SUFFOLK UNIVERSITY LAW SCHOOL
JOURNAL OF HIGH TECHNOLOGY LAW

VOL. II 2003 NO. 1

Cite as: 2 J. HIGH TECH. L. 1 (2003)

Federal Issues in Trade Secret Law[†]

Jerry Cohen, Esq.*

I. INTRODUCTION

The general picture of trade secret law is that it is governed by state law as summarized in Restatement of Torts[1] and Restatement of Unfair Competition (Third)[2] and codified in more or less uniform state enactments based on the Uniform Trade Secrets Act.[3] The American Bar Association's Section of Intellectual Property soundly rejected a proposal for a preemptive federal trade secrets statute at its 1992 meeting in San Francisco.[4] Yet, long prior to the 1992 meeting, and at an accelerating pace thereafter, there have been several areas of federal relevance established in the law and practice of trade secret

* The author acknowledges the valuable assistance of William M. Simmons, Esq., Of-Counsel to Perkins, Smith & Cohen, LLP, Boston, Massachusetts, in preparation of this paper. This paper was presented at Suffolk University Law School Center For Advanced Legal Studies, Trade Secrets Seminar, Friday, March 14, 2003 (Co-Sponsored with Boston Patent Law Association). Jerry Cohen, Esq., Perkins, Smith & Cohen, LLP, Boston, Massachusetts, jcohen@pscboston.com.

1. RESTATEMENT (FIRST) OF TORTS § 757 cm. b (1982). Restatement drafters defined trade secrets, in part, as "consisting of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it." *Id.* Among the illustrative list of uses includes a "formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers." *Id.*

2. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995) (defining a trade secret as "any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford as actual or potential economic advantage over others").

3. 18 U.S.C. § 1905 (2000).

4. *Annual Report*, 1992-93 A.B.A. SEC. IPL 300-09 (rejecting resolution 410 previously introduced, debated and defeated).

 ISSN 1536-7983

protection.[5] One must also consider federal issues presented by the Fourth, Fifth, Eleventh and Fourteenth Amendments, federal court jurisdiction to enforce state trade secret law, federal tax law and bankruptcy laws.[6]

II. THE (FEDERAL EMPLOYEE) TRADE SECRETS ACT (TSA)

Early on, Congress recognized a need to codify the protection that federal agencies had given to data collected from private parties on an ad hoc basis. Various trade secret codifications in such sections as 15 U.S.C. § 1776, 18 U.S.C. § 112, 19 U.S.C. § 1335 and in various portions of the Revised Statutes (RS) were, in June, 1948, consolidated into the Trade Secrets Act (TSA).[7] After several subsequent amendments, the act now appears at 18 U.S.C. §§ 1905, 1906, 1907 and 1909. TSA provides criminal penalties for a federal civil servant revealing trade secrets of private parties.[8] In turn, the civil servant can invoke the statute as a basis of privilege when asked to reveal the information in a judicial proceeding until the court overrules the privilege.[9]

TSA provides a safe harbor exception to the ban on revealing trade secrets or the like. Parties may reveal such information to the extent " . . . authorized by

---

5. Including, at least, the following (Federal Employees) Trade Secrets Act, 18 U.S.C. § 645 (2000); Government Procurement Regulations, Industrial Security Manual, Grants, Subcontracts; Federal Freedom of Information Act (FOIA), 5 U.S.C. § 552(h) (2000); Trade Secret Exceptions to Sunshine Government and Federal Agencies' Responsibilities and Options re Trade Secrets; Privacy vs. Police Power: Computer and Network Regulations Affecting Protection of Trade Secrets and Intellectual Property and Autonomy Interests - Wiretap Act, 18 U.S.C. § 2511 (2000); Electronic Communications Privacy Act, 18 U.S.C. § 2701 et seq. (2000); Computer Fraud and Abuse Act, Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified in 18 U.S.C. § 1030); Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994), (codified in 47 U.S.C. § 1001 et seq. (2000); Foreign Intelligence Surveillance Act, 50 U.S.C. § 1802 (2000); Bank, Health, Postal Privacy Act, 5 U.S.C. § 552(a) (2000); USA PATRIOT Act, Pub. L. No. 107-56 (2001); Homeland Security Act, Pub. L. No. 107-296 (2002); Interstate Transport of Stolen Property Act, 18 U.S.C. § 2314 (2000); Economic Espionage Act, 18 U.S.C. § 1831 (2000); Goods and Data Export Controls; Transaction Controls; Invention Secrecy Act, 35 U.S.C. § 181 (2000). Other federal involvement with Trade Secret law including Bankruptcy Law, Tax Law, Antitrust Law, Encryption and E-Commerce Standards, Digital Millennium Copyright Act, Pub. L. No. 105-304 (1998).

6. *See, e.g.*, 28 U.S.C. § 1338(b) (2000) (recognizing federal issues including diversity, unfair competition claims adjunct to patent and copyright cases and federal claims).

7. Trade Secrets Act, 1948, ch. 645, § 1, 62 Stat. 791 (1948) (current version at 18 U.S.C. § 1905 (2000)). The Trade Secrets Act, recodified in 1948 in 18 U.S.C. § 1905, stems from customs duties provisions in R.S. § 3167 (1894) and 19 U.S.C. § 1335 (1943 ed.). Trade secrets referred to an unpatented secret, commercially valuable plan, appliance, formula or process used in connection with preparation for sale of trade commodities. Section 1905 - Disclosure of confidential information generally - is a criminal statute that prohibits by any officer or employee of the United States or any defendant or agency thereof to disclose or make known "in any manner or to any extent not authorized by law any information coming to him in the course of his employment on official duties." 18 U.S.C. § 1905 (2000). The court may fine violators not more than $1000 or imprison violators for not more than one year, or both, and remove them from office or employment. *Id*. In 1980, Congress amended Section 1905 to apply specifically to "agents" of the DOJ retained in connection with enforcement of antitrust laws. 15 U.S.C. § 1311(j) (2000). In 1992, Congress again amended section 1905 to include "any person acting on behalf of the Office of Federal Housing Enterprise Oversight." 18 U.S.C. § 1905.

8. 18 U.S.C. § 1905 (2000). The offender may face a fine or imprisonment not to exceed one year. *Id.*

9. *Id.*

law . . . ."[10] As to banking information, the safe harbor extends to instances of express permission in writing from the Comptroller of the Currency, Board of Governors of the Federal Reserve System, or certain other organizations under the Federal Reserve Act or the Federal Deposit Insurance Corp.[11] The term "trade secret" provides a built-in screening limitation and a common sense threshold of significance. The "authorized by law" exception includes federal agency regulations promulgated within the scope of rule-making authority granted to the agency by Congress.[12]

TSA does not per se provide a private right of civil action to enjoin disclosure, though TSA in tandem with the Administrative Procedure Act (APA) works to that end in principle.[13] Much of TSA application has been subsumed in practice into trade secret and business privacy exemptions of the Freedom of Information Act (FOIA),[14] procurement laws and regulations, and specific governing statutes and regulations for regulatory agencies described below. TSA, however, retains a vital modern role in holding federal employees and agencies responsible for treatment of information.[15]

III. GOVERNMENT PROCUREMENT CONTRACTING AND SUBCONTRACTING; INDUSTRIAL SECURITY MANUAL; SUBCONTRACTORS

The Federal Acquisition Regulation (FAR), along with some supplementation by particular agencies, notably the Department of Defense (DOD) Supplement to FAR (DFAR), govern the U.S. government's procurement of goods and services.[16] FAR exemplifies a structure of

---

10. 18 U.S.C. § 1905 (2000).

11. 18 U.S.C. § 1906 (2000); *see also* Chrysler Corp. v. Brown, 441 U.S. 281 (1979). The phrase "authorized by law" in Trade Secrets Act, 18 U.S.C. § 1905, imposes criminal sanctions on government employees who disclose in any manner "not authorized by law" certain classes of information submitted to a federal agency. *Id*. Hence, the phrase contained within the statute, includes trade secrets and confidential statistical data, but does not have a particular limited meaning. *Id*.; 18 U.S.C. § 1906 (2000).

12. *See* Chrysler Corp. v. Brown, 441 U.S. 288 (1979) (holding no private right of action). The trade secret owner can proceed in an APA to block disclosure citing TSA as a basis to characterize the contemplated disclosure action as not in accord with law and/or arbitrary or capricious. 5 U.S.C. § 702 (2000).

13. Chrysler Corp., 441 U.S. at 316; Chevron Chem. Co. v. Costle, 641 F.2d 104, 115 (3d Cir. 1981) (holding that although § 1905 does not grant a provide cause of action, it may provide a standard of review for proposed agency disclosures), *cert. denied*, 452 U.S. 961 (1982). *But see* Conax Florida Corp. v. U.S., 625 F. Supp. 1324, 1326 (D.D.C. 1985) (holding plaintiff's allegations sufficient to confer jurisdiction under the Trade Secrets Act through the Administrative Procedure Act), *reh'g granted*, 641 F. Supp. 408, *aff'd*, 824 F.2d 1124 (D.C. Cir. 1986).

14. 5 U.S.C. § 552(h) (2000).

15. *See, e.g.*, Parker v. BLM, 141 F. Supp. 2d 71, 81 n. 14 (D.D.C. 2001) (finding TSA prohibited disclosure of documents falling within Exemption 4); Mallinckrodt, Inc. v. West, 140 F. Supp. 2d 1, 5 (D.D.C. 2000) (concluding Exemption 4 of the POIA shielded rebates and incentives from disclosure).

