HOLDING FOREIGN NATIONS CIVILLY ACCOUNTABLE FOR THEIR ECONOMIC ESPIONAGE PRACTICES

CHRISTOPHER G. BLOOD*

I. INTRODUCTION

On February 20, 2001 a veteran FBI counterintelligence agent, Robert Hanssen, was arraigned on charges of spying for Russia over a period of fifteen years.[1] The espionage activities of Hanssen subsequently received a great deal of attention and led to the expulsion of Russian diplomats from the United States.[2] On the same day that Hanssen was arraigned, however, another case of espionage was revealed that has received comparatively little attention. The second case involved a Swedish man working for a Swiss-Swedish industrial firm who was arrested by Swedish police.[3] This Swedish spy, like the FBI agent, had allegedly been working for the Russians and was charged with "grave espionage" by the Swedish government, a charge that only five people have been arrested for in Sweden since World War II.[4] Despite the relative rarity of those charges, the Swedish case received but a fraction of the media coverage accorded the Hanssen case.[5]

---

* The author is a May 2001 graduate of the Thomas Jefferson School of Law in San Diego, CA.

1 *See e.g.* Robin Wright & Robert L. Jackson, *U.S. Charges FBI Agent with Spying for Russia Since 1985*, L.A. Times A1 (Feb. 21, 2001).

2 *See e.g.* Robin Wright & Eric Lichtblau, *U.S. Orders 50 Diplomats From Russia to Leave*, L.A. Times A1 (Mar. 22, 2001) (indicating that the story continues to reverberate a full month later).

3 *See e.g.* Associated Press, *Sweden Detains Man Suspected of Spying*, Milwaukee Journal Sentinel (Milwaukee, Wis.) (Feb. 21, 2001).

4 *See id.*

5 *See e.g.* Brian Knowlton, *FBI Agent Accused of Passing Grave Secrets to Russians*, International Herald Tribune 2001 WL 4852058 (Feb. 21, 2001); Ben McIntrye, *Double Agent was Neighbor Above Suspicion*, The Times of London 2001 WL 4877224 (Feb.

Why so much attention to one story and almost none to the other? Perhaps Russia's former head of the Federal'naya Sluzhba Bezopasnosti ("FSB") intelligence service summed it up best. He first denied any Russian involvement with the American FBI agent, and then went on to state that the Swedish case was "presumably a highly insignificant case of technical espionage."[6] It seems as if economic espionage,[7] the targeting and acquisition of trade secrets and sensitive financial and economic policy information by a foreign government, is not to be viewed in the same light as traditional espionage, which is defined as the clandestine collection of national defense information by a foreign government.[8] The belief so candidly expressed by the former Russian intelligence chief, that economic espionage should be considered "insignificant," is a belief that has cost U.S. firms billions of dollars.[9]

Targeting of proprietary economic information by foreign nations has been labeled a "growing concern" by U.S. government officials.[10] Further, many of the instances of economic espionage documented by the FBI have involved U.S. allies.[11] This paper seeks to provide an overview of the espionage threat to U.S. firms, and advocates increased efforts to hold those responsible for such acts civilly liable. The magnitude of the economic espionage problem is outlined in Part II of this paper. Part III discusses the lack of international resolve to stem the problem. Lastly, Part IV discusses judicial remedies within the United States for holding

---

21, 2001); Paul Koring, *Trusted FBI Agent Arrested For Spying*, The Toronto Globe and Mail A10 (Feb. 21, 2001). These non-U.S. publications ran stories on the Hanssen case but made no mention of the Swedish case. While U.S. media coverage of the FBI agent case might be expected to be, and indeed was, much greater than that of the Swedish case it is noteworthy that foreign media coverage likewise has been so disproportionate.

6 Deutsche Presse-Agentur, *Russia's Ex-Intelligence Chief Doubts U.S. and Swedish Spy Cases*, (Feb. 21, 2001).

7 Darren S. Tucker, *The Federal Government's War on Economic Espionage*, 18 U. Pa. J. Int'l Econ. L. 1109, 1112 (1997).

8 *See id.* at 1112-1113. The author goes on to provide the following definition of 'industrial espionage': "A corporation's use of illegal techniques to collect information, such as trade secrets, not voluntarily provided by the source." *Id.* at 1113.

9 *See e.g.* Edwin Fraumann, *Economic Espionage: Security Missions Redefined*, 57 Pub. Admin. Rev. 303 (1997).

10 *See* Annual Report to Congress on Foreign Economic Collection and Industrial Espionage (1999) <http://www.nacic.gov/fy99rpt.html> [hereinafter Annual Report 1999] (visited April 1, 2001).

11 Peter Schweizer, *The Growth of Economic Espionage: America is Target Number One*, Foreign Affairs, Jan./Feb. 1996, 11 [hereinafter Growth of Economic Espionage].

offending nations accountable for their actions and proposes making greater use of a 1976 federal statute to combat the problem of economic espionage.

