protective Steps

If all the industry insiders know it, it is hard to show secrecy. Industry knowledge, something mobile employees regularly bring with them, the subject of talks or papers at conferences, disclosures in patents,[8] copyrights or public bids are hard to be protected as secrets. It must be "sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use".[9]

The owner must also "keep" the secret. If security measures are foolproof, you can stop reading now. If someone "gets away" with the secrets, then by definition, security is imperfect. Failure to take reasonable precautions can cause the lawsuit to be lost. Locks, passwords, limited access, visual protection, shredders, computer security, explanations and consistent procedures can all help. Cases are lost when blueprints are left lying about and employees freely take information home.

The Taking or Use Violates Some Duty or Involves Some Other Wrongful Act

The definition of the wrong pigeonholes trade secret and unfair competition cases. Ex-employees may have acted in violation of a duty of loyalty to their employer, violated an express contract such as a "Non-compete" agreement, a specific employment agreement, or acted contrary to guidelines such as a policy manual. Interpreting these agreements in the US varies from state to state. Enforceability varies based on the form and timing of agreement and the interrelationship of agreements and policies.

Trade Secrets Acts bring more uniformity to trade secret law. The definition of what can be a trade secret and the standards for what constitutes wrongful taking are provided in these statutes. Trade secret misappropriation covers the disclosure or use of a trade secret without consent of its owner.

Misappropriation does not require evil intent. A trade secret violation can occur where knowledge that is so intimately involved with the operation of its business that working for a competitor will inevitably disclose the secrets.

Information Protectability Depends on Its Nature, Medium and the Steps Taken to Protect

A first step is to identify the information. Identification before the horse escapes the barn will enhance the utility of closing the door. Thoughtful consideration of what ought to be protected will enhance the protective mechanism. The medium in which the property is maintained will suggest security measures. Passwords for computers will not necessarily protect actual blueprints or manufacturing processes which should be screened from visitors, but consideration of those other pieces of property will then suggest drawers, locks, screens, security passes and even visitors' confidentiality agreements.

If the worst happens and it is necessary to enforce the proprietary rights, having their identification in hand will at least enhance the speed at which a remedy can be sought, and may be required.[10] It is not enough to point to broad areas of technology and assert that something there must have been secret and misappropriated. The plaintiff must show concrete secrets.[11] Finally, consideration of the nature and medium of the property may suggest other modes of protection, such as copyright.[12]

Contractual and Employment Law Considerations

1. Planning

The considerations above enable planning for appropriate communication of concerns to employees and prospective employees, consistent emplacement of policies and appropriate drafting of contractual obligations. Employees at different levels will have different obligations and opportunities to negotiate.

But thought should be given to the use of 'boilerplate' language. The language may be appropriate, but the analysis should loop back to a check on what property the company has that needs to be protected, the steps needed to protect the property and whether the current system is adequate.

Consider the phrase "No employee may discuss or disclose any Company trade secrets or proprietary or other confidential information outside the Company…". Are there three categories of information (1) trade secret, (2) proprietary information and (3) confidential information? Should one add the category "non-public" information? Are these redundant because of the UTSA's preemption, or common law?[13]

2. Definition of the Protected Information

Many types of information, the use or disclosure of which would be undesirable, are in the above categories and protectable independent of trade secret law. "Proprietary" information, derived from the word property –in some contexts might encompass patent, trademark or trade dress subjects.[14] Nevertheless, the term is typically used in a context where it is expected to cover trade secrets.[15]

'Confidential information' is also a term often used interchangeably with 'trade secrets.' Indeed, its theft can give rise to a mail fraud claim because confidential business information is property.[16]

'Non-public' information that does not rise to level of trade secret protection may even exist.[17] Even attempted secrecy can be sufficient for protection.[18]

If 'not generally known' is applied literally, things may be 'non-public' and therefore meet that prong for trade secrets. A more narrow interpretation could yield information that is known to a sufficiently large or diverse 'audience', yet is still not 'public.' There may also be nuances such as individual pieces of information being public while a particular

assemblage is not. These 'should' be trade secrets, but a contract having a more broad term could be advantageous because a breach of contract case can be maintained without preemption.