16. The U.S. government is the world's largest customer of goods and services. *See generally* Federal Acquisition Regulation, Dep't of Defense Supp., 48 C.F.R. pts. 1-53 (2002). As a joint project of General Service Administration, DOD and NASA, replacing the Federal Procurement regulation system (41 C.F.R. Subtitle A) and Defense Acquisition Regulation (32 C.F.R. ch. 11). *See* 48 C.F.R. §§ 52.227-14-227-15, 252.227-7013-.227-7014, 227.403-70 (2002) (establishing procedures to identify rights in technical data); *see*

government acquisition of technical data or computer software with "limited" or "unlimited" rights.[17] The term "limited rights" refers to use for defined government purposes but excludes use for competitive procurement.[18] Along with the negotiations between a contractor and the government regarding limited versus unlimited rights pertaining to data, comes the issue of how much data to give in the first instance.[19]

Often, a redacted data delivery can satisfy government purposes. Modern standards of quality control and zero-defect goals, as well as growing capacity for data storage and management, militate increasingly against acceptability of redacted data deliveries. This does not mean that the good days for contractors are nearing an end. The contractor and government lawyers, however, must work harder for compatibility of disclosure needs versus secrecy needs.[20]

A. Procurement Contracts and Proposals

Generally, a request for proposals and the resultant contract spells out the ground rules for data and software acquisition with limited or unlimited rights to data, which is consistent with the general standard of development or not at private expense.[21] In some cases, however, development history is ambiguous. In those occasions, a contracting officer will decide the issue, subject to review by an agency board of appeals and, in turn, by federal courts. In the instances of an equity claim, that process may be bypassed under TSA and APA as mentioned above. In either case, the decision-maker will apply a highly deferential standard of review.[22] In other cases, the procurement overrides the usual standard and stipulates unlimited rights notwithstanding development at private expense. There, a company presumably has fair warning and can decline to submit a proposal or go ahead and propose with its price reflecting its valuation of the surrendered rights.[23]

---

also generally, M.S. Gimchak et al, *A Few Words of Advice: Protecting Intellectual Property When Contracting With the Department of Defense*, 23 PUB. CONT. L. J. 141 (Winter 1994).

17. 48 C.F.R. § 252.227-7013 (2002).

18. *See id*.; *see also* M.S. Gimchak et al, *A Few Words of Advice: Protecting Intellectual Property When Contracting With the Department of Defense*, 23 PUB. CONT. L. J. 141 (Winter 1994).

19. *See, e.g.*, JAMES POOLEY, TRADE SECRETS § 14.02[1] (2002).

20. *Id*. at § 14.02[2] (suggesting to maintain confidentiality by making liberal use of legends and conspicuous stamps). Such proactivity will help to prevent possible FOIA and inadvertent disclosure. *Id*.

21. *See generally* JOHN COSGROVE MCBRIDE & THOMAS J. TOUHEY, 1B-9 GOVERNMENT CONTRACTS: LAW, ADMIN & PROC. § 9.30 (2001).

22. *See, e.g.*, Bell Helicopter Services, ASBCA No. 29112, 85, .3BCA ¶ 18,415 (1985). Contract Disputes Act, 41 U.S.C. §§ 601-613 (2000) (190 as amended by the Tucker Act, 28 U.S.C. §§ 1346(a)(2), 1491 (2000)) (providing U.S. Claims Court jurisdiction for contract disputes). The milestone case for distinguishing contract claims from agency action is Megapulse, Inc. v. Lewis, 672 F.2d 959 (D.C. Cir. 1982) (involving a government contractor's effort to enjoin release of the contractor's trade secret by the purchasing agency). The Court held that the case was one triable under TSA and APA and not a contract case limited to trial in the Court of Claims. *Id*.

23. *See* 48 C.F.R. §§ 252.227-7013(a)(12) (2002) (defining "developed at private expense" as dealing with such subtleties as private development costs indirectly (rather than directly) reimbursed by the government

Occasionally, a potential contractor submits an unsolicited proposal and disputes develop over whether an implied contract to respect confidentiality of data disclosed in the proposal binds the government.[24] Proper marking of information can be critical to gaining protected status or holding on to it.[25] A typical legend reads:

Limited Rights Legend

Contract No. _____
Contractor: _____

> Limited rights shall be effective until _____, thereafter the limited rights will expire and the Government shall thereafter have unlimited rights to the data. The restrictions govern use of the data as set forth in the definitions "limited rights" in par. (a)(15) at 252.227-7013 of the contract listed above.

In the 2002 case, *Xerxe Group, Inc. v. United States*,[26] the U.S. Court of Appeals for the Federal Circuit affirmed a decision of the U.S. Claims Court rejecting compensation or injunctive relief to a contractor who failed to mark its unsolicited proposal as required in applicable FAR practices.[27] The Plaintiff had marked the cover page of its proposal but failed to so mark each page containing the data.[28] The regulation marking for an unsolicited proposal reads:

Use and Disclosure of Data [Title Page Legend]

> The proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed-in whole or in part-for any purpose other than to evaluate this proposal.[29] If the Government awards a contract to this offeror as a result of – or in connection with – the submission of these data, however, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in these data if they obtain such from another source without restriction. The data subject to this restriction are contained in Sheets [insert numbers or other identification of sheets].
>
> [(b) The offeror shall also mark each sheet of data it wishes to restrict with the

---

as part of overhead pools of "independent research and development" and "bid" and "proposal" costs). These are still deemed private expense developments. *Id*.

24. POOLEY, *supra* note 19, at § 14.02[1] (suggesting that including the phrase "for government internal evaluation only" would effectively create an implied-in-fact contract which would confidentially bind the government).

25. *See, e.g.*, Secure Serv.'s Technologies Inc. v. Time & Space Processing, Inc., 722 F. Supp. 1354, 1360 (E.D. Va. 1989) (holding failure to mark data or on legend forfeits protected status).

26. 278 F.3d. 1357 (Fed. Cir. 2002).

27. *Id*. at 1359; *see also* 48 C.F.R. §§ 15.608(b), 15.609(a), (b) (2002).

28. *Xerxe Group*, 278 F.3d at 1360.

29. *See generally* JERRY COHEN & ALAN S. GUTTERMAN, TRADE SECRETS PROTECTION AND EXPLOITATION 140-142 (1998).

following legend:]

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

B. Bid Protests

The government's policy is to enter the commercial marketplace and conform to legal and moral standards of that marketplace. Accordingly, it is a misuse of government funds to deal on any other basis. The Comptroller General (CG) branch of the General Accounting Office (GAO) has a well recognized jurisdiction,[30] considers bid protests and instructs procuring agencies to terminate invitations for bids, requests for proposals, and even contract work in progress based on misappropriation of a rival company's trade secrets.[31] Nevertheless, CG discretion sometimes inclines to favor price competition rather than intellectual property (IP).

One must also compare the interaction among trade secrets, patents and copyrights.[32] The government can give authorization and consent to contractors and subcontractors to infringe a patent or copyright.[33] The IP owner can not seek an injunctive remedy, however, but rather may assert the right to make a compensation claim to the agency involved in the transaction.[34] If that right is

---

30. Competition in Contracting Act of 1984 (codified as 31 U.S.C. §§ 3551- 3556 (2000)).

31. *See* 4 C.F.R. pt. 21 (2002) (setting out bid protest rules). *See generally* GOVERNMENT CONTRACT LAW, THE DESKBOOK FOR PROCUREMENT PROFESSIONALS 146-160 (2d ed. 1999) (discussing GAO bid protests in depth).

32. *See generally* COHEN & GUTTERMAN, *supra* note 29, at 27.

33. 48 C.F.R. § 52.227-1 (2002).

> (a) The Government authorizes and consents to all use and manufacture, in performing this contract or any subcontract at any tier, of any invention described in and covered by a United States patent (1) embodied in the structure or composition of any article the delivery of which is accepted by the Government under this contract or (2) used in machinery, tools, or methods whose use necessarily results from compliance by the Contractor or a subcontractor with (i) specifications or written provisions forming a part of this contract or (ii) specific written instructions given by the Contracting Officer directing the manner of performance. The entire liability to the Government for infringement of a patent of the United States shall be determined solely by the provisions of the indemnity clause, if any, included in this contract or any subcontract hereunder (including any lower-tier subcontract), and the Government assumes liability for all other infringement to the extent of the authorization and consent hereinabove granted. (b) The Contractor agrees to include, and require inclusion of, this clause, suitably modified to identify the parties, in all subcontracts at any tier for supplies or services (including construction, architect-engineer services, and materials, supplies, models, samples, and design or testing services expected to exceed the simplified acquisition threshold (however, omission of this clause from any subcontract, including those at or below the simplified acquisition threshold, does not affect this authorization and consent.)

Id.

34. *See* 28 U.S.C. § 1498 (2000); 48 C.F.R. § 27.201-1(a) (2002). The rule prohibits the patent owner from bringing suit against the government contractor or subcontractor. *Id.* The contractor or subcontractor, however, may be liable to the Government for any damages paid by the Government to the patent owner. *Id.* The Act insulates government contractors and subcontractors from patent infringement suits and injunctive proceedings in the district courts. *See id.*

unavailing, the IP owner may sue in the U.S. Claims Court for compensation.[35]

The Tucker Act[36] resolves trade secret 'takings' for issues grounded in contract.[37] The Federal Tort Claims Act[38] resolves trade secret torts.[39] Lastly, in equitable situations outside the scope of the foregoing, an APA claim resolves the trade secret dispute when an allegation of TSA violation involves a government officer.[40]

C. Industrial Security Manual, Military Secrets, State Secrets

An essential element of a defense effort is secrecy – protection of information about strengths, weaknesses, state of readiness and deployment of our military resources and our knowledge of similar factors for present or potential adversaries.[41] The U.S. military trains its uniformed defense force personnel well in such considerations and disciplines them to create and implement systems for facilities and information security. The military also disciplines its personnel in disclosure issues on a need to know basis using encryption and other tools of protection.[42] The great dependence of the military on the private sector (and vice-versa, the famed "military-industrial complex") presents challenges of maintaining the discipline through layers of thousands of contracting and subcontracting companies, and millions of their employees, consultants, shareholders, creditors, bankers, insurers, spreading further to family members and friends.[43] Acting pursuant to the War Powers Act[44] and Executive Orders, DOD considerations of moving military security to the contracting community coalesce in DOD's Industrial Security Manual (ISM).[45]

---

35. 28 U.S.C. § 1498. The availability of this remedy (and indemnification of the government by contractors), prompted the Comptroller General to instruct agencies that they must accept low bids without regard to allegations of patent infringement by a competing bidder. Herbert Cooper Co., 38 Comp. Gen. 276, 277 (1958); *see also* Richmond Screw Anchor Co. v. United States, 275 U.S. 331 (1928) (stating that acceptance of the allegedly infringing articles by the Government is sufficient to make the United States amenable to suit by the patent owner in the Court of Federal Claims).