II. THE MAGNITUDE OF THE ECONOMIC ESPIONAGE PROBLEM

Foreign governments procure U.S. trade secrets in a variety of ways.[12] Some nations have long-standing associations between their governments and industries within the United States.[13] Alternatively, foreign nations exploit existing nongovernmental organizations to carry out their intelligence activities or even create new organizations for that purpose.[14] Further, foreign governments create "front" companies to conceal their identity and activities, and enter into joint ventures with American companies with the primary objective of illicitly obtaining information.[15] Moreover, foreign nations sponsor research at U.S. universities and research centers for the express purpose of gaining proprietary information from those U.S. facilities.[16] Indeed, it was recently reported that fifty-eight percent of the suspicious activities targeting critical technologies were either directly sponsored by foreign governments or carried out by a business affiliated with a foreign government.[17] In other instances yet, it is merely indeterminable whether the attempt to collect intelligence was sponsored by a foreign government or whether it resulted from a foreign corporation acting on its own.[18]

Economic espionage is not an activity carried on solely by the United States' former cold war adversaries.[19] In fact, one FBI analysis determined that dozens of nations were surreptitiously attempting to obtain advance technologies from U.S. companies.[20] It should be noted, though, that much intelligence gathering by foreign nations within the U.S. is

---

12 *See* Annual Report to Congress on Foreign Economic Collection and Industrial Espionage (2000) <http://www.nacic.gov/fy00rpt.html> [hereinafter Annual Report 2000] (visited April 1, 2001).

13 *See* Annual Report to Congress on Foreign Economic Collection and Industrial Espionage (1997) <http://www.nacic.gov/fy97rpt.html> (visited April 1, 2001).

14 *See* Annual Report to Congress on Foreign Economic Collection and Industrial Espionage (1995) <http://www.nacic.gov/fy95rpt.html> (visited April 1, 2001).

15 *See id.*

16 *See id.*

17 Annual Report 2000, *supra* n. 12.

18 *See id.*

19 *See* Peter Schweizer, *Friendly Spies*, Atlantic Monthly Press (1993).

20 Growth of Economic Espionage, *supra* n. 11, at 11.

legitimate.[21] Nevertheless, foreign nations have frequently engaged in activities that can only be described as trade secret theft.

Japanese agents, operating out of the Japanese consulate in San Francisco, worked with a researcher at Fairchild Semiconductors in Silicon Valley to steal corporate plans and secrets on computer developments.[22] As much as 160,000 pages of confidential information may have been passed through consular officials to Japanese corporations that were in competition with Fairchild.[23] Indirect support for such activities by foreign governments is not uncommon.[24] As early as 1972, the Japanese Parliament established the Economics Industry Deliberation Council to direct intelligence gathering.[25] Oversight of this council was by the Ministry for Trade and Industry,[26] which decades earlier had been the conduit for the Japanese government to subsidize worldwide travel by thousands of Japanese businessmen for the purpose of gathering information on foreign technological advances.[27] By the late 1980s, a CIA classified report indicated that more than three-fourths of Japan's intelligence resources were aimed at acquiring secrets and information on technological advances from the United States and Western Europe.[28]

Japan is certainly not the only Asian nation that represents a threat to U.S. companies through surreptitious attempts at intelligence gathering. In 1980, the Korean CIA reorganized itself into the National Security Planning Agency with one of its four main objectives to gather economic intelligence in the U.S. and Japan.[29] Further, a 1998 survey of 1300 American companies indicated that China was viewed as the greatest economic espionage threat.[30] Indeed, the Chinese Ministry of State Security

---

21 *See* Annual Report to Congress on Foreign Economic Collection and Industrial Espionage (1998) <http://www.nacic.gov/fy98rpt.html> (visited April 1, 2001).

22 *See Friendly Spies*, *supra* n. 19, at 38-39.

23 *See id.*

24 *See id.* at 78.

25 *See id.*

26 *See id.*

27 *See Friendly Spies*, supra note 19, at 74.

28 *See id.* at 71.

29 *See id.* at 206.

30 *See e.g.* Edward A. Robinson & Ann Harrington, *China's Spies Target Corporate America in the Great Game of Economic Espionage*, Fortune Magazine 1998 WL 2501093 (Mar. 30, 1998).

has an extensive network of agents within the U.S. who are routinely tasked to gather products or data that will benefit Chinese industry.[31]

Nor are Asian nations alone in their intelligence gathering efforts targeting the United States. As early as the 1970s, French intelligence installed electronic listening devices in the business class sections of Air France flights between New York and Paris.[32] In 1991, American executives of GTE, NCR, and AT&T all reported returning to their Paris hotel rooms to find confidential documents containing trade secrets stolen from their briefcases and laptop computers.[33] Further, French officials have gone on record essentially sanctioning such conduct. The head of the French Intelligence Agency that was responsible for bugging the commercial airlines said in his memoirs, "Spying in the proper sense is becoming increasingly focused on business and the economy, science, and industry -- and very profitable it is. It enables the Intelligence services to discover a process used in another country, which might have taken years and possibly millions of francs to invent or perfect."[34]

Another former director of French Intelligence, Pierre Marion, defended economic espionage against the U.S.: "In economics, we are competitors, not allies. I think that even during the Cold War getting intelligence on economic, technological, and industrial matters from a country with which you are allies is not incompatible with the fact that you are allies."[35] Thus, it should have come as no surprise when French Intelligence took up residence in Seattle with sophisticated telemetry equipment and microwave transmission receivers to collect data from Boeing's test flights of its new jumbo jet in 1988.[36] Nor should it have come as a surprise that Airbus, a French government-subsidized aerospace company, placed similar Boeing style navigation systems in its aircraft just two years later.[37]

France is not the only European ally that has had designs on illicitly procuring U.S. technologies. In one economic espionage case involving a special agent of the West German intelligence service, the Bundes-

---

31 *See id.*

32 *See Friendly Spies*, *supra* n. 19, at 103-104.

