Minnesota Journal of Law, Science & Technology

Volume 10 | Issue 2 Article 5

2009

# Economic Espionage: A Framework for a Workable Solution

Mark E. A. Danielson

DANIELSON MEA. Economic Espionage: A Framework for a Workable Solution. MINN. J.L. SCI. & TECH. 2009;10(2): 503-548.

# Economic Espionage: A Framework for a Workable Solution

**Mark E.A. Danielson***

## I. INTRODUCTION

Economic espionage is a serious problem. In general terms, it is the act of targeting or acquiring trade secrets from domestic companies or government entities to knowingly benefit a foreign state.[1] It differs from industrial espionage in that the activities are carried out or sponsored by government, as opposed to private, entities. States have shifted their focus from building military security towards achieving economic supremacy.[2] Many states now consider economic espionage a matter of national security.[3] It profits participants[4] and saves the time and financial resources required to develop technologies independently.[5] The effects of the



* Mark Danielson, B. Mgmt (Dalhousie), JD (Bond), LLM (Georgetown). Mark is completing his articles at Pushor Mitchell LLP (Canada).

1. *See* 18 U.S.C. § 1831 (2006).

2. Peter Schweizer, *The Growth of Economic Espionage: America is Target Number One*, 75 FOREIGN AFF. 9, 14 (1996).

3. THE JOURNALISM SCHOOL, COLUMBIA UNIVERSITY, WERT ECONOMIC ESPIONAGE 4 (Nov. 11, 2005), Go to http://www.journalism.columbia.edu/, search "WERT Economic Espionage" and click on the link [hereinafter WERT].

4. *See, e.g.*, Schweizer, *supra* note 2, at 12 ("That so many states practice economic espionage is a testament to how profitable it is believed to be."); *see also* JOHN A. NOLAN, ECONOMIC ESPIONAGE, PROPRIETARY INFORMATION PROTECTION: THE GOVERNMENT IS HERE TO HELP YOU – SERIOUSLY 2 (1997), http://www.hanford.gov/oci/maindocs/ci_r_docs/econesp.pdf ("It doesn't take the President of the World Bank to figure out that if you spend $500,000 bribing a research scientist in the United States to get the trade secret or proprietary information that an American company has spend $750,000,000 developing, the intelligence operation has just netted $700 million.").

5. Karen Sepura, *Economic Espionage: The Front Line of a New World*

practice are felt globally, but it most acutely impacts U.S. businesses, as they have the distinction of being targeted more than those of other states.[6] The fact that the United States spends more money on research and development than any other state,[7] coupled with the open nature of its economy, makes it an attractive target for states seeking low-cost technological upgrades.[8] Further, the proliferation of electronically-stored information has made the stealing of electronic information as easy as the push of a button. Economic espionage diminishes a business's goodwill and reputation while lessening its competitive advantage, core technologies, and profitability.[9] States' attempts to outspend one another to acquire the other's secrets are ultimately wasteful.[10] The problem has reached epic proportions and will not go away on its own.[11]

This article highlights the damaging effects of economic espionage. It illustrates how the United States and the international community have tried to cope through existing legislation and agreements. Ultimately, it demonstrates that the establishment of a convention prohibiting economic espionage—once impossible due to prevailing international attitudes towards competition—is now possible. The article proposes a general

---

*Economic War*, 26 SYRACUSE J. INT'L. L. & COM. 127, 133 (1998).

6. Darren S. Tucker, Comment, *The Federal Government's War on Economic Espionage*, 18 U. PA. J. INT'L ECON. L. 1109, 1114–15 (1997).

7. Catherine Dominguez, *FBI Launches Education Campaign Targeting "Economic Espionage,"* SAN ANTONIO BUS. J., Jan. 18, 2008, *available at* http://sanantonio.bizjournals.com/sanantonio/stories/2008/01/21/story4.html.

8. OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXECUTIVE, ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE 2005, at 12 (2006), *available at* http://www.ncix.gov/publications/reports/fecie_all/FECIE_2005.pdf [hereinafter ONCE REPORT].

9. ASIS INT'L, TRENDS IN PROPRIETARY INFORMATION LOSS 3 (2007), *available at* http://www.asisonline.org/newsroom/surveys/spi2.pdf.