36. 28 U.S.C. § 1941 (2000).

37. 3 MILGRIM ON TRADE SECRETS § 12.05[2] (2002) (stating that because proceedings under the Tucker Act must be brought in Claims Court, the Court could only award damages as oppose to equitable remedies).

38. 28 U.S.C. §§ 1291, 1346, 1402, 2401, 2402, 2411, 2412, 2671- 2680 (2000).

39. International Eng'g Co. v. Richardson, 512 F.2d 573, 578-579 (D.C. Cir. 1975) (holding that the government's use of the secret beyond the contractual right constituted a breach of contract rather than a tort).

40. 5 U.S.C. §§ 553-559, 701-706 (2000).

41. *See generally* Gary Langer, *ABCNEWS Poll: War and the Media Americans Favor Military Secrecy Over Press Freedom During Wartime*, ABCNews.com, January 16, 2003, *at* http://abcnews.go.com/sections/nightline/DailyNews/war_media_poll_030117.html (finding that in wartime, seventy-five percent of Americans agree that military secrets trump freedom of the press).

42. *See* Patrick J. Geary, *The Perils of Paperless: Some Questions About the Latest Defense Business Trend*, *at* http://www.nwc.navy.mil/press/Review/2001/Summer/sd2-su1.htm (last visited April 30, 2003).

43. *See generally* Military Industrial Complex, Center for Defense Information, *available at* http://www.cdi.org/issues/usmi/complex/mic.html (last visited May 1, 2003).

44. Pub. L. No. 93-148, 87 Stat. 555 (1973).

45. National Industrial Security Program Operating Manual (NISPOM), January 1995, *available at* http://www.dss.mil/isec/nispom_0195htm (last visited April 28, 2003).

As the core of a system of cleared facilities, the ISM requires DOD to clear personnel at progressive levels of sensitivity, establish procedures for document generation and control including multi-levels, encryption, training, maintenance right and audit.[46] The ISM-based system becomes a competitive advantage for contractors of high level clearance versus those offering lesser or no clearance.[47] An overload crisis of recent years (even before 9/11/01) has slowed the rate of new facilities and personnel clearances and the situation has worsened rather than improved since 9/11.

The ISM-based procedures present an ideal world of the protective measures and economic advantages based on secrecy as contemplated by the Restatement of Torts[48] and the Uniform Trade Secrets Act[49] as the essence of a protectable trade secret.[50] Competitive intelligence efforts to access and use trade secrets developed by a contractor for the government (or acquired by the contractor from the government) can amount to treason in such an environment and in any event prove difficult and dangerous.[51] In some instances, competitors can have the same level of access and their competition, mediated by the purchasing agency, can give way, for better or worse, to cooperation in the interest of national defense.

In war or pseudo-war, laws of civil liberties fall silent.[52] War times may also subdue antitrust laws and diminish the ability of citizens and the press to scrutinize actions of public officials.[53] The need for perpetual balancing and rebalancing of defense concerns and other national values is apparent and through the years, in Republican and Democrat administrations alike, the federal government has tried to do just that.

The war against terrorism will produce grotesque mimicry of the relatively disciplined infrastructure of military security designed for wars and potential wars with other nations' armed forces. Federal grants and other assistance to state and local police, fire and emergency preparedness agencies present grantees with diluted models of the ISM system and some reliance on existing state and local personnel screening and information management systems.

Companies must build skills to protect their own trade secrets and at the

---

46. *Id*.

47. *See id*.

48. *See supra* note 1 and accompanying text.

49. 18 U.S.C. § 1905 (2000).

50. *See* NISPOM, *supra* note 45.

51. *See* 18 U.S.C. § 2381 (2000). The Federal Sentencing Guidelines Manual states, "[t]reason is a rarely prosecuted offense that could encompass a relatively broad range of conduct, including many of the more specific offenses in this Part," to which the manual lists trade secrets among others. Federal Sentencing Guidelines Manual, Treason § 2M1.1, *at* http://www.ussc.gov/2000guid/CHAP2-4.htm.

52. *See generally* Associated Press, *High Court Prepares for Anti-Terrorism Cases; Justice Breyer Foresees Difficulty Balancing Public Protection, Civil Liberties*, WASHINGTON POST, April 05, 2003, at A06.

53. *See, e.g.*, Brit Hume, Mort Kondracke, Fred Barnes, Mara Liasson, *All-Star Panel Discuss Reactions to Bush's Speech and Reactions to Senator Daschle's Comments*, FOX NEWS – FOX SPECIAL REPORT WITH BRIT HUME, Transcript # 031805cb.254, March 18, 2003.

same time work to comply with the rigorous security demands of their growing federal, state and local government customer prospects.[54] Sometimes these multiple requirements will be complementary or even coincident, and in other times, in conflict. The company's lawyers can train themselves to be valuable guides.

D. Litigation Between Competing Contractors and Transforming Disputes Between Contractors and Sub-Contractors into Claims vs. Government

When a trade secret owner competes in bidding for government business with company B that misappropriates A's trade secrets, does company A have a remedy? In short, the answer is yes. Under the trade secret law,[55] company A has a remedy even if the government purchaser participated in the misappropriation. In *Curtiss-Wright Corp. v. Edel-Brown Tool & Die Co.*,[56] a Massachusetts case, the Navy used drawings submitted by Curtiss-Wright (C-W) to attract competitive bids.[57] The SJC affirmed the Superior Court's decision allowing an injunction in favor of C-W against competing bidder Edel-Brown (EB).[58] The Navy might have tried to acquire C-W's trade secret right by negotiation or even some form of taking, in either case with due compensation.[59] In this case, however, the government did not take any action.

There is an elaborate flow-down system of contract clauses of the government-prime contractor contract to subcontractors mandated by regulations.[60] At the same time, the government studiously denies aid with the subcontractor. The practice has developed for subcontractors aggrieved by government action in connection with a project to have the prime contractor bring a subcontract appeal to the contracting officer and the agency board of appeals on behalf of the subcontractor.[61] An overly aggressive reach for a subcontractor's trade secrets would complicate this process because the prime contractor would likely be partially at fault and/or might have an indemnity obligation to the government agency.

E. Federal Grants

Apart from purchase of goods and services from the private sector (including purchasing of R&D services), government agencies make substantial grants to

---

54. As well as goods and data export control laws and other cooperation with law enforcement needs as noted later in this article.

55. The suit would be in a state court or a federal court as surrogate state court under diversity jurisdiction, if available.

56. 407 N.E. 2d 319 (Mass. 1980).

57. *Id*. at 323.

58. *Id*. at 327.

59. *See id*. at 319.

60. *See* MARGARET M. WORTHINGTON & LOUIS P. GOLDSMAN, CONTRACTING WITH THE FEDERAL GOVERNMENT 57 (4th ed. 1998).

61. At a price of the sub waiving any relief against the prime contractor per se.

universities, research institutions and other not-for-profit organizations (NFPs) under guidelines set in enabling legislation of the agencies and their regulations, and in budgets and appropriation legislation controlled by the Office of Management and Budget's (OMB) regulation doctrines and circular, notably OMB Circular A-110.[62] Most of A-110 (and other regulations, circulars and bulletins of OMB) addresses financial controls and reporting, but it includes a provision (section 36(d)) for the government and public to have the benefit of grant-sponsored work (underlying data) used in developing published reports of federal agency action. The steps needed to enjoy this financial benefit, however, are sometimes not worth the expended effort.

In 1999, the fine print in an appropriations measure required grantees, which influence public policy through their research findings, to make underlying data available, including data from medical/psychological clinical studies.[63] The NFP community reacted volcanically and persuaded OMB and Dept. of Health and Human Services, the principally involved granting agency, to construe and apply the new measure narrowly.[64] The interests affected included patient privacy, integrity of research and, frankly, the jockeying among research institutions for money and prestige, which were all further affected by the ability or inability to maintain traditional degrees of confidentiality of research results, at least for limited times.[65]

F. State Secrets in Courts

The State Secrets doctrine, as promulgated by the U.S. Supreme Court and fleshed out by lower courts,[66] empowers the head of an agency to certify personally that certain disclosures in a pending criminal or civil judicial proceeding would be detrimental to national security.[67] Upon such exercise of power by the agency head, a federal court excludes the evidence and may (and in some instances must) shut down the proceeding.[68] It is a rarely invoked

62. Office of Management and Budget, Circular A-110 (revised 11/19/93, as further amended 9/30/99), *available at* http://www.whitehouse.gov/omb/circulars/a110/a110.html (last visited April 27, 2003).