33 *See id.* at 105.

34 *See id*. at 105. The statement was made by Count de Marenches, who was head of the Service de Documentation Exterieure et de Contre-Espionnage ("SDECE") from 1970-1981.

35 *See id*. at 9 (quoting Pierre Marion who succeeded Marenches as head of the SDECE in 1981).

36 *See id.* at 123.

37 *See id.* at 124.

Bundesnachrichtendienst ("BND"), the operative targeted a high-tech company near Boston and seduced a mid-level administrator.[38] The BND agent persuaded the administrator to provide sensitive documents on the company's biochip research.[39] Once the administrator had provided several sets of documents, the agent then used the threat of revealing these actions to get her to continue pilfering secrets.[40] The woman eventually attempted suicide when security officials questioned her about the missing documents, and the BND agent returned to Europe to presumably continue his work elsewhere.[41]

Nor is it merely European and Asian allies that direct their economic espionage efforts at the United States. The Israeli Defense Ministry's Scientific Affairs Liaison Bureau ("LAKAM") has targeted companies in the United States, as well as in Japan, France, Germany, Great Britain, and Switzerland.[42] A Swiss engineer was persuaded to pass blueprints for the French Mirage fighter aircraft to Israeli agents: within four years of the time that the engineer was caught and convicted, the Israelis had developed their Kfir fighter aircraft, a near carbon copy of the Mirage.[43] Later, an Illinois company, Recon Optical, which had contracted with the Israeli military to produce aerial reconnaissance cameras for the Israeli Air Force, caught Israeli officers who worked at the plant trying to ship trade secrets to an Israeli defense firm.[44]

While many of the aforementioned cases occurred in the 1980s and 1990s, economic espionage continues to this day.[45] The most recent report by the National Counterintelligence Center indicates that there has been no reduction in attempts by foreign governments, companies, and individuals to acquire U.S. trade secrets.[46] The CIA recently reported that the intelligence services of more than a half dozen nations are presently trying to steal U.S. proprietary economic information.[47] The American Society of Industrial Security recently estimated the cost to U.S. firms from economic

---

38 *See Friendly Spies*, *supra* n. 19, at 169.

39 *See id.* at 170-171.

40 *See id.* at 173.

41 *See id.* at 175.

42 *See id.* at 213.

43 *See Friendly Spies*, *supra* n. 19, at 220.

44 *See id.* at 236.

45 Annual Report 2000, *supra* n. 12.

46 *See id.*

47 *See e.g.* Sean Webby, *Foreign Spies in High Technology Industries Hard to Catch*, Knight Ridder Tribune Business News, 2001 WL 13621804 (Feb. 11, 2001).

and industrial espionage at $1 trillion dollars.[48] Indeed, one of President Clinton's last presidential directives before leaving office was an order establishing a counterintelligence board with a heightened focus on economic espionage.[49]

III. THE LACK OF INTERNATIONAL RESOLVE TO STEM THE PROBLEM

Given the extent of foreign nations' involvement in attempts to procure U.S. trade secrets, it is natural to question why these nations are so unhesitant in their targeting of United States' firms. The answer may be because, in general, there appears to be little international will to recognize and address the problem of trade secret theft. Indeed, it is possible that some foreign nations do not view economic espionage as being a violation of international law, and thus do not view their actions of espionage as a serious offense at all.[50] After all, spies in general are viewed as patriots by their nations.[51] The U.S., for instance, has no specific national legislation that would prohibit espionage against other nations.[52] In fact, the domestic law of many if not most nations promotes the intrusion upon foreign territories for the collection of intelligence information.[53]

Nor does international law look very harshly on the practice of economic espionage. One accepted way of ascertaining the international law on a particular subject is via an examination of the general principles of law recognized by civilized nations.[54] If so many countries are collecting intelligence information surreptitiously, some nations may reason, then the activity must not be too great of an offense. Further, the law of war does not recognize spying as an international violation during wartime;[55] and some nations may view their peacetime attempts at procurement of corporate intelligence as mere extensions of their wartime practices that are now justified by 'economic war.'

---

48 *See id.*

49 *See e.g.* David A. Vise, *Clinton Creates Counterintelligence Board; The FBI, CIA, Defense Dept. Will Combine Efforts to Find Strategies to Fight Spying*, Washington Post (Washington, D.C.) A5 2001 WL 2534279 (Jan. 5, 2001).

50 Scott, *supra* n. 50.

51 *See id.* at 218.

52 *See id.* at 220.

53 *See id.* at 226.

54 *See Hilton v. Guyot*, 159 U.S. 113, 144 (1895); Statute of the International Court of Justice, June 26, 1945, chap. II, art. 38, 59 Stat. 1031, 33 U.N.T.S. 993.

55 *See e.g.* Scott, *supra* n. 50 at 218 (Referencing the Operations Law Handbook, at 17-5).