10. Schweizer, *supra* note 2, at 14.

11. Pamela A. MacLean, *Frustrations Abound for Spycatchers*, NAT'L L. J., May 15, 2006, at S1. FBI statements regarding the cost of economic espionage reference the ASIS study. Director Robert Mueller has said "Theft of trade secrets and critical technologies—what we call economic espionage—costs our nation upwards of $250 billion a year." Robert S. Mueller, Director, Fed. Bureau of Investigation, Address at the Detroit Economic Club (Oct. 16, 2003), *available at* http://www.fbi.gov/pressrel/speeches/director101603.htm.

framework for such an agreement and discusses the implementation problems it would encounter.

### A. ECONOMIC COSTS

Quantifying the losses attributed to economic espionage is a difficult task. Thefts often go unreported to federal or state law enforcement agencies. Businesses may be reluctant to step forward and admit being targeted for a myriad of reasons. An admission may signal to investors that a company is unable to protect its valuable proprietary information.[12] Such concerns are valid: studies have indicated that a company's stock tends to decline following an admission it has been struck by economic espionage.[13] An admission may compromise joint ventures or forestall lucrative government contracts.[14] By naming names, a business may prejudice its ability to obtain future contracts in that state.[15] Further, organizations may worry that by coming clean they may reveal vulnerabilities and signal to copycats that they are an easy target.[16]

A recent survey by ASIS International ("ASIS"), the largest global organization of security professionals, highlighted the problem: in many instances, businesses could not or would not, disclose how proprietary information theft occurred, by whom, or the value of the information stolen.[17] Additionally, businesses may operate under the assumption that economic espionage is a low priority on law enforcement agencies' to-do lists.[18] This is not unwarranted given the historic reluctance to prosecute crimes for intellectual property ("IP") theft,[19] coupled with the fact that IP

---

12. Sepura, *supra* note 5, at 137.

13. Chris Carr & Larry Gorman, *The Revictimization of Companies by the Stock Market who Report Trade Secret Theft under the Economic Espionage Act*, 57 BUS. LAW. 25, 30 (2001).

14. Schweizer, *supra* note 2, at 11.

15. INTERAGENCY OPSEC SUPPORT STAFF, IOSS INTELLIGENCE THREAT HANDBOOK: ECONOMIC ESPIONAGE 44 (2004), *available at* http://www.fas.org/irp/threat/handbook/economic.pdf.

16. Sam Vaknin, *The Industrious Spies*, GLOBAL POLITICIAN, June 1, 2006, http://www.globalpolitician.com/articledes.asp?ID=1824&cid=1&sid=27.

17. ASIS INT'L, *supra* note 9, at 11–13.

18. Robert C. Van Arnam, *Business War: Economic Espionage in the United States and the European Union and the Need for Greater Trade Secret Protection*, 27 N.C. J. INT'L L & COM. REG. 95, 99 (2001).

19. Throughout the 1970-80s, computer crimes were reluctantly prosecuted. The crimes' complexity posed a steep learning curve for

theft is often extremely difficult to investigate.[20] Businesses may pursue civil remedies in lieu of criminal action,[21] though doing so becomes prohibitively difficult when the perpetrator is backed by a foreign state.[22]

Up to seventy-five percent of an American business's market value may be attributed to IP assets.[23] These assets rarely undergo formal valuations and are not usually protected at a level that reflects their importance to the business.[24] Significantly, a business may not be able to accurately estimate the damages caused by an intrusion for many months, or even years, down the line.[25] It may not immediately realize its ever-dwindling market share is the direct result of a competitor successfully assimilating stolen information into its product.[26] These factors indicate cost estimations are likely to be underrated.

The attempts to estimate these costs have yielded staggering results. An ASIS survey released in 1998 estimated the cost to U.S. businesses at $250 billion per year.[27] The losses have increased since the survey. Eighty-one percent of respondents to an ASIS survey released in 2007 indicated that the cost impact of proprietary information theft was comparable or higher in 2005

---

prosecutors and made it difficult to persuade juries. Legislative action was not taken until large banks, investment houses, and other organizations began to suffer the effects of such crimes. *See* NOLAN, *supra* note 4, at 1.

20. Van Arnam, *supra* note 18, at 99.

21. *Id.* at 99.

22. Perpetrators of economic espionage may try to claim foreign sovereign immunity in relation to their activities. For a discussion on foreign sovereign immunity in relation to trade secret theft, see Christopher G. Blood, *Holding Foreign Nations Civilly Accountable for their Economic Espionage Practices*, 42 IDEA 227, 241–46 (2002).