3. Labeling

Labeling information "trade secret" or "confidential information" does not conclusively establish that such information is in fact a trade secret.[19] But it helps corroborate treatment as secret by the proprietor and knowledge of that treatment by the recipient.

Business and Legal Multidiscipline

At this stage in the story, a recap shows that we are touching on a number of management functions. Executives need to decide whether the value of a trade secret is worth the time spent in protecting them. Depending on the secret, Research & Development and engineering are traditional repositories for trade secrets, but marketing and financial information is also valuable[20]. Information Technology and physical security needs to be evaluated. Human Resources will typically be the interface with the employee and likely have mechanisms in place to announce a policy and have employees acknowledge that policy.

Contracts with employees or others who receive trade secrets can address address different aspects. These can include the existence and acknowledgement of the secrets, their non-disclosure and often non-compete terms after the relationship has ended.

Contractual Limits in Scope

Non-compete agreements familiarly are required to be limited in scope and time[21]. Confidentiality agreements similarly have been interpreted to require scope and time limits.[22]

As mobility and the remote transaction of business have increased, courts will consider the proposition that no geographical limit is required, where necessary to protect the business. For example a former executive, whose office was in California was enjoined from competing anywhere in the world[23]. The term was necessary to protect the former employer's trade secret information. The contractual requirement for territorial limitation (or not) may not be read into an action under the UTSA[24].

Incoming Secrets and Property

When hiring, the thought process must shift from offense to defense. Receiving and using confidential information can be actionable. New hiring should be accompanied by a thoughtful review of what can and cannot be used.

Multidisciplinary Legal Doctrines

Just as different business functions overlap and address portions of trade secret concerns, separate legal doctrines can come to play. The UTSA preempts common law counts that provide remedies for conduct equivalent to trade secret misappropriation, preserving only breach of contract. Thus, causes of action for fraud[25], breach duty of loyalty, tortious interference[26], and breach of fiduciary duty[27], have been preempted. Equitable actions such as *quantum meruit*[28] and quasi-contract[29], have also been held preempted. Depending on proper pleading and adequate factual distinctions, some causes of action are preempted, or not, including tortious interference[30], conspiracy to steal confidential information, conversion[31], tortious interference[32] and unjust enrichment[33] may or may not be preempted.

UTSA preemption does not extend to Federal actions. Often trade secrets claims arise in cases along with trademark infringement[34], trade dress infringement[35] or copyright infringement[36]. Trade secrets involving technology can interrelate to patent subject matter[37]. Indeed, state law false advertising also avoids preemption, where not based upon the misappropriation of trade secrets[38].

Just as careful planning before the misappropriation can make or break the cause of action, careful evaluation of all the misconduct and pleading the same can preserve alternative remedies. The model outlined above for maximum protection may not be met by real world facts. The trade secret case may be in doubt, or the misconduct may go beyond mere trade secret misappropriation.

Applying Legal Theories In Fact Situations

It is important to consider all aspects of the fact situation when it arises. The general considerations described for laying the groundwork for trade secret protection discussed above will often be addressed by counseling from a general business or employment perspective. Trade secret situations are fact intensive. These facts point to complementary areas of the law. The employment lawyer may deal with wage and loyalty issues, the intellectual property lawyer with patent, trademark and copyright and the commercial litigator with a full range of contractual and tortious actions. Too narrow a focus can lead to missed opportunities. Three anecdotal situations point out these overlaps and opportunities.

1. The Independent Contractor Hypothetical

Assume a service business organized on a model in which the business does the advertising, promotion and receives orders for services. The actual services are performed by independent contractors, who work on a commission, but deliver their call reports and payments to the business. One independent contractor decides that a higher percentage would be in his best interest. Instead of turning in a series of call reports and checks from customers, he starts his own competing business, calling on many of the same referral sources. In order to bet up to speed faster, he uses the call report forms of the business. As a trade secret case there are potential issues. In the absence of an agreement recognizing confidentiality, proof of the secrecy of the customer list, and indeed proof that it in fact belonged to the business, would lead to a complex case. Fortunately, the business had registered a copyright in its forms. A Federal complaint for copyright infringement could lead to rapid resolution of the dispute by judgment entered in favor of the business. Copyright damages and attorneys fees offset the unpaid commissions – the contractor asserted his own right to wages[39]. Depending on the relationship and conduct of the business, other rights might be implicated, such as the in Sales Representative termination laws[40].