63. Pub. L. No. 105-277, 112 Stat. 2681 (1998).

64. *See, e.g.*, Sarah Brookheart, *Who Owns Your Research? Proposed Changes to OMB Circular A-100 Would Allow FOIA Access to Data*, APS OBSERVER, April 1999, Vol. 12, No. 4, *available at* http://psychologicalscience.org/observer/1999/12_4_1.html; Department of Health and Human Services, National Institutes of Health, National Institute on Drug Abuse, *Minutes of the 71st Meeting of the National Advisory Council on Drug Abuse*, *available at* http://www.drugabuse.gov/NACDA/minutes71st.html (last visited April 28, 2003).

65. *See* Jerry Cohen, *Strategies for Dealing With Stealth Law*, BOSTON GLOBE, Feb. 16, 1999.

66. *See* United States v. Reynolds, 345 U.S. 1 (1953); Ellsberg v. Mitchell, 709 F.2d 51 (D.C. Cir. 1983), *cert. denied*, 465 U.S. 1138 (1984).

67. *See, e.g.*, Stillman v. Dept. of Defense, et al, 209 F. Supp. 2d 185, 230 (D.C. Cir. 2002) (finding that the government failed to meet its burden of showing why disclosure in information would harm national security); Ronald J. Baumgarten, Jr., *Protecting the President Or Serving the Truth" The Arguments For and Against the Protective Function Privilege*, 80 B.U.L. REV. 233, 253 (Feb. 2000).

68. United States v. Reynolds, 345 U.S. 1, 10 (1953) (stating that when a reasonable danger exists in exposing military information relating to national security, the government should not divulge the evidence).

power but could become more frequent. More often, federal prosecutors, and government lawyers decline to bring a case or mount a defense that would compromise state secrets.

To the extent the federal government allows a case to go forward, it can take measures to clear the trial judge, as well as his or her officers, clerks, bailiffs and other court personnel, as well as counsel and staffs and offices of opposing parties – all in addition to conventional litigation protective order measures. Our legal system has not yet assessed the effect of increasing jurisdiction of special courts established under the USA PATRIOT Act[69] and Homeland Security Act of 2002.[70]

IV. FREEDOM OF INFORMATION ACT (FOIA), TRADE SECRET EXCEPTIONS TO SUNSHINE GOVERNMENT AND FEDERAL AGENCIES RESPONSIBILITIES AND OPTIONS

In the 1950s and 1960s, a growing popular appreciation of transparency in government led Congress to enact the 1966 Freedom of Information Act (FOIA).[71] Congress amended the FOIA several times thereafter to make access to federal government records easy and inexpensive and to circumscribe exemptions to a general mandate of disclosure. Under the FOIA, the identity of the requester is irrelevant.[72] The FOIA contains eight exemptions to the disclosure provision.[73]

The courts generally construe the FOIA exemption (4) "trade secrets" term more narrowly than the definition of trade secrets under state laws modeled after the Uniform Trade Secrets Act.[74] The "commercial or financial information" [that is] confidential part of exemption (4) also has a limited coverage.[75] The word "privileged," under exemption (4), refers to classic attorney-client privilege and the like.[76]

Additionally, the Court stated that once the government appropriately invokes this privilege, the judge should not insist upon reviewing evidence, even if the judge is alone in chambers. *Id*.

69. Pub. L. No. 107-56, 115 Stat. 272 (2001).

70. Pub. L. No. 107-296, 116 Stat. 2135 (2002) (amending 18 U.S.C. § 842(i) (2000)).

71. Pub. L. No. 89-559, 80 Stat. 383 (1966) (codified in 5 U.S.C. § 552 (2000)).

72. *Id*.

73. *Id*. Among the eight exemptions includes: (3) [matters][specifically exempted from disclosure by][a] statute [that], "(A) requires that the matter be withheld from the public in a manner that leaves no discretion on the issue or (B) establishes particular criteria . . . ." and "(4) trade secrets and commercial or financial information obtained from a person and confidential or privileged . . . ."

74. *See, e.g.*, Public Citizens Health Research Group v. Food & Drug Admin., 704 F.2d 1280, 1288 (D.C. Cir. 1983) (rejecting the Restatement's definition of trade secrets and defining the term narrower in its common law sense, "which incorporates a direct relationship between the information at issue and the productive process").

75. *See* Nat'l Parks and Conservation Ass'n v. Morton, 498 F.2d 765 (D.C. Cir. 1974), *aff'd in part* and *rev'd in part*, 547 F.2d 673 (D.C. Cir. 1976); AT&T Info. System, Inc. v. GSA, 627 F. Supp. 1396 (D.D.C. 1986).

76. *See* Anderson v. HHS Dept., 907 F.2d 936, 945 (10th Cir. 1990) (recognizing the types of privileges accepted under Exemption 4, historically included "privileges not otherwise specifically embodied in the

FOIA requires agencies to give notice to a submitter of data with purported restrictions to enable reasonable protection and resort to (limited) judicial review.[77] The general theme of the Federal Trade Secrets Act and FOIA exemption (4) is also echoed in various regulatory enactments, including (a non-exhaustive listing) the laws and/or regulations applicable to many agencies.[78] There is an overlap in trade secret and personal privacy protection in some of these restrictions. That itself presents an interesting case of how a (would be) trade secret proprietor can piggyback on privacy rights of customers, employees and others to create trade secret status.[79]

Generally, courts will protect trade secrets or compensate for misappropriation as a taking of property where there is an investment-backed expectation of protection.[80] In fact, federal product safety regulations allow a chemical manufacturer to omit trade secrets from materials safety data sheets with immunity from product liability based on such omission.[81] Nevertheless, agencies do have considerable latitude to disclose information they acquire from private parties to other agencies, to congressional committees and even to the public. Essentially, the risks to trade secret owners are greater than those to the agency.

---

language of Exemption 4 such as the attorney-client privilege").

77. Exec. Order No. 12.600, 52 Fed. Reg. 23.781 (1987).

78. *See generally* Internal Revenue Service, (IRC §§ 6103, 6110, 7213); SEC (15 U.S.C. §§ 78(x)(a) and 176(a) (2000) and 17 C.F.R. §§ 240.246-1, 6-2 (2002)); EPA (7 U.S.C. § 136h(a)(b), 135j (a)(2)(D) (2000); 42 U.S.C. § 7607(a) (2000)); OSHA (29 U.S.C. § 664 (2000)); Commerce Department (15 U.S.C. §§ 1193(1), 1263(h) (2000)); EEOC (42 U.S.C. § 2000e-8e (2000)); Postal Service (39 U.S.C. § 410 (2000)); CPSC (15 U.S.C. § 2055 (2000)); FDA (21 U.S.C. §§ 331 (j), 360j(c) (2000)); Patent & Trademark Office (35 U.S.C. § 122 (2000); 37 C.F.R. § 1.14(b) (2002)). In general, for some two hundred years, patent applications were wholly secret until the government issued the patent. In 2000, Congress amended the law to provide for publication of pending applications in cases if and to the extent the subject matter would be published in a corresponding foreign or international applications. The change complicates the requirement of U.S. patent law for a fulsome disclosure (35 U.S.C. § 112 (2000)) including 'best mode' contemplated at least as of the patent application filing data. A more extensive treatment of patenting vs. trade secret use considerations appears in Prof. Beckerman-Rodau's paper in these Seminar Proceedings. *See* Andrew Beckerman-Rodau, *The Choice Between Patent Protection and Trade Secret Protection: A Legal and Business Decision*, CENTER FOR ADVANCED LEGAL STUDIES - INTELLECTUAL PROPERTY LAW CONCENTRATION CONFERENCE ON TRADE SECRETS, March 14, 2003, at 97 (originally published in 84 J.P.T.O.S. 371 (2002)); *see also* 37 C.F.R. § 202.20(d) (2002). This rule allows the deposit of redacted or otherwise limited specimens to the Copyright Office to back up a copyright registration where a full specimen would destroy trade secret protection. *Id*.

79. For example, pharmaceutical companies regard data from clinical trials as trade secrets and protest when generic competitors try to bootstrap abbreviated new drug applications safety and efficacy claims on the more extensive data of a pharma proprietor who introduced the drug (or a medical device or process) with extensive (and expensive) clinical data as backup. The agency protects the data, but the private party submitter is aggrieved by the free ride.

80. *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1020 (1984). *Cf.*, Phillip Morris Inc. v. Harshbarger, 159 F.3d 670 (1st Cir. 1998) (issuing a preliminary injunction against a state (Massachusetts compulsion to requiring that data be disclosed to the public); Philip Morris v. Reilly, 312 F.3d 24, 47 (1st Cir. 2002) (affirming permanent injunction).

81. *See* Boyette v. L.W. Looney & Son, Inc. 932 F. Supp. 1344, 1348 (D. Utah 1996) (finding defendant was not reckless in not disclosing trade secret because non-disclosure permitted by law).

V. PRIVACY V. POLICE POWER: COMPUTER AND NETWORK REGULATION AFFECTING PROTECTION OF TRADE SECRETS AND RELATED PROPERTY AND AUTONOMY INTERESTS

The legal protection of company trade secrets allows the company to conduct product and facility development and acquisition in peace and with efficiency and gives the company the opportunity to profit from its investment in such development and/or acquisition. Similar considerations attend the law's protection of unhampered use of the company's computer software and network facilities, regardless of whether the software and facilities satisfy the traditional "trade secret" definition (though they often do).[82] Hackers are no less a threat to business than trade secret misappropriators.[83] These two classes of business enemies often overlap and indeed the hacker may have to misappropriate a trade secret or two in aid of his mischief. This section considers several laws passed to protect the integrity of business operations, computer hardware/software and networks, as well as personal information.