A second and related reason why many foreign nations take such a cavalier attitude regarding their practice of economic espionage may be because of the failure of international treaties to specifically prohibit the practice. The Paris Convention for the Protection of Industrial Property,[56] a treaty designed to safeguard intellectual property rights, has been in effect in various forms since 1883. This treaty does not explicitly require signatory nations to enact legislation to protect trade secrets. The closest that the Paris Convention comes to such a prohibition is in Article 10*bis*(1), which directs members to assure their nationals protection against unfair competition.[57] Article 10*bis* then goes on to define unfair competition as "acts of competition contrary to honest practices in industrial or commercial matters."[58] Article 10*bis* does specify particular acts that are prohibited: 1) acts of a nature that will create confusion with the goods of a competitor, 2) false allegations to discredit the goods of a competitor, and 3) allegations liable to mislead the public as to the characteristics of goods.[59] Unfortunately, there is no mention in the Paris Convention that theft of proprietary information qualifies as the type of unfair competition that is specifically barred by this treaty.

A second international treaty that speaks more directly to the issue of trade secrets is the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS").[60] Article 39 of TRIPS specifically comes under the heading of "Protection of Undisclosed Information."[61] Article 39 states:

> 1. In the course of ensuring effective protection against unfair competition as provided in Article 10*bis* of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3.
>
> 2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices[10] so long as such information:
>
> (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or read-

---

56 Paris Convention for the Protection of Industrial Property, Mar. 20, 1883, 21 U.S.T. 1538, 828 U.N.T.S. 305 (last revised July 14, 1967) [hereinafter Paris].

57 *See id.* at art. 10*bis* (1).

58 *See id.* at art. 10*bis* (2).

59 *See id.* at art. 10*bis* (3).

60 Agreement on Trade-Related Aspects of Intellectual Property Rights, 33 I.L.M. 1197 (Apr. 15, 1994) [hereinafter TRIPS].

61 *See id.* at § 7, art 39.

> ily accessible to persons within the circles that normally deal with the kind of information in question;
>
> (b) has commercial value because it is secret; and
>
> (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.[62]

Unfortunately two provisions in Article 39 undercut its effectiveness in protecting trade secrets from economic espionage. The first is seen in paragraph 1 of Article 39.[63] In specifically referencing the Paris Convention's Article 10*bis*, TRIPS leaves itself open to being construed to afford no more protections against unfair competition than those accorded by the Paris Convention. And those protections, as was pointed out earlier, are virtually nil with regard to the protection of trade secrets. The second provision of Article 39 that undercuts its effectiveness at safeguarding trade secrets is found in footnote 10 referenced within Article 39(2). This footnote reads as follows:

> For the purpose of this provision, "a manner contrary to honest commercial practices" shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition.[64]

By providing specific examples of activities "contrary to honest commercial practices," and by failing to specifically include the unlawful taking of proprietary information, the TRIPS treaty may implicitly suggest to its signatories that the protection of trade secrets is of but ancillary importance in the overall scheme of intellectual property rights protection.

Other contributing factors to the view that economic espionage within the United States is acceptable behavior are not altogether clear. But, while international law principles do not specifically allow espionage, the widespread practice of this activity by civilized nations suggests that, at least by one measure of international law,[65] these activities may not be violative of the laws of nations. And, international treaties pertaining to intellectual property right protections[66] do not provide any real justification for nations to fear sanctions if they are caught procuring trade secrets. Hence, it may be that it is largely incumbent upon U.S. firms to act on their

---

62 *See id.* at art. 39.

63 *See id.* at art. 39(1).

64 *See id.* at art. 39(2) n. 10.

65 Statute of the International Court of Justice, June 26, 1945, chap. II, art. 38(1)(c), 59 Stat. 1031, 33 U.N.T.S. 993.

66 TRIPS, *supra* n. 56, 60.

own behalves if targeted by foreign governments seeking proprietary information.

IV. REMEDIES AVAILABLE TO U.S. FIRMS

Given the economic espionage threat to American firms, and the relative lack of international resolve to prevent such activities, the question arises as to what recourse a U.S. company has when it has been targeted by a foreign nation seeking to illicitly procure proprietary information. Theft of trade secrets is costing U.S. firms billions of dollars,[67] and these firms need the tools to fight back. While criminal sanctions against the defendant may provide an offended firm some satisfaction, when a business has been subject to an illicit action costing them a substantial monetary loss the most desirable remedy will generally be compensation for that injury.

A. *State Law Remedies*

One way of seeking compensation from those that steal trade secrets is by bringing an action in state court. The Supreme Court, in *Kewanee Oil Co. v. Bicron Corp.*, held that state trade secret laws are not preempted by federal law.[68] Thus, corporations may seek civil damages via a common law tort action or through state legislation modeled after the Uniform Trade Secrets Act.[69]

The Restatement of Unfair Competition (Third) is one basis for bringing a tort action, and provides the following definition of a trade secret: "A trade secret is any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others."[70] The Restatement goes on to hold that "One is subject to liability for the appropriation of another's trade secret if: 'the actor acquires by means that are improper under the rule stated in § 43 information that the actor knows or has reason to know is the other's trade secret."[71]

The Restatement then defines acquiring by improper means in the following manner:

---

67 Webby, *supra* n. 47.

68 *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470 (1974).

69 *See* Uniform Trade Secrets Act (West Supp. 1997) [hereinafter USTA].

70 Restatement *(Third)* of Unfair Competition § 39 (1995).

71 *Id.* at 40.