2. Blueprints and Technical Information

A classic trade secret, blueprints can convey much key information. Misappropriation can enable a start- up to be up to competitive speed without substantial research and development. Manufacturing technology is a classic subject for patents but patent planning and prosecution may not be fast enough to address a misappropriation. At the other end of the spectrum, the patent is public, and expires, so some information may be kept trade secret out of a conservative concern that infringement may be hard to discover (so why tell all the secrets) or the competitive edge may be hoped to be perpetual. Patent law may not necessarily provide the remedy, for strategic, tactical or factual reasons.

Blueprints provide an example of other twists in protecting information. First, consider the traditional blueprint – paper, imprinted with graphics – and second the modern Computer Aided Design (CAD) computer file[41]. Unlike many forms of business information, blueprints are intensely graphic. The paper versions are typically large and must be precisely drawn and reproduced. The computer versions can include complex layering, enable zooming on detail, and can be in three dimensions. Yet, both can be reproduced, and are most useful if reproduced exactly.

Unauthorized copying of blueprints and use by a competitor is a classic misappropriation of trade secrets scenario and therefore requires proof of things like the steps taken to preserve secrecy. Suppose, however, that blueprints were left out in a workshop, shown to vendors[42] or were generally not secured in locked drawers, and the like. In the digital age, burning a CD or e-mailing a blueprint to a customer or even prospective customer is the equivalent of leaving the paper document out for all to see.

However, as a graphic work, the blueprint is copyrighted and can be registered. Even where misappropriation is discovered and time is short, Copyright Office regulations permit “Special Handling.”

Both basic copyright considerations — creation, ownership and originality — and specific special handling considerations must be addressed. Time is often of the essence, but short-cuts must be avoided. Consider authorship, work-made-for-hire and derivative work issues promptly[43]. Complete the application thoroughly and thoughtfully and get any necessary assignments in order.

Every copyright application must be accompanied by a deposit, in the normal case, or identifying material, where the nature of the work requires[44]. Depositing an entire disclosure of a trade secret in the Library of Congress is a good way to lose secrecy. However federal copyright is now available for unpublished works that the author intends never to see the light of day[45].

The use of identifying material is key. Depending on the nature of the work and its medium, three alternatives are typical. First, unpublished pictorial or graphic works expressly are expressly permitted to be supported by either one complete copy or identifying material. Second, but not typically applicable to the graphic feature of blueprints, for computer code, identifying material is required, comprising typically the first 25 pages and last 25 pages of code[46]. Third, the Register of Copyrights also permits special relief[47]. Between copyright office rules and practices, a redacted blueprint meeting the "necessary to show the entire copyrightable content" and not "less than an adequate representation of such content" standards should suffice. Consideration of various redaction methods, e.g. graphically masking 49%, redacting dimensions, turning off or using an illegible font for CAD layers, could all be considered.

With the letter transmitting, explaining the reason for special handling, and which may include the request for special relief, the application and identifying material, the regular fee[48] and special handling fee[49] need to be submitted. The Copyright Office's aspirational goal for special handling is five business days. Copyright may be a viable option.

3. Customer Lists

Customer lists and mailing lists are problematic in trade secret cases. Their source, security and protectability are subject to both the individual fact situations and their own legal rules[50]. Consider, however, that in the digital age, most customer lists and mailing lists are maintained on computer and are truly a 'database.' Like business forms and blueprints, ease and precision frequently give rise to copying and an act effectuating misappropriation. Simply 'running' a program in a general purpose computer typically writes all or a portion of the program to memory (RAM) resulting in an infringing copy[51].