A. Federal Wiretap Law and Electronic Communications Privacy Act

The earliest telephones were party lines with no expectation of privacy. Development of point to point connection via modern switching equipment created such expectations and that in turn led to development of wiretapping technology and zeal for usage by law enforcement authorities and business competitors (not to mention jealous spouses). The Federal Communications Act of 1934[84] included a ban on interception and divulgation of telephone communications without sender permissions.[85] Several decades of efforts at self-restraint by law enforcement did not produce good models of behavior. Consequently, advancing technology created a climate for amendment of the communications act in the 1968 enactment of the Omnibus Crime Control and Safe Streets Act (OCCSSA).[86] Title III of OCCSSA is the Electronic Communications Privacy Act[87] (ECPA), which forbids the interception of wire

---

82. MILGRIM, *supra* note 37, at § 1.09.

83. *See generally* REVELATION LOA—ASH, THE ULTIMATE BEGINNER'S GUIDE TO HACKING AND PHREAKING, PROAC MANIAC CLUB § I, *at* http://www.proac.com/crack/hack/files/starthak.txt (Aug. 4, 1996) (defining hacking as "the act of penetrating computer systems to gain knowledge about the systems and how it works").

84. The Federal Communications Act, ch. 652, Title VII [Title VI], § 707 [607], 48 Stat. 1105 (1934) (current version at 47 U.S.C. §§ 151 et. seq. (2000)).

85. 47 U.S.C. §§ 151 et. seq. (2000) (building on anti-interception provisions of the Radio Acts of 1912 and 1927). There are provisions for phone companies to create systems amenable to tapping by law enforcement (with a warrant), a precursor of decades later Clipper Chip-Capstone efforts, cited below. *Id*. In 1978, The Foreign Intelligence Surveillance Act was passed allowing a greater range of federal wiretapping against foreign threats. Pub. L. No. 95-51 (codified at 50 U.S.C. §§ 1801-11 (2000)). The Nixon administration used it against domestic 'enemies.'

86. Pub. L. No. 90-351, 82 Stat. 197 (1968).

87. Pub. L. No. 99-508, 100 Stat. 1848 (1986). Section 605 of the Communications Act and making wire tapping a federal crime. 18 U.S.C. §§ 1510, 2510-2522, 2701-2709, 3121-3126 (2000). There are significant

or oral communications where neither party has consented (one-party consent), with safe harbors for law enforcement.[88] One early failing of the act, since corrected, was the failure to sanction data interception. ECPA also made it a federal crime to manufacture, distribute, possess, advertise, sell or ship any electronic device primarily useful for surreptitious monitoring of conversations.[89]

B. Computer Fraud and Abuse Act

Sabotage of computer systems directly or via a network is a federal crime. Such activity gives rise to civil liability under the 1984 Computer Fraud and Abuse Act[90] (CFAA) and thereafter echoed in states in baby-CFAAs.[91] CFAA makes it illegal to access a computer without authorization or to exceed authorization.[92] The need for CFAA is quite clear. Recently, a hacker broke into a computer database containing eight million American Express, Visa and MasterCard numbers.[93] The FBI is pursuing the case while the financial institution's legal department considers whether to inform the affected customers and/or issue new cards.[94]

C. USA PATRIOT Act; Homeland Security Act; and Pending Patriot II

The enactments of the USA PATRIOT Act[95] the Homeland Security Act of 2002[96] include reduction of privacy protections, clarification that ECPA, Wiretap Act and tracer-enabling statutes apply to cable services and further that

---

exceptions for government use of pen register without a probable cause threshold. The background also included a strong Fourth Amendment decision, Katz v. United States, 389 U.S. 347 (1967) over-ruling Olmstead v. United States, 227 U.S. 438 (1928). A precursor to *Katz* was Silverman v. United States, 36 U.S. 505 (1961) (spike-mike usage violated Fourth Amendment).

88. Some states, including Massachusetts, enacted stricter two-party consent laws.

89. 18 U.S.C. § 2511(1) (2000).

90. Computer Fraud and Abuse Act, Pub. L. No. 98-473, 98 Stat. 2190 (1984) (as codified in 18 U.S.C. § 1030 (2000)).

91. *See, e.g.*, CAL. PENAL CODE § 502 (West 2000) and N.Y. PENAL LAW §§ 156.00 to 156.50 (McKinney 2000); *see also* Eli Lederman, *Criminal Liability For Breach of Confidential Commercial Information*, 38 EMORY L.J. 921 (1989).

92. Computer Fraud and Abuse Act, Pub. L. No. 98-473, 98 Stat. 2190 (1984) (as codified in 18 U.S.C. § 1030 (2000)). Accessing a computer without authorization or to exceed authorization thereby (a) obtain information contained in records of a financial institution, consumer reporting agency, federal agency, a private protected computer (if interstate or international commerce is used) or interfere with operation of such a computer and (b) the intrusion causes loss(es) aggregating $5,000, or more, in a one year period to one or more persons/entities, impairs medical diagnostics or treatments, causes physical injury or threatens health or safety. *Id.*

93. Fred Katayama, *Hacker hits up to 8M credit cards, Secret Service and FBI probe security breach of Visa, MasterCard, Amex and Discover card accounts*, CNNMONEY, February 27, 2003, *available at* http://money.cnn.com/2003/02/18/technology/creditcards/.

94. Processing new cards cost about $25 per card.

95. Pub. L. No. 107-56 (2001). Amendments to 18 U.S.C. §§ 1030, 2331 (domestic terrorism definition) 2702, 2703, 2712, 3103 (delayed notice of search warrants), 3121-27 (2000); 50 U.S.C. §§ 1804-1823 (2000).

96. Pub. L. No. 107-296 (2002).

"computer trespassers" have no privacy right.[97] Additionally, Congress revised the CFAA to provide remedies against "any impairment of the integrity of availability of data, a program, a system or information."[98] The loss definition can include remediation costs, revenue loss and other consequential damages as well as certain aggregation of damages in multiple incidents to meet the $5,000 threshold.[99]

The new era also includes the Total Information Awareness Program,[100] (TIAP) now at DARPA and CAPSII (computer assisted physical screening), in addition to national ID cards and more complete tracking of persons and goods as the next likely steps. TIAP will also involve greater sharing of data with foreign governments.[101] Congress recently has put the legislation on hold for ninety days and seeks assurances of some checks and balances.[102] Many industries applaud this congressional scrutiny and search for balance.[103]

One must also note the older Foreign Intelligence Surveillance Act[104] (FISA) as amended by the later acts and its secret court review process. A recently released FBI memo catalogs high frequency of mistakes in warrant requests under FISA.[105]

The Attorney General will soon propose still further anti-terrorism legislation ("PATRIOT II")[106] adjusting the checks and balances of civil liberties and effectiveness of protection including lessening of limits on wiretapping and police spying and a shift of review responsibilities to the Foreign Intelligence Surveillance Court (FISC).[107] In some circumstances, the

---

97. The acts expanded government access to company records on employees, customers and their habits and personal data, and loosened the evidence needed to justify wiretapping or physical search, including secret searches.

98. USA PATRIOT Act § 814(1)(3), Pub. L. No. 107-56, 115 Stat. 272 (2001) (revising CFAA § 1030(e)(8)).

99. 18 U.S.C. § 1030(e)(11) (2000 & Supplement 2003).

100. Pub. L. No. 108-7, Div. M., § 111, 117 Stat. 534 (2003). Admiral John Poindexter heads the Office of Information Awareness.

101. *See id*.; *see also* Timothy Edgar, *Security vs. Freedom In Intelligence Gathering*, Federal Document Clearing House Congressional Testimony, April 9, 2003.

102. *See generally* John Markoff, *Technology; Software Pioneer Quits Board of Groove*, THE NEW YORK TIMES, March 11, 2003 at 7 (reporting that software pioneer quit board of Groove upon notice that the Dept. of Defense was using Groove for its Total Information Awareness Program). Congressional negotiators gave the Department of Defense ninety days to provide a report to Congress "detailing its costs, impact on privacy and civil liberties and likelihood of success against terrorists." *Id*. Failure to issue a report within the ninety days would compel Congress to stop the Program. *Id*.

103. *See generally* Electronic Privacy Information Center, *Total Information Awareness – Latest News*, *available at* http://www.epic.org/privacy/profiling/tia/ (last visited May 4, 2003).

104. 18 U.S.C. § 1801 et. seq. (2000).

105. 7 (41) BNA Electronic Commerce Law Report 1056-57 (October 23, 2002).

106. *See* Draft of Domestic Security Enhancement Act of 2003, The Center For Public Integrity, *available at* http://www.publicintegrity.org/dtaweb/downloads/Story_01_020703_Doc_1.pdf (last visited April 28, 2003).

107. *See* Charles Lewis & Adam Mayle, *Justice Dept. Drafts Sweeping Expansion of Anti-Terrorism Act*, The Center For Public Integrity, Feb. 7, 2003, *available at* http://publicintegrity.org/dtaweb/report.asp?ReportID=502&L1=10&L2=10&L3=0&L4=0&L5=0

legislation may even let the FBI bypass FISC to spy on foreign and even domestic parties, restrict public access to information about dangerous chemicals, limit defense challenges to secret evidence, and gag grand jury witnesses from discussing their own testimony with media.[108] Also, the legislation may allow for sampling and cataloging of genetic information, revival of the TIPS program (which was shelved after a false start in 2002) and expedited deportation. The expanded roles for data-management, network services and computer systems providers by government contractors and subcontractors in the brave new world are obvious. The spillover into private parties' privacy and trade secret litigation is more subtle, but surely leading to a rethinking of "proper" and "improper" means of acquiring information under USTA and, also, the prospect that another will take (or intercept) proprietary data without controls or compensation.

D. Private Litigation

Private civil cases enforcing the ECPA and/or CFAA are numerous.[109] The traditional trade secret type cases decided under CFAA include *Shurgard Storage Ctr. v. Safeguard Self Storage, Inc.*[110] In *Shurgard*, a departing employee sent his old employer's trade secrets to the new employer via email.[111] This conduct exceeded authorized access to the old employer's electronic file.[112] In another case, spamming was also actionable under CFAA where, an AOL user musician extracted names of other AOL users to develop a spamming list.[113] Accordingly, CFAA is growing into a powerful adjunct to USTA rights and remedies.