> "Improper" means of acquiring another's trade secret under the rule stated in § 40 includes theft, fraud, unauthorized interception of communications, inducement of or knowing participation in a breach of confidence, and other means either wrongful in themselves or wrongful under the circumstances of the case. Independent discovery and analysis of publicly available products or information are not improper means of acquisition.[72]

Further, the Restatement goes on to provide the basis for any sought-after compensation:

> One who is liable to another for an appropriation of the other's trade secret under the rule stated in § 40 is liable for the pecuniary loss to the other caused by the appropriation or for the actor's own pecuniary gain resulting from the appropriation, whichever is greater, unless such relief is inappropriate under the rule stated in Subsection (2).[73]

Thus, under § 39, the sensitive information on biochip research documents that were obtained by the spying "Lothario" from the German BND, cited in Part II earlier, clearly qualify as trade secrets. The documents could be used in the operation of a business, and they were sufficiently valuable to afford an actual or potential economic advantage to the possessor of that information. Further, under § 40, one is subject to civil liability for the appropriation of a trade secret if the actor knowingly acquires that secret information by improper means. The sensitive documents obtained by the BND agent certainly did not fall into his hands unknowingly—the agent went to great lengths to acquire them.[74] Further yet, § 43 defines 'improper means' to include theft, fraud, unauthorized interception, and inducement of or knowing participation in a breach of confidence. And that is exactly what the German Lothario did—he induced the administrative assistant to breach a confidence with her employer and to provide him the secret documents. Finally, § 45 of the Third Restatement holds the offender liable to the extent of the wronged business' actual pecuniary loss or for the amount of the trade secret stealer's gain, whichever is greater.

A second vehicle for bringing a state action for theft of trade secrets is under state legislation modeled after the Uniform Trade Secrets Act ("UTSA").[75] Most states have enacted legislation that parallels the UTSA,[76] which is shown, in pertinent part, below:

---

72 *Id.* at 43.

73 *Id.* at 45.

74 *See Friendly Spies*, *supra* n. 19, at 168-173.

75 UTSA, *supra* n. 69.

> §1. Definitions
>
> As used in this Act, unless the context requires otherwise:
>
> (1) "Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means.
>
> (2) "Misappropriation " means: (i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means;
>
> (4) "Trade secret" means information, including a formula, pattern, compilation, program device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[77]

Thus, under legislation modeled after the UTSA, a firm could bring an action against the spying "Lothario" on the basis of any formulas, methods, techniques, or processes[78] that were in the documents which were obtained by the agent inducing a breach of duty to maintain secrecy.[79] Moreover, under "UTSA-type" legislation not only can the firm collect damages for the actual pecuniary loss or for the amount of "Lothario's" unjust enrichment,[80] but they may also seek attorney fees[81] and obtain punitive damages equal to twice the actual loss suffered by the firm.[82] One potential drawback to suing for theft of trade secrets is the fact that those secrets are subject to discovery in the course of litigation.[83] However, legislation modeled after the UTSA has a provision for protection of those secrets during the course of litigation.[84]

---

[76] Jeff Augustini, *From Goldfinger to Butterfinger: The Legal and Policy Issues Surrounding Proposals to Use the CIA for Economic Espionage*, 26 Law & Pol'y Int'l Bus. 459, 475 (1995).

[77] UTSA, *supra* n. 69, at § 1.

[78] *Id.* at § 1(4).

[79] *Id.* at § 1(1).

[80] *Id.* at § 3(a).

[81] *Id.* at § 4.

[82] *Id.* at § 3(b).

[83] James H.A. Pooley, Mark A. Lemley & Peter J. Toren, *Understanding the Economic Espionage Act of 1996*, 5 Tex. Intell. Prop. L.J. 177, 206 (1997).

[84] UTSA, *supra* n. 69, at § 5(b).

B. *Federal Law Remedies*

Remedies under federal law may also apply where a firm has been the subject of trade secret theft. There is a federal Trade Secrets Act,[85] but this legislation only applies to federal employees who divulge trade secrets. The National Stolen Property Act ("NSPA") penalizes those who, in foreign commerce, have transported goods known to have been stolen and that have a value of more than five thousand dollars.[86] A major drawback to the use of the NSPA, however, is that intellectual property was held by a federal Court of Appeals not to constitute the "goods, wares, merchandise, securities, or money" that is covered in the NSPA.[87] Additionally, the Supreme Court has held that the property rights of copyright holders have a character distinct from the possessory interest of the owner of simple goods, as is required by the NSPA.[88] Thus, it appears that trade secrets, as with other forms of intellectual property, will not qualify as property protected by the NSPA.

The Economic Espionage Act ("EEA") of 1996[89], another federal law dealing with trade secret theft, in pertinent part states:

> (a) In general.--Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly--
>
> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
>
> (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;[90]

As used in this chapter--

> (1) the term "foreign instrumentality" means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially

---

85 18 U.S.C . § 1905.

86 18 U.S.C. § 2314.

87 *United States v. Brown*, 925 F.2d 1301, 1308, 17 U.S.P.Q.2d 1929 (1995).

88 *Dowling v. United States*, 473 U.S. 207, 221, 226 U.S.P.Q.529 (1985).

89 18 U.S.C. §§ 1831-39.

90 18 U.S.C. § 1831.