Accessing an electronic customer list will typically require a computer and likely a user identification and password. Use of a company computer and 'burning' a copy gives rise to one fact situation, but use of a personal computer and remote access or access after a user id and password became unauthorized yield added facts. A database is entitled to unique copyright protection. Unauthorized use on a computer network implicates computer fraud with both civil and criminal consequences.

a. Database Copyright

The Copyright law addresses databases. A comprehensive list has long been copyrightable[52]. This protection is adequate for print publication where a copy can be sent as a deposit to the Copyright Office with a registration. Indeed, one could register one's customer list periodically, and repetitively. Dynamic databases that are frequently changing are problematic under traditional registration procedures. Often a customer list changes minute-by-minute, so there is an issue about what is actually registered.

The Copyright Office issues registrations for Automated Databases. This can be for either single basic registration covering the database as published on a given date or, if unpublished, as created on a given date as a group registration for a database with its updates or revisions (or for only its updates/revisions) added over a period of time. The latter specifically addresses the dynamic database or mailing list.

Specific registration procedures are provided by the Copyright Office. Notable is the treatment of the nature of authorship — original data or a compilation — and the derivative status of the work — compiled from previously published, or use of unpublished information. Precise identification of the date and version of the database is important. Deposit procedures include identifying material for each "file" included in the database. Special relief dealing with trade secrets is specifically mentioned. Group registration addresses the updates to a constantly changing database[53]

The timely registered customer list will enable the owner to obtain statutory damages, attorneys fees, willful infringement damages and injunctive relief. Even if not registered within 3 months of publication (or before infringement) actual damages and injunctive relief will be available in Federal court.

b. Computer Fraud

Password protection potentially implicates computer fraud. The Computer Fraud and Abuse Act[54] recognizes violation through either unauthorized access or exceeding authorized access.[55] Illinois has its own Computer Crime statute, with certain civil remedies.[56] The second scenario gives the fact of exceeding authority, at a minimum, or unauthorized access. This has been called by one commentator a "Federal Trade Secrets Act" equivalent.

Conclusion

A multidisciplinary approach crosses business lines and legal lines. Preparation on the business side greatly enhances likely protection if misappropriation occurs. Identification of protectable subject, notice, security and, where possible, contractual protection can be enhanced by working with those responsible for human resources, research and development and executive functions. Anticipation of intellectual property protection, filing patent and copyright applications where applicable can provide benefits when information is taken, because this property may embody the information. Crossing legal lines between contract, tort and intellectual property can maximize remedies through thoughtful and careful pleading of remedies to reach the goal of halting unfair competition.