E. Other Federal Privacy Protections and Invasions

On April 14, 2003, long debated rules of the Health & Human Services Department (HHS) go into effect pursuant to the Health Insurance Portability

---

108. *See generally* Shannon McCaffrey, *Justice seeks sweeping new powers in hunt for terrorists*, KNIGHT RIDDER WASHINGTON BUREAU, March 30, 2003.

109. In re Double Click, Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001); In re Intuit Privacy Litigation, 138 F. Supp. 2d 1272 (C.D. Cal. 2001); In re America Online Inc. Version 5.0 Software Litigation, 168 F. Supp. 2d 1359 (S.D. Fla. 2001); and In re Toys 'R Us Privacy Litigation (MDL, 2001 U.S. Dist. Lexis 16947 (N.D. Cal. 2001); all being consolidated multi-district litigation matters including numerous respective defendants a motley assemblage of classic rogue hackers and ordinary business competitors, the common link being frustration of a business model of the computer or networks proprietor. *See also* Chance v. Avenue Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001); In re Amazon.com, Inc./Alexa Internet Privacy Litigation, 2000 U.S. Dist. Lexis 8201 (JPML June 7, 2001); In re Real Networks Privacy Litigation, 2000 U.S. Dist. Lexis 1458 (J.P.M.L. Feb. 10 2000). An example of a one-on-one case is eBay, Inc. v. Bidders Edge, Inc; 100 F. Supp. 2d 1058 (C.D. Cal. 2001).

110. 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

111. *Id*. at 1123.

112. *See id.; see also* E.F. Cultural v. Explorica, 274 F.3d 577 (1st Cir. 2001) (finding "website visitor use of 'scraper ' tool exceeded authorized access" in view of history of parties prior relationships).

113. America On-Line, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450-451 (E.D. VA. 1998).

and Accountability Act (HIPAA) after two years of HHS activity and congressional impasse.[114] Elsewhere, proponents heralded the Gramm-Leach-Bliley Financial Services Modernization Act of 2001[115] (GLB) as a measure with teeth to enforce privacy respect by financial service providers (including trust and estate lawyers). On closer analysis, however, the GLB allows trafficking in customer data that becomes a valuable trade secret for the "owner" financial service provider.

The Department of Commerce 'Safe Harbor' privacy standards approximately matches the European Union Data Protection Directive.[116] The Safe Harbor standards are voluntary, but the FTC and SEC will sanction company misstatements of compliance.

Corporate and accounting scandals of recent years, coupled with a stock market melt down, have brought new attention to the quality of disclosures to investors.[117] Sarbanes-Oxley Act of 2002[118] enlists corporate officers and even lawyers as delegates to police corporate reports of status and earnings/loss prospects.[119] The vitality of company IP (including trade secrets) can be an important part of the reportable information. Also, material acquisition or loss of IP rights can be an important item within the rules for immediate public reporting. Reporting and fair disclosure requirements are not limited to public companies.[120] Private companies (especially close corporations and partnerships) may have similar obligations to shareholders under state law fiduciary duties.[121]

The general reaction to corporate reporting and accounting abuses has generated a demand for private scrutiny of corporate reports or stockholder action groups such as Center for Financial Research and analysis, TIAA-CREF, CalPers, Council of Institutional Investors.[122] Meanwhile the SEC has moved

---

114. 45 C.F.R. pts. 160 and 164 (2002).

115. 15 U.S.C. § 6861 (2000).

116. EU Directive 95/46/EC, Official Journal L 282/31. Oct. 11, 1995, *at* http://www.cdt.org/privacy/eudirective/EU_Directive_.html; U.S. Dept. of Commerce July 21, 2000 announcement, 65 Fed. Reg. 45.666 (July 24, 2000), accepted by the EU Commission, *available at* www.europa.eu.int/comm/internal-market/eu/dataprot/adequacy/index.htm.

117. *See, e.g.*, Andrew Countryman, *A distaste for earnings guidance; Predictions can lead to misdeeds, some experts say*, CHICAGO TRIBUNE, December 22, 2002, at 3; John M. Berry, *Official Criticizes Disclosure Status Quo; Securities Insiders Told to Take Initiative*, WASHINGTON POST, November 09, 2002, at E01; Andrew Countryman, *SEC adopts rules to tighten fiscal disclosure*, CHICAGO TRIBUNE, August 28, 2002, at 1.

118. Pub. L. No. 107-204, 116 Stat. 745 (2002).

119. *Id*. at § 302.

120. *See generally* Appletree Square I Limited Partnership v. Investmark, Inc., 494 N.W.2d 889 (Minn. Ct. App. 1993) (duty of disclosure could not be contractually modified so as to require general partner to provide information only on demand).

121. *See generally* JAMES D. COX, THOMAS LEE HAZEN & F. HODGE O'NEAL, CORPORATIONS § 14.16 (2002) (stating that "most recent decisions and some statutes affirm that [a fiduciary] duty is owed to the corporation's shareholders, as well as to the corporation itself").

122. Center for Financial Research, *at* http://www.cfraonline.com/; TIAA-CREF, *at* http://www.tiaa-cref.org/; CalPers, *at* http://www.calpers.org/; Council of Institutional Investors, *at* http://www.cii.org/.

to cut back privileged access of investment analysts. Much of the proprietary information picture of the financial industry will change.[123] In all these instances, a private party becomes an unwilling participant in a government procedure that overlaps the party's own trade secret system, sometimes reinforcing it and sometimes conflicting with it.

On another matter, the government illustrates protective guidance with its National Strategy to Secure Cyberspace (NSSC).[124] The NSSC provides a voluntary blueprint for government and industry cooperation regarding Internet security issues.[125]

VI. INTERSTATE TRANSPORT OF STOLEN PROPERTY ACT; ECONOMIC ESPIONAGE ACT

The Interstate Transport of Stolen Property Act (ITSPA),[126] also known as the National Stolen Property Act, often amended since its 1948 enactment, is a general federal criminal statute making it a federal crime to transport $5,000, or more, of stolen "goods, wares, merchandise, securities or money" in interstate and foreign commerce.[127] The statute works against misappropriation of documentation or electronic media copies of trade secrets where the copies are of high value, but not where value is indeterminate or clearly low.[128]

The Economic Espionage Act of 1996[129] adds §§ 1831-1839 to the Criminal Code making the theft of (or trafficking in) trade secrets for foreign governments, instrumentalities or agents a criminal act.[130] EEA also makes any

123. For example, under Sarbanes-Oxley, investment companies will disclose how they vote their proxies, companies will show off-balance sheet activity to a higher degree, lawyers will become whistle blowers to a higher degree and rating agencies are in danger of aiding and accessory to fraud liability unless they increase their scrutiny and disclosures. And this is just the beginning.

124. National Strategy to Secure Cyberspace, *available at* http://www.whitehouse.gov/pcipb/ (last visited May 5, 2003).

125. *See id*. The NSSC includes goals of (a) empowering home and small business users to protect their cyber resources and access, (b) improving security of federal information and technology, (c) partnership of government (federal and state) with industry to integrate information and IT for security, (d) increased identity trails to help catch perpetrators of hack attacks, (e) leveraging market forces to promote security, and (f) various words of obeisance to privacy and civil liberties values. *See id*.

126. 18 U.S.C. § 2314 (2000).

127. *Id*.

128. *See id*.

129. Pub. L. No. 104-294; 110 Stat. 3488 (1996) (codified in 18 U.S.C. § 1831 (2000)).

130. 18 U.S.C. § 1831 (2000). The EEA defines trade secret as follows:

> (3) the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineers program devices, formulas, designs, prototypes, method, 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 to the public. . . .

Id.

other conversion of a trade secret related to a product produced for interstate or foreign commerce a criminal act.[131] In addition to the criminal remedies, the U.S. Attorney General can bring a civil action to enjoin any violations of EEA.[132] Early on, the government primarily prosecuted under § 1832 even though some of the defendants had apparent links to foreign governments and could have been indicted under § 1831. DOJ proceeded cautiously in implementing the law. For the first five years Main Justice approval was necessary to go forward with an EEA complaint. Now that the five years has expired, regional U.S. attorneys can approve a § 1832 complaint, but Main Justice re-instituted its § 1831 approval need because such may involve delicate matters of foreign relations.

In EEA cases, courts have established that an attempt to steal trade secrets is actionable even if success was impossible.[133] EEA usage has expanded recently and the courts have observed the provision in the act to protect trade secrets during trial.[134] Companies are rightly cautious, however, about invoking criminal remedies for matters that they can resolve by civil action, negotiation or technological measures.[135] Nevertheless, EEA, coupled with ever-ratcheting-up sentencing guidelines, has totemic value signifying the government's will to help owners protect their trade secrets.[136]

VII. EXPORT/TRANSACTION CONTROLS; INVENTION SECRECY ACT

There has been a regime of controls in place regarding control of goods and data since World War I, made pursuant to the War Powers Act.[137] There are also controls on trade and financial transactions with certain countries, including, but not limited to, "enemies." The Export Administration Agency in the Department of Commerce, consulting with DOD and private industry panels, maintains lists of products, data and countries and a matrix of forbidden exports. These exports are the type that can be made pursuant to a specific validated license and made under a general license, with an exception for art

131. 18 U.S.C. § 1832 (2000).

132. Pub. L. No. 104-294, § 101, 110 Stat. 3488 (1996).

133. United States v. Yang, 281 F.3d 534 (6th Cir. 2002) (holding that regardless if the information was a trade secret, legal impossibility was not a defense to a charge of attempted theft of trade secrets); United States v. Hsu, 155 F.3d 189 (3d Cir. 1998) (holding that legal impossibility is no defense to attempt and conspiracy charges).