> owned, controlled, sponsored, commanded, managed, or dominated by a foreign government;
>
> (2) the term "foreign agent" means any officer, employee, proxy, servant, delegate, or representative of a foreign government;
>
> (3) the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if--
>
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
>
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public;[91]

Thus, if the BND incident were to happen today, the German agent probably could be found guilty of theft of a trade secret under Section 1831 when he obtained the trade secrets by "fraud, artifice or deception."[92] The biochip technology mentioned in the BND incident certainly would come within the definition of a trade secret by virtue of the fact that it is scientific, technical, or engineering information.[93] Under the EEA there is also a provision for the court to take all measures to maintain the confidentiality of the information during the courtroom proceedings.[94]

However, the downside to a targeted firm with all three of the just mentioned federal actions is that they provide for criminal penalties and not civil liabilities. The targeted firm can go to federal law enforcement agencies and complain but the most they will get out of the experience is seeing the offender behind bars. The EEA does provide for criminal forfeitures of the stolen trade secrets,[95] but this will often be long after the damage was incurred. Interestingly, there may be a provision for recovering any proceeds that were obtained from the illicit theft, [96] but again, this action would solely be in the hands of the federal prosecutors bringing the case.

---

91 18 U.S.C. § 1839.

92 18 U.S.C. § 1831.

93 18 U.S.C. § 1839.

94 18 U.S.C. § 1835.

95 18 U.S.C. § 1834.

96 *Id.* at 1834(b).

C. *Combining State Law Remedies with a Federal Statute*

Where trade secrets are stolen, and the perpetrator has either fled the country or is without much in the way of financial resources, the firm will have little to gain by bringing a civil suit. But, where the perpetrator was a representative of a foreign government, as is quite often the case, the targeted firm may at times employ the tactic of bringing a civil suit against the foreign government itself to obtain compensation for the theft. This might best be accomplished through a combination of state law and a federal statute.

With limited exceptions, U.S. citizens are prohibited by the doctrine of sovereign immunity from seeking monetary damages from their own government.[97] Just as our own government is immunized from suit, foreign governments are similarly immune from suit by U.S. citizens.[98] As early as 1812, the Supreme Court recognized the concept of sovereign immunity as being the one exception to the absolute jurisdiction of a nation within its territory.[99] While continental Europe was applying limits to the notion of sovereign immunity in the 19th century, the U.S. was moving toward absolute recognition of foreign sovereign immunity within its territory.[100] In the 20th century, however, the notion of absolute sovereign immunity for foreign nations fell out of favor in the United States.[101] In 1976, the U.S. codified its new "restrictive" principle[102] of sovereign immunity in the form of the Foreign Sovereign Immunities Act ("FSIA").[103] The FSIA still recognizes foreign sovereign immunity, but now seven exceptions to this immunity are statutorily delineated.[104]

At issue, then, is whether the FSIA can be used by a U.S. firm to obtain jurisdiction over foreign governments when those nations have been involved in the theft of trade secrets from that firm. There are two major

---

97 *See e.g.* Stephen G. Breyer, Richard B. Stewart, Cass R. Sunstein & Mathew L. Spitzer, Administrative Law and Regulatory Policy 812 (1999).

98 *See Schooner Exchange v. M'Fadden*, 11 U.S. 116, 145-46 (1812).

99 *See id.* at 147.

100 *See* Joan E. Donoghue, *Taking the "Sovereign" out of the Foreign Sovereign Immunities Act: A Functional Approach to the Commercial Activity Exception*, 17 Yale J. Int'l L. 489, 496 (1992).

101 *See id.* at 497.

102 *See e.g.* Peter Malanczuk, Akehurst's Modern Introduction to International Law 119 (7th Edition 1997). Under the restrictive principle, nations do not enjoy immunity for their commercial transactions.

103 28 U.S.C. §§ 1602-11.

104 28 U.S.C. § 1605.

hurdles that firms must overcome to use the FSIA. First, the perpetrator of the offense must qualify as a foreign state, which is defined in the FSIA as:

> (a) A "foreign state", except as used in section 1608 of this title, includes a political subdivision of a foreign state or an agency or instrumentality of a foreign state as defined in subsection (b).
>
> (b) An "agency or instrumentality of a foreign state" means any entity--
>
> (1) which is a separate legal person, corporate or otherwise, and
>
> (2) which is an organ of a foreign state or political subdivision thereof, or a majority of whose shares or other ownership interest is owned by a foreign state or political subdivision thereof, and
>
> (3) which is neither a citizen of a State of the United States as defined in section 1332(c) and (d) of this title, nor created under the laws of any third country.[105]

Under this definition, the Israeli officers, mentioned in Part II, caught by Recon Optical trying to ship secrets to Israel, would qualify as a foreign state. Military officers are separate legal persons; they, as members of the military, are an organ of a foreign state; and, they are not citizens of the United States. Similarly, if the spying "Lothario" can be tied to the German BND, he also qualifies as a 'foreign state' under 1603.