Endnotes

[1] *Bimba Mfg. Co. v. Starz Cylinder Co*. 119 Ill. App. 2d 251, 256 N.E.2d 357 (1969); *Smith v. Dravo Corp*. 203 F.2d 369 (7th Cir. 1953)
[2] *ILG Industries, Inc. v. Scott* 49 Ill. 2d 88, 273 N.E.2d 393 (1971); *Schulenburg v. Signatrol, Inc.* 33 Ill. 2d 379, 212 N.E.2d 865 (1965)
[3] *Warner-Lambert Pharmaceutical Co. v. John J. Reynolds, Inc.* 178 F. Supp. 655, (S.D. N.Y. 1959), aff'd 280 F.2d 197 (2d Cir. 1960); *Laff v. John O. Butler Co.* 64 Ill. App. 3d 603, (Ill. App. Ct. 1978)
[4] *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1268, 35 U.S.P.Q.2d 1010 (7th Cir, 1995) cited with approval in *Strata Marketing, Inc., v. Murphy* 317 Ill. App. 3d 1054, 740 N.E.2d 1166 (1st Dist, 2000)
[5] *Zdeb v. Baxter International, Inc.* 697 N.E.2d 425 (1st Dist. 1998)
[6] *Cardinal Health 414, Inc. v.. Adams*, 582 F.Supp.2d 967 (M.D. Tenn. 2008) ("… profit and loss statements, customer pricing information, and other private and confidential information of a sensitive nature …" and "…spreadsheet listing of every one of Cardinal's Nashville customers and the date that customer's contract expired or was set to be automatically renewed … ."); *Hauck Mfg. v. Astec Indus*., 376 F.Supp.2d 808 (E.D. Tenn. 2005) ("one of its primary witnesses, John A. Marino (Plaintiff's senior vice president for technology and business development), did generally testify as to the confidential and proprietary nature of a host of different types of information, including information about Plaintiff's research and development process (Tr. at 145), manufacturing drawings (Tr. at 159-60), general know-how as to service and emissions testing (Tr. at 167-68), Plaintiff's discount schedule (Tr. at 169-70), production costs (Tr. at 171), labor requirements for burner production (Tr. at 217-18, 273), a computer program used in servicing burners (Tr. at 235-36), material costs (Tr. at 273), and internal part numbers (Tr. at 204-09, 547).") ; *National Reprographics, Inc. v. Strom*, 621 F.Supp.2d 204 (D.N.J., 2009) (1. Strategic Business Planning; 2. Customer Identity, Relationship details; Sales, Analysis; 3. Pricing; 4. Profit Reports; 6. Operations Manual; 7. Equipment; 8. Production Procedures, Practices, Management and Allocation of Resources; 9 Recruitment; 10. Training)
[7] *AMP Inc. v. Fleischhacker* 823 F.2d 1199, 3 USPQ2d 1421, 1424 (7th Cir 1987)
[8] *Vital State Canada, Ltd. v. Dreampak, LLC*, 303 F.Supp. 2d 516, 525 (D.N.J. 2003)
[9] *Ruckelshaus v. Monsanto Co*., 467 U.S. 986, 1002 (1984); *CVD, Inc. v. Raytheon Co*., 769 F.2d 842, 850, 227 USPQ 7 (1st Cir. 1985); *ECT Int'l, Inc. v. Zwerlein*, 597 N.W.2d 479, 482 (Wis. App. 1999) *BondPro Corp. v. Siemens Power Generation Inc*., 463 F3d 702, 80 USPQ2d 1207 (7th Cir. 2006)
[10] *IDX Sys. Corp. v. Epic Sys. Corp*., 285 F.3d 581, 62 U.S.P.Q.2d 1278 (7th Cir. 2002)
[11] *Composite Marine Propellers, Inc. v. Van Der Woude*, 962 F.2d 1263, 1266, 22 USPQ2d 1568 (7th Cir. 1992).
[12] *Storage Technology Corp. v. Custom Hardware Engineering & Consulting Inc*., 421 F3d 1307, 76 USPQ2d 1065 (Fed. Cir. 2005), see also *Thomas & Betts Corp. v. Panduit Corp*., 108 F.Supp.2d 968, 55 USPQ2d 1698, (N.D. Ill. 2000)) (trade dress) *Celeritas Techs. v. Rockwell Int'l Corp*. 150 F.3d 1354; 47 U.S.P.Q.2d 1516 (Fed Cir 1998), *Caterpillar Inc. v. Sturman Industries Inc*., 387 F.3d 1358, 73 USPQ2d 1609 (Fed. Cir. 2004) (patent).