134. *See* United States v. Hsu, 15 F.3d at 205 (expecting that on remand the district court will conduct an in camera review to determine whether the documents have been properly redacted to exclude only confidential information and to assess whether the redacted information is "material" to the defense).

135. *See* J. Hosteny, *The Economic Espionage Act: A Very Mixed Blessing*, *at* www.hosteny.com/articles/espionage.html

136. A more extensive discussion of EEA is given in Juliane Balliro's paper also in these Seminar Proceedings. *See* Juliane Balliro, Esq., *Criminal Law and Trade Secrets*, CENTER FOR ADVANCED LEGAL STUDIES - INTELLECTUAL PROPERTY LAW CONCENTRATION CONFERENCE ON TRADE SECRETS, March 14, 2003, at 371.

137. 50 U.S.C. Appdx. § 2403-1 (2000).

products and data controlled under International Traffic in Arms Regulations (ITAR)[138] and regarding nuclear materials (DOE), pharmaceuticals (FDA) and agricultural products (USDA), U.S. Department of Treasury Administration Foreign Asset Control Regulations, Cuban Asset Control Regulations and currency transactions generally. Thus, a private sector free trader can come to act as an involuntary trade secret proprietor and a willing trade secret proprietor gets encouragement (at least in the international trade sphere) from the government.

Another special case of control of exports of data is the Invention Secrecy Act (ISA),[139] which establishes a regime of DOD review of new patent applications. In some occasions, ISA allows requests to the Director of the U.S. Patent & Trademark Office (PTO) to issue a secrecy order, renewable year-to-year, that locks up an application within the PTO so that a U.S. patent cannot issue until the PTO lifts the order and prevents the applicant from filing corresponding foreign applications.[140] The Act provides a compensation remedy.[141]

VIII. OTHER FEDERAL INVOLVEMENT TRADE SECRETS

A. Federal Jurisdiction (and non-jurisdiction)

Federal courts act as surrogate state courts in diversity cases and produce about a third of all published decisions as state trade secret law. Federal courts also have federal question jurisdiction to consider the whole panoply of situations mentioned above including claims under federal procurement contracts, claims for taking of private trade secret property through regulation or direct appropriation standing in tort or contract, privacy invasion claims under ECPA, CFAA and the like, under export control laws, and when bankruptcy or tax proceedings involve trade secrets. Also, complainants can join an unfair competition claim (e.g. a trade secret claim) with a patent or copyright cause of action in federal court.[142] Also, a remedy is available at the U.S. International Trade Commission to prevent unfair competition in import commerce by violation of U.S. intellectual property rights including trade secrets, as well as patent, copyright and trademark infringement.[143]

A peculiarity of federal jurisdiction is the Constitution's Eleventh Amendment, which forbids a federal court from awarding damages remedy against a state or any of its instrumentalities.[144] This has made states effectively

138. 22 C.F.R. pts. 120-130 (2002). The U.S. Department of State administers the ITAR.
139. 35 U.S.C. §§ 181-186 (2000).
140. *See id.*
141. 35 U.S.C. § 183 (2000).
142. 27 U.S.C. § 1338(b) (2000).
143. 19 U.S.C. § 1337 (§ 37 of the Trade Act of 1930, as amended) (2000).
144. U.S. CONST. amend. XI. *See, e.g.*, Ex parte New York, 256 U.S. 490, 497 (1921) (finding that federal

immune from monetary claims for patent and copyright infringement. Congress tried to repair the problem by amendments to patent and copyright (and trademark) laws,[145] but the courts have held its enactments unconstitutional.[146] The Eleventh Amendment would apply to block a federal court damages award against a state or any of its agencies or instrumentalities (e.g. a state university) except when the state has consented to be sued in federal court.[147] The next attempt of Congress to provide damages remedies in federal courts for state patent, copyright and trademark infringement should also reach out to cover trade secret misappropriation.[148] In any event, federal courts can enjoin a state official from violating federally protected rights.[149]

Occasionally, non-preemption couples with non-jurisdiction. For example, federal courts have held that patent and copyright law does not preempt state trade secret law.[150] One must distinguish such cases, however, from those cases that applied a false mantle of trade secrets or something akin to it.[151]

There is a continuing effort in Congress to enact a database protection bill similar in application to the European Union's now ten years old Data Base Directive.[152] The Senate Judiciary and Energy committees are working on this and have set April 15, 2003 as the deadline for developing a new bill.[153] It is inevitable. U.S. law has a model in the 1984 Semiconductor Chip Protection

---

courts lack jurisdiction to entertain suit against state by citizens of another state, because of Eleventh Amendment); Edelman v. Jordan, 415 U.S. 651, 662-663 (1974).

145. 35 U.S.C. § 271(h) (2000) (patents); 17 U.S.C. § 511 (2000) (copyrights), 15 U.S.C. § 1122 (2000) (trademarks)

146. College Sav. Bank v. Florida Prepaid Postsecondary Educ. Expense Bd. et al., 527 U.S. 666 (1999); Florida Prepaid Postsecondary Educ. Expense Bd. v. College Sav. Bank, 527 U.S. 627 (1991); Rodriguez v. Texas Comms'n on the Arts, 199 F.3d 279 (5th Cir. 2002) and Chavez v. Arte Public Press, 204 F.3d 601 (5th Cir. 2000). Congressional bills (S. 1611, S. 2031, H.R. 3204) to correct the situation died with the 107th Congress in committee. A new attempt will be made, but trade secrets have been left out of previous attempts and are likely to be left out again. The past and expected bills address patents, copyrights and trademarks.

147. U.S. CONST. amend. XI. *See, e.g.*, Gwinn Area Cmty. Sch. v. Michigan, 741 F.2d 840 (6th Cir. 1984) (holding that action may not be removed unless state waives its Eleventh Amendment immunity and unequivocally expresses its consent to suit in federal court).

148. Federal courts have exclusive jurisdiction of patent and copyright cases and concurrent jurisdiction with state courts under federal and state trademark law, exclusive or non-exclusive jurisdiction under diverse federal laws relating to trade secrets, privacy and/or hacking, and concurrent jurisdiction with state courts as to federal trademark law.

149. *See* Ex parte Young, 209 U.S. 123 (1908).

150. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974), Technicon Med. Inf. Sys. Corp. v. Green Bay Pkg'g, Inc., 687 F.2d 1032, cert. denied, 459 U.S. 1106 (1983); Data General Corp. v. Grumman Corp., 36 F.3d 1147 (1st Cir. 1994); Gates Rubber Co. v. Bando Chem. Indus., 9 F.3d 823 (10th Cir. 1993).

151. Bonito Boats Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141 (1989) (Florida plug-modem statute preempted); Sears Roebuck & Co. v. Stiffel Co., 376 U.S. 255 (1964); and Compco Corp. v. Day-Brite Lighting, Inc., 376 U.S. 234 (1964). In 1998, Congress added a federal plug modem statute to copyright law.

152. *See* Scientific Access to Data and Information, *A Summary of Database Protection Activities*, *available at* http://www.codata.org/data_access/summary.html (last visited May 1, 2003).

153. *See generally*, American Library Association, *available at* http://www.ala.org/Content/NavigationMenu/Our_Association/Offices/ALA_Washington/Issues2/Copyright1/Database_Protection_Legislation/Database_Protection_Legislation.htm#status (discussing the background of database protection and providing an overview of dueling database protection bills).

Law[154] adding a form of *sui generis* protection to integrated circuit layouts and related technology including photographic masks (collectively "Mask Works"), including a provision giving a partial remedy against 'reverse engineering.'[155] In future years, we may see more examples of hybrid forms of protection in the federal realm.

B. Bankruptcy Law

Prior to 1988, a problem existed for intellectual property licenses involving bankrupt companies. In the event of a licensor company bankruptcy, the trustee could "reject" (cancel) an executory contract such as a license granted by the bankruptcy licensor. Economically frail companies feared that licensees would insist on assignments rather than take a license. Congress solved the problem that year in substantial measure by enacting the Intellectual Property Bankruptcy Protection Act of 1988,[156] which added section 365(n)(1) to the Bankruptcy Code covering licenses of patents, copyrights and trade secrets. That section allows a licensee to insist on retaining benefit of the license.[157] The licensee must pay royalties and forego any counter-claims or offsets that would otherwise reduce the royalties.

More subtle forms of the preemption issue are emerging. In *Bowers v. Baystate Technologies*,[158] the court did not preempt a contract prohibiting reverse engineering.[159] Judge Dyk, dissenting, said that state law could thus eviscerate federal law, a peculiar reversal of federal supremacy.[160]

C. Tax Law

Trade secrets constitute property eligible for treatment as a capital asset under IRC § 1231 and for non-recognition when donated to newly formed corporations as LLC under IRC § 351.[161] As for depreciation of such assets, the general rule of *Associated Patentees v. Commissioner*[162] is available to allow estimates of useful life and since 1993, IP transactions (including trade secret licenses) have been eligible for a default 15-year depreciation period.[163]

---

154. Pub. L. No. 98-620, Title III, § 301, 98 Stat. 3347 (1984) (codified in 17 U.S.C. §§ 901-914 (2000)).

155. *See id*.

156. Pub. L. No. 100-506, 102 Stat. 2538 (1988) (codified as amended at 11 U.S.C. §§ 101(52)-(53), 365(n) (2000) (relieving the debtor of its ongoing affirmative performance obligations under the executory license agreement, as well as relieving the debtor of its passive obligation to permit the licensee to use the intellectual property).

157. 11 U.S.C. § 365(n) (2000).

158. 320 F.3d 1317 (Fed. Cir. 2003) (reliance on First Cir. precedent).