The second hurdle to obtaining jurisdiction over the offending foreign state is to show that one of the seven FSIA sovereign immunity exceptions encompasses the theft of trade secrets. Depending upon the exact circumstances, there may be several exceptions that would allow a U.S. firm to sue for damages. One possible FSIA exception to immunity is 1605 (a)(2) which states:

> in which the action is based upon a commercial activity carried on in the United States by the foreign state; or upon an act performed in the United States in connection with a commercial activity of the foreign state elsewhere; or upon an act outside the territory of the United States in connection with a commercial activity of the foreign state elsewhere and that act causes a direct effect in the United States;[106]

Thus, a U.S. firm could bring an action in federal court for unfair competition or violation of their state trade secret laws if the theft of the trade secrets was in connection with a commercial activity carried on by the foreign entity in the United States. To use the Israeli officers at Recon Optical as an example again, they were indeed involved in a commercial activity as they were working at the plant to produce aerial reconnaissance cameras; and the activity was being carried out in the United States.

---

[105] 28 U.S.C. § 1603.

[106] 28 U.S.C. § 1605(a)(2).

More problematic, however, is whether a court would rule that the commercial activity was carried on "by" the foreign state. In the present example that is questionable because the commercial activity was primarily carried on by a U.S. firm, Recon Optical. The same holds true with "Lothario," for the German BND agent himself was involved in no commercial activity. Thus, 1605(a)(2) is limited as to the instances of economic espionage to which it might apply. Therefore, other exceptions under the FSIA will need to be deemed applicable for this legislation to be used effectively in many of the types of economic espionage incidents that occur within U.S. boundaries.

A second possible avenue for suing foreign nations for trade secret theft is via the exception to foreign immunity in 1605 (a)(3), which states:

> in which rights in property taken in violation of international law are in issue and that property or any property exchanged for such property is present in the United States in connection with a commercial activity carried on in the United States by the foreign state; or that property or any property exchanged for such property is owned or operated by an agency or instrumentality of the foreign state and that agency or instrumentality is engaged in a commercial activity in the United States;[107]

A primary obstacle under this exception is whether trade secrets represent rights in property taken in violation of international law. While the argument has been made that espionage may not violate 'international law' as defined by one standard,[108] international law is also determined by an examination of international treaties.[109] And the TRIPS Convention in particular,[110] and the Paris Convention more generally,[111] are international treaties that accord at least some levels of protection to trade secrets. Under these conventions the theft of a trade secret might qualify as property taken in violation of international law.

But a second more formidable obstacle under 1605(a)(3) is that the property must be present in the U.S. in connection with a "commercial activity carried on in the United States by the foreign state."[112] As with 1605(a)(2) the firm seeking to sue the foreign government must prove that the theft occurred in conjunction with a commercial activity "by" the

---

107 28 U.S.C. § 1605(a)(3).

108 Scott, *supra* n. 50. That standard was 'the general principles of law recognized by civilized nations.'

109 Statute of the International Court of Justice, art. 38(1)(a), June 26, 1945, 59 Stat. 1055, 1060 (1954).

110 TRIPS at art. 39, *supra* n. 60.

111 Paris at art. 10bis, *supra* n. 56.

112 28 U.S.C. § 1605(a)(3).

foreign state. While on occasion a foreign government may set up a commercial activity in the U.S. as a vehicle to obtain proprietary information,[113] which would then constitute the activity required by this exception, more typically the theft of trade secrets is accomplished through intelligence agents.[114] Thus, as with 1605(a)(2), the clause in 1605(a)(3) requiring commercial activity by a foreign state will often prove a limitation on U.S. firms seeking to sue foreign governments.

However, another of the FSIA exceptions to foreign sovereign immunity may be useful to American firms in seeking compensation for trade secret theft under a wide range of scenarios. The exception to immunity of 1605(a)(5) states:

> not otherwise encompassed in paragraph (2) above, in which money damages are sought against a foreign state for personal injury or death, or damage to or loss of property, occurring in the United States and caused by the tortious act or omission of that foreign state or of any official or employee of that foreign state while acting within the scope of his office or employment;[115]

In essence, this provision allows for compensation to be sought for damage to or loss of property in the U.S. caused by the tortious act of an employee of a foreign government acting within the scope of his duties. While it is doubtful that Congress had theft of trade secrets in mind when writing this immunity exception, 1605(a)(5) could prove to be the best vehicle for U.S. firms to hold a foreign government accountable for its actions.

Whether the 1605(a)(5) exception could be used depends upon whether trade secrets qualify as property. As early as 1907, the Supreme Court recognized confidential stock exchange quotations to be "property" deserving of protection.[116] A decade later, the Court recognized news transmitted by the International Press as "quasi-property" and noted that it had "all the attributes of property necessary for determining that a misappropriation of it" is unfair competition.[117] Much more recently, a unanimous Court held that the Wall Street Journal's business information, which was intended to be kept confidential, "was its property."[118] Furthermore, trade secrets were specifically recognized by the Supreme Court to be property

---

113 *See* Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 1998. *See also* <http://www.nacic.gov/fy98rpt.html> (visited April 1, 2001).

114 *See id.*

115 28 U.S.C. § 1605(a)(5).

116 *Clarence P. Hunt v. New York Cotton Exchange*, 205 U.S. 322, 333 (1907).

117 *International News Service v. Associated Press*, 248 U.S. 215, 240-42 (1918).

118 *Carpenter v. United States*, 484 U.S. 19, 28, 5 U.S.P.Q. 1059 (1987).

for 'Takings Clause' purposes.[119] Thus, it seems logical that trade secrets would be recognized as "property" for FSIA purposes as well.