[13] *Delta Medical Systems v. Mid-America Medical* 331 Ill. App. 3d 777 (1st Dist 2002) (breach of loyalty and tortious interference involved misappropriation of trade secrets, therefore preempted 765 Ill. Comp. Stat. 1065-2 et seq.) See also Unikel, "Bridging the 'Trade Secret' Gap: Protecting 'Confidential Information' Not Rising to the Level of Trade Secrets," 29 Loy. U. Chi. L.J. 841, 887-88 (1998)
[14] *Duncan v. Stuetzle* 76 F.3d 1480, 37 U.S.P.Q.2d 1758 (9th Cir 1996) (trademark) *Celeritas Techs. v. Rockwell Int'l Corp*. 150 F.3d 1354; 47 U.S.P.Q.2d 1516 (Fed Cir 1998) (patent and breach of contract for non-disclosure).
[15] *Formax, Inc. v. Hostert* 841 F.2d 388, 5 U.S.P.Q.2d 1939 (Fed Cir 1988) (misappropriation of trade secrets can rise to RICO acts)
[16] *Carpenter v. United States*, 108 S.Ct. 316, 98 L.Ed.2d 275 (1987)
[17] *ABBA Rubber Co. v. Seaquist*, 235 Cal.App.3d 1 (1991) (holding that a trade secret is protectable if it has not yet been ascertained by others)
[18] *DVD Copy Control Assn., Inc. v. Bunner*, 116 Cal. App. 4th 241, 69 U.S.P.Q.2d 1907 (Cal. App. 6th Dist. 2004)
[19] *Morlife, Inc. v. Perry*, 56 Cal. App. 4th 1514, 45 U.S.P.Q.2d 1741 (Cal. Ct. App. 1997)
[20] *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1268, 35 U.S.P.Q.2d 1010 (7th Cir, 1995)
[21] *Eichmann v. National Hospital* 308 Ill. App. 3d 337; 719 N.E.2d 1141 (1st Dist 1999)
[22] *Disher v. Fulgoni*, 124 Ill. App. 3d 257, 464 N.E.2d 639, 643 (1984), aff'd after remand, 161 Ill. App. 3d 1, 514 N.E.2d 767 (1987). But see *Hanchett Paper Co. v. Melchiorre* 341 Ill. App. 3d 345, 792 N.E.2d 395 (2d Dist. 2003)
[23] *Estee Lauder Companies, Inc. v. Batra*, 430 F. Supp. 2d 158, (S.D.N.Y., 2006)
[24] *Strata Marketing, Inc. v. Murphy*, 740 N.E.2d 1166 (1st Dist 2000)
[25] *C.H. Robinson Worldwide, Inc. v. Command Transp*., LLC, 2005 U.S. Dist. LEXIS 28063 (N.D. Ill. Nov. 16, 2005)
[26] *Delta Medical Systems v. Mid-America Medical* 331 Ill. App. 3d 777 (1st Dist 2002)
[27] *Combined Metals of Chicago Ltd. Partnership v. Airtek, Inc.*, 985 F. Supp. 827 (N.D. Ill. 1997), *Thermodyne Food Serv. Prods., Inc. v. McDonald's Corp*., 940 F. Supp. 1300 (N.D. Ill. 1996)
[28] *Tax Track Sys. Corp. v. New Investor World, Inc.*, F. Supp. 2d , 2005 U.S. Dist. LEXIS 7241 (N.D. Ill. Mar. 24, 2005)
[29] *Fox Controls, Inc. v. Honeywell, Inc*., 2004 U.S. Dist. LEXIS 7231 (N.D. Ill. 2004)
[30] *Delta Medical Systems v. Mid-America Medical* 331 Ill. App. 3d 777 (1st Dist 2002)
[31] *AutoMed Techs., Inc. v. Eller*, 160 F. Supp. 2d 915, 2001 U.S. Dist. LEXIS 9728 (N.D. Ill. 2001), *Caterpillar Inc. v. Sturman Indus*., F. Supp. 2d , 2001 U.S. Dist. LEXIS 25891 (C.D. Ill. Dec. 10, 2001)
[32] *Bagley v. Lumbermens Mut. Cas. Co*., 100 F. Supp. 2d 879, 2000 U.S. Dist. LEXIS 8353 (N.D. Ill. 2000)
[33] *Fox Controls, Inc. v. Honeywell, Inc*., 2004 U.S. Dist. LEXIS 7231 (N.D. Ill. 2004), *Web Communications Group, Inc. v. Gateway 2000, Inc*., 889 F. Supp. 316 (N.D. Ill. 1995)