159. *Id*. at 1326.

160. *Id*. at 1337.

161. *See, e.g.*, Revenue Ruling 64-56/1964 (pt. 1) C.B. 1330 69-1969-2 C.B. 301; DuPont & Co. v. United States, 288 F.2d 904 (Ct. Cl. 1961) (redefining definitional aspects).

162. 4 T.C. 979 (1945), acq. 1959-2 CB 3; Rev. Rlg. 67-136, 1967-1 C.B. 58.

163. I.R.C. § 379 (2000).

D. Antitrust Law

Remedies in monopolization cases have included forced licenses of intellectual property at zero rate or mandated low rate royalties, sometimes with consent of the defendant, sometimes not. In their antitrust case, Microsoft and DOJ considered such licensing but did not adopt it in the final settlement (still under attack by some states).[164] The FTC and DOJ are analyzing the effect on competition of private standards-setting organizations and will consider IP licensing (including licensing of trade secrets) to mitigate adverse effects.

A modified form of such licensing occurs for communications carriers regulated by the FCC. Local and distance carriers must provide complementary services to each other. This often involves technology transfers or exposure for compatibility between licensees or transfers of license privilege. Some carriers have used the excuse of protection of their trade secrets (or protection of trade secrets licensed to them by third parties) to avoid full compliance with their transfer or exposure obligations.[165]

Generally, the antitrust agencies respect the benefits of IP licensing, as shown in the 1994 DOJ-FTC guidelines on licensing and more recent merger guidelines.[166] The establishment of technology and innovation market concepts, however, has provided tools usable to threaten merger and acquisition transactions.

E. Encryption and E-Commerce Standards

Federal defense and law enforcement agencies (including National Security Agency (NSA) and the National Institute for Standards and Technology (NIST) have had a large role in shaping encryption standards for software and messaging.[167] There has been great debate over back-door access to encryption for law enforcement agencies and as to the level of encrypted software

---

164. *See* Motions, Orders, and Settlement in United States v. Microsoft, *at* http://www.dcd.uscourts.gov/microsoft-2001.html (last visited April 30, 2003).

165. *See* David Rice, *Copyright as Talisman: Expanding Property in Digital Works*, INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY (2001). It is a continuing story as indicated by a recent 3-2 FCC decision excusing local exchange carriers from sharing and unbundling broadband-enabling facilities with long distance competitors (FCC 2/20/03 press release).

166. Antitrust Guidelines for the Licensing of Intellectual Property, 49 BNA PAT. TRADEMARK & COPYRIGHT J. 714, § 5.3, April 13, 1995, *available at* http://www.usdoj.gov/atr/public/guidelines/ipguide.htm.

167. Data Encryption Standard (DES) is an offshoot of that work, translated to private sector by cooperative efforts of NSA, IBM, and NIST's predecessor and NIST is working on an Advanced Encryption Standard (AES). Government contractors and grantees (including MIT, BBN) and private sector spin-offs developed public key encryption standards and the government encourages certification authorities (cyber-notaries and the like). But a well-funded private sector provided explosive growth. NSA designed Clipper Chip and Capstone key structure with a view to mandated use in private encryption schemes to allow a law enforcement back door. For some ten years industry resisted efforts of Republican and Democratic administrations to impose Clipper/Capstone. But after 9/11/01, a great usage of such artifacts is likely. *See generally* www.fbi.gov/nipc, the website of the National Infrastructure Protection Center.

exportable under general license.[168]

At the same time, federal law encourages electronic (digital) signatures,[169] a system generally reliant on encryption, and tries to promote electronic commerce. Recent FTC hearings on e-commerce have shown a growing movement for preemptive federal legislation.[170]

The Federal Reserve Board, NIST and Office of Controller of Currency are major drivers of financial data interchange standards. Non-financial industries are also increasingly relevant on electronic data interchange (EDI) backed by federal infrastructure creation.

G. Digital Millennium Copyright Act

The Digital Millennium Copyright Act of 1998 (DMCA)[171] protects copyrights from cyber-infringement by establishing a protected realm of copyright owners' anti-circumvention and copyright management controls.[172] It basically limits sophisticated technology burglar tools that infringers might otherwise use to overcome less sophisticated technological protection measures.[173] Expressing it in trade secret terms, the copyright owner can take adequate or reasonable measures, not necessarily heroic ones, to limit access to copyright protected material. The law will protect the owner from interference even before the issue of illegal copying of the content occurs.[174] At times, enforcement of DMCA gets out of hand, but the American legal system can correct its own mistakes.

On December 17, 2002, a California jury acquitted Elcomsoft of a criminal trafficking violation of DMCA through a sale by it software to overcome Adobe's blocking software.[175] On January 21, 2003, the U.S. District Court for District of Columbia held a contrary development finding that an ISP (Verizon Internet Services) must provide customer names to a copyright owner group (Recording industries Ass'n of America) seeking out downloaders of music.[176]

---

168. John Schwartz, *Disputes on Electronic Message Encryption Take on New Urgency*, NEW YORK TIMES, September 25, 2001 at C1.

169. Electronic Signatures in Global and National Commerce (E-Sign Act), Pub. L. No. 106-229, Title I, § 1, 114 Stat. 464 (2000) (as codified in 15 U.S.C. § 7001 et seq. (2000)).

170. Testimony: State Impediments to E-Commerce, Federal Trade Commission, September 26, 2002, *at* http://www.ftc.gov/os/2002/09/020926testimony.htm.

171. Pub. L. No. 105-304, § 1, 112 Stat. 2860 (1998) (as codified in 17 U.S.C. pt. 12, §§ 1201-1209 (2000)).

172. 17 U.S.C. § 1201 (2000); *see also generally* 3 NIMMER ON COPYRIGHT, § 12A.03 (2002).

173. *See* NIMMER ON COPYRIGHT, § 12A.03.

174. The law also protects other 17 U.S.C. § 106 exclusive right violations.

175. Alex Salkever, *Digital Copyright: A Law Defanged?*, BUSINESSWEEKONLINE, December 19, 2002, *at* http://www.businessweek.com/technology/content/dec2002/tc20021219_4518.htm (stating that chief software programmer, Dmitry Sklyarov, testified against Elcomsoft in exchange for immunity); Lisa M. Bowman, *ElcomSoft verdict: Not guilty*, C/NetNews.com, December 17, 2002, *available at* http://news.com.com/2100-1023-978176.hmtl.

176. In Re: Verizon Internet Services, Inc., Subpoena Enforcement Matter, Recording Industry Association of America v. Verizon Internet Services, 240 F. Supp. 2d 24 (D. D.C. 2003); 2003 U.S. Dist. LEXIS 6778

Even apart from the U.S. DMCA there are ominous trends in balancing law enforcement with privacy. In Australia recently, music recording companies EMI, Sony and Universal urged the federal court for an order against the University of Melbourne to allow plaintiffs' experts to review all email accounts of students to find sound files as evidence of copyright infringement.[177] The university has agreed to preserve files but continues to resist turnover.[178] Record labels have also warned 300 large companies that they must act to stop illegal song swapping on their company networks.[179]

In the Summer of 2002, the U.S. legislature filed bills that would give immunity to copyright proprietors who use advanced technological means to prevent file swapping even if user computers are thereby disabled to some extent.[180] Opponents warn that this would be the beginning of a war of escalating technologies for protecting versus accessing file content over P2P networks.[181]

H. International Issues

In international relations, the government has obtained some measure of voluntary respect for IP, including trade secrets, from other nations in one on one negotiations backed by threats of economic sanctions. The TRIPS agreement part of the 1994 GATT, amended in the Uruguay-Round, produced some additional harmonization in Article 39 of the World Trade Organization (WTO) Treaty.[182] As a result of that effort, computer treaty parties may now protect secret information as a whole (though components are known), attain commercial value due to the secrecy, and take reasonable steps to protect it. Articles 40-50 relate to civil process to enforce IP rights including trade secrets.[183]

IX. CONCLUSION

The federal government involvement with private trade secrets arises out of

---

(April 14, 2003).

177. Phil Hardy, *EMI, SME and UMG seek the email records of Australian students' accused of downloading music illegally*, MUSIC & COPYRIGHT, March 05, 2003.

178. Simon Hayes, *Telstra raided in $60m piracy probe*, THE AUSTRALIAN, March 06. 2003.

179. Jon Healey, *Industry Targets File Swappers' Employers*, LOS ANGELES TIMES, March 18, 2003 at 1 pt. 3 (informing companies that their computers were being used by workers for illegal file-swapping and threatening "significant legal damages" for employers and employees alike).

180. H.R. 5211, 107th Cong. (2002) (proposing to provide a safe harbor provision at 17 U.S.C. § 574).

181. Drew Clark, *On The Hill: Rep. Issa Plays Referee Between Hollywood, Silicon; Valley*, NATIONAL JOURNAL'S TECHNOLOGY DAILY, November 4, 2002 (pledging that the legislature will work on this bill, or a successor bill, that both sides can embrace).

182. Similar language appears in Article 1711 of NAFTA,

183. A more substantial review of treaties and law of foreign countries are given by Kevin O'Connor elsewhere in these Seminar Proceedings. *See* Kevin O'Conner, *Trade Secret Protection Outside the United States*, CENTER FOR ADVANCED LEGAL STUDIES - INTELLECTUAL PROPERTY LAW CONCENTRATION CONFERENCE ON TRADE SECRETS, March 14, 2003, at 59.

government procurement, regulation of interstate and international commerce (including many health and safety matters once left to state control), state secrets overlapping private trade secrets and diverse forms of federal court jurisdiction over ordinary trade secret cases. The take-home point is that counsel for trade secret owners and their competitors must consider federal law issues and how those will affect protectability of particular items of information and the efficiency of protecting those items from misappropriation or even expropriation.