But, does the theft of trade secrets represent a "loss or damage" to such property? Intellectual property, which includes trade secrets, often is not so much stolen as it is downloaded or reproduced.[120] In cases of downloading, the information would still reside with the firm, so technically there would be no 'loss' of property for FSIA purposes. However, one could argue that the theft "damaged" the trade secret. The Uniform Trade Secrets Act requires that a trade secret derive independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by . . . persons who can obtain economic value from its disclosure or use.[121] Similarly, the Restatement defines a trade secret as having value because its secrecy gives an economic advantage to its owner.[122] Thus, by definition a trade secret has value because it is secret. It can be argued that the secret is "damaged," for FSIA purposes, by its very disclosure. For once a trade secret is known to others its value to the original owner is diminished, and "loss of value" is a common definition of damage.[123]

Under 1605(a)(5), in order for the firm to argue for compensation resulting from damage to its property by the theft of a trade secret, the damage must have been caused by a tortious act of an employee of a foreign state, where that employee was acting within the scope of his employment.[124] The misappropriation of trade secrets clearly is recognized as a tortious act.[125] Thus, the last element to prove for FSIA jurisdictional purposes is that the tort was committed by an employee of a foreign state within the scope of his employment. If the tortfeasor is an intelligence agent, as was the case with the German Lothario, then he is most certainly an employee of a foreign government. Further, if the agent's business is collecting intelligence, then the misappropriation of the trade secrets occurs within the scope of his employment. Similarly, the Israeli air force officers caught with the trade secrets at Recon Optical indisputably were employees of Israel. Because they had been assigned to work at Recon as part of the

---

119 *See Ruckelshaus v Monsanto Co.*, 467 U.S. 986, 1020 (1984).

120 *See e.g. United States v. Riggs*, 739 F. Supp 414 (1990).

121 UTSA 1(4), *supra* n. 69.

122 Restatement *(Third)* § 39.

123 *See e.g.,* The Random House Dictionary of the English Language defines 'damage' as "injury or harm that reduces value of usefulness." Random House Dictionary of the English Language 504 (Stuart Berg Flexner ed., 2d. ed, Random House 1987).

124 28 U.S.C. § 1605(a)(5).

125 *See* W. Page Keeton, Prosser and Keeton on The Law of Torts 1022 (5th ed., 1984).

contract with that firm for the development of the aerial reconnaissance cameras, those officers were acting within the scope of their employment when the trade secrets were misappropriated. Hence, when the misappropriator of a trade secret can be tied to a foreign government, 1605 (a)(3) of the FSIA likely can be used to obtain jurisdiction in federal court over the nation sponsoring that misappropriator.

Once the offended firm has overcome the high jurisdictional hurdle associated with foreign sovereign immunity then it rather mechanically proceeds under state common law[126] or state statutory law,[127] as outlined earlier in Section A of this Part. Under these state actions, the plaintiff must simply prove that the information was obtained through improper means and that the information was of value as a result of its secrecy. And faced with the embarrassment of being caught, the expense of a trial, and the likelihood of a large damage award by a jury unsympathetic to foreign spies, it is quite possible that a foreign government would move quickly to settle any suit brought in federal court under the FSIA. This might be especially true for U.S. allies, where the embarrassment would be the greatest.

Much of the incentive for combining the FSIA with state law is that the firm may bring the suit on its own, independent of the U.S. Government. Utilizing the FSIA to gain jurisdiction over a foreign nation, in conjunction with the appropriate state law proscribing trade secret theft, is perhaps the best way for a firm to obtain compensation when it has been the victim of economic espionage. Effective use of these laws by companies might also serve to deter the widespread economic espionage that occurs within U.S. borders.

V. CONCLUSION

United States firms are routinely targeted by foreign nations in attempts to obtain trade secrets.[128] This practice has gone on for years, and there appears to be a sense among offending nations that economic espionage is to be viewed as a considerably lesser offense than political espionage.[129] The United States has enacted criminal legislation aimed at punishing offenders,[130] but this legislation provides little consolation to a

---

126 Restatement *(Third)* § 39.

127 USTA, *supra* n. 69; Most states have versions of the USTA, *supra* n. 76.

128 Annual Report 2000, *supra* n. 12.

129 *See e.g. supra* n. 6, 34, 35.

130 18 U.S.C. § 1831-39.

firm that has incurred substantial economic damages from the theft of its trade secrets. Attempts to bring an individual into a state court in a civil action for trade secret theft has the problems of the offender fleeing the country before the theft is discovered, or the lack of 'deep pockets' on the part of any individual offender. However, if the wronged firm has evidence that the offender was an agent or instrumentality of a foreign government, then several exceptions to sovereign immunity allow the foreign country to be haled into federal court by the firm that has been wronged.

The FSIA has been used at least once by a firm to gain jurisdiction over a foreign nation for theft of a trade secret.[131] While jurisdiction was granted in that particular instance, it was granted with strong dissent emanating from the issue of whether the activity was based upon commercial activity carried out in the United States. Thus, how the Supreme Court would view such a suit today is open to question. However, by using 1605(a)(5), with its emphasis on "damage to property," rather than using other FSIA exceptions that look to "commercial activities by a foreign nation," U.S. firms may increase their probability of success in obtaining jurisdiction over foreign nations and in ultimately holding them accountable for their misappropriations of proprietary information.

---

[131] *Gould, Inc. v. Mitsui Mining & Smelting Company*, 947 F.2d 218, 222-23 (6th Cir. 1991).