[34] *BAB Sys. v. Pilatus Inv. Group Inc.* 2005 U.S. Dist. LEXIS 25737 (N.D. Ill. Oct. 27, 2005)
[35] *Thomas & Betts Corp. v. Panduit Corp.*, 108 F.Supp.2d 968, 55 USPQ2d 1698, (N.D. Ill. 2000)
[36] *Storage Technology Corp. v. Custom Hardware Engineering & Consulting Inc.*, 421 F3d 1307, 76 USPQ2d 1065 (Fed. Cir. 2005), *Do It Best Corp. v. Passport Software, Inc.*, 2004 U.S. Dist. LEXIS 14174 (N.D. Ill. July 23, 2004)
37 *Russo v. Ballard Medical Products*, 550 F.3d 1004 (10th Cir., 2008) ("the fact that patents may be used as evidence in aid of a trade secret claim is not the same thing as raising a substantial (or really, any) question of federal patent law,") citing Uroplasty Inc. v. Advanced Uroscience Inc., 239 F.3d 1277, 1280, 15 USPQ2d 1726 (Fed. Cir. 2001).
[38] *Chemetall GMBH v. ZR Energy, Inc.*, 62 USPQ2d 1202 (N.D. Ill. 2000), aff'd 320 F.3d 714 (7th Cir, 2003) (state law contract, tortious interference, Unfair and Deceptive Trade Practices claim not preempted, *but see Seaga Mfg. v. Fortune Metal, Inc.,* 2001 U.S. Dist. LEXIS 16341 (N.D. Ill. Oct. 10, 2001))
[39] See 820 ILCS 115/2, 3, 5 (West 2002).
[40] *Maher & Associates v. Quality Cabinets* 267 Ill. App. 3d 69, 640 NE2d 1000 (1994)
[41] see e.g. *Vermont Microsystems Inc. v. Autodesk Inc.*, 39 USPQ2d 1421 (2d Cir. 1996) for misappropriation of trade secrets involving development of CAD program itself
[42] *Rockwell Graphic Systems Inc. v. DEV Industries Inc.*, 17 USPQ2d 1780 (7th Cir. 1991)
[43] See e.g. *qad inc. v. ALN Assoc.* 770 F. Supp. 1261, 19 USPQ2d 1907 (N.D. Ill., 1991) (preliminary injunction later vacated because copyright procured without disclosing derivative nature of work)
[44] 37 C.F.R. § 202.21
[45] *Chicago Board of Education v. Substance Inc.*, 354 F3d 624, 69 USPQ2d 1447 (7th Cir. 2003)
[46] 37 C.F.R. 202.20 (c) (iv)
[47] 37 C.F.R. 202.20 (d)
[48] in January, 2009, $35 for electronic filing and $45 for a paper filing,
[49] in January, 2009, $685
[50] *Hanchett Paper Co. v. Melchiorre* 341 Ill. App. 3d 345, 792 N.E.2d 395 (2d Dist. 2003)
[51] *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 517-519, 26 USPQ2d 1458 (9th Cir. 1993)
[52] *Feist Publ. Inc. v. Rural Tel. Serv. Inc.* 499 US 340, 111 S Ct 1282, 18 USPQ 2d 1275 (1991)
[53] Seven requirements need to be met, see Circular 65 on Group Registration for Automated Database. Updates/Revisions
Group registration is possible only if all the following conditions are met:
1. all updates or revisions need to be fixed in machine readable form;
2. a three month period in the same calendar year is covered;
3. the same owner owns all the updates or revisions
4. all the updates share the same title
5. the updates are similar in content
6. the updates are similar in organization, and
7. if published before March 1, 1989, there is an appropriate copyright notice.
[54] 18 U.S.C. § 1030
[55] *Yonkers v. Celebrations The Party and Seasonal Superstore* 428 F.3d 504 (3d Cir. 2006), a "hacking" case, affirmed denial of an injunction, but also recognized decisions the Computer act provided a civil remedy, citing *Theofel v. Farey-Jones*, 359 F.3d 1066, 1078 (9th Cir. 2003) ("The civil remedy extends to `[a]ny person who suffers damage or loss by reason of a violation of this section.'") and *I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, 307 F.Supp.2d 521, 526 (S.D.N.Y. 2004) (stating that § 1030(g) affords civil action for any violation of CFAA). The *Yonkers* court stated: "Accordingly, we conclude that civil relief is available under § 1030(g)"; Cases may diverge in application — to corporate hackers *Int'l Ass'n of Machinists & Aero Workers v. Werner-Matsuda*, 390 F.Supp.2d 479, 495 (D.Md. 2005) or to employee misconduct exceeding authority *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006); see also *Lasco Foods, Inc. v. Hall and Shaw Sales, Marketing, & Consulting, LLC* 600 F.Supp.2d 1045 (E.D. Mo., 2009) and *Cardinal, supra*, interpreting Stored Wire and Electronic Communications Act ("SECA"), 18 U.S.C. § 2701, et seq.
[56] Illinois' Computer Crime Prevention Law ("CPPL"), 720 ILCS 5/16D-1 *et seq.*, *Sotelo v. Directrevenue, LLC*, 384 F.Supp.2d 1219 (N.D. Ill., 2005) (class action for Spyware)