23. ASIS INT'L, *supra* note 9, at 1.

24. *Id.*

25. ONCE REPORT, *supra* note 8, at 1 n.3.

26. *Id.*; *see also* ASIS INT'L, *supra* note 9, at 40 (reporting that sixty percent of respondents to the most recent ASIS International survey indicated it would take less than twelve months for a competitor, having acquired stolen information, to assimilate it into a comparable product or service. It is important to note that only 12 of 144 respondents answered with something other than "not available," "not applicable," or "unable to calculate." It is possible the low response rate has to do with the difficulty in detecting economic espionage or a reluctance to admit to being victimized).

27. STEVEN FINK, STICKY FINGERS: MANAGING THE GLOBAL RISK OF ECONOMIC ESPIONAGE 193 (2003).

than in 2004 within their organizations.[28] Furthermore, eighty-eight percent of respondents indicated their information compromise attempts were higher in 2005 than in 2004.[29] While approximately eighty-six percent of the world's IP is generated in the United States, it only recognizes about fifty percent of the profit due to theft.[30]

## B. EFFECTS

The effects of economic espionage are almost wholly negative. Economic espionage erodes the value of a target state's assets.[31] It may disrupt trade between target states and potential buyers.[32] It discourages innovation.[33] It may destroy a business's hard-earned competitive advantage and stifle economic momentum.[34] It may undermine current business plans, ruin profit projections,[35] and "spell the difference between extinction and profitability."[36] Research costs may have to be recouped by charging higher prices to customers.[37] Businesses already undercut by lower overseas production costs may not be viable after factoring in the cost of these thefts. On a larger scale, economic espionage may have the long-term effect of weakening existing military alliances and trade coalitions.[38] Economic espionage has been compared to warfare since both challenge the security and stability of sovereign nations.[39]

---

28. ASIS INT'L, *supra* note 9, at 26.

29. *Id.* at 25.

30. WERT, *supra* note 3, at 2.

31. Susan W. Brenner & Anthony C. Crescenzi, *State-Sponsored Crime: The Futility of the Economic Espionage Act*, 28 HOUS. J. INT'L L. 389, 448–49 (2006).

32. Schweizer, *supra* note 2, at 12.

33. Sepura, *supra* note 5, at 138.

34. ASIS INT'L, *supra* note 9, at 41.

35. *Id.*

36. Vaknin, *supra* note 16.

37. Thierry Olivier Desmet, *The Economic Espionage Act 1996: Are We Finally Starting to Take Corporate Spies Seriously?*, 22 HOUS. J. INT'L L. 93, 95–96 (1999).

38. IOANNIS L. KONSTANTOPOULOS, RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES, MACROECONOMIC ESPIONAGE: INCENTIVES AND DISINCENTIVES 20 (2006) (Greece), go to http://www.isn.ethz.ch/ search "Macroeconomic Espionage: Incentives and Disincentives" and click on the first link (speculating that traditional military alliances such as NATO will be harmed by economic espionage and dependence on trading blocs will increase in the future).

39. Brenner & Crescenzi, *supra* note 31, at 449.

## C. PARTICIPANTS

All states are motivated to spy on their "competition."[40] It would be irresponsible for a state to be unconcerned about its neighbor's activities. However, since the end of the Cold War, traditional spying has become less important as states focus their efforts on building economic, not military, security.[41] As economic security grows more important to national security, the interest in economic espionage becomes more significant.[42] This trend is expected to continue.[43]

Economic espionage is most prevalent in economically competitive countries.[44] Thus, it is generally advanced Western states that bear the burden of economic espionage. As previously noted, the United States is a prime target.[45] The most recent ASIS survey indicates that the top three foreign countries seeking to access U.S. information in 2005 were China, Russia, and India.[46]

This balance is shifting. States previously uninterested in gathering economic information are fixing their sights on the United States. Entities from a record number of countries—108—sought to retrieve sensitive or protected information between October 1, 2004 and September 30, 2005.[47] Seventy percent of information compromises reported by those firms responding to the most recent ASIS survey were intended to benefit foreign individuals, firms, or governments.[48] This figure only includes those incidents in which the recipient could be identified. In many instances, respondents were unable (or unwilling) to identify whether information was intended to benefit U.S. or foreign entities.[49] Often, a conclusive link between a foreign government and the culprit cannot be established.[50] Unsurprisingly, when a

---

40. Van Arnam, *supra* note 18, at 98.
41. Schweizer, *supra* note 2, at 13.
42. Sepura, *supra* note 5, at 127–28.
43. ONCE REPORT, *supra* note 8, at v.
44. *See* Van Arnam, *supra* note 18, at 98.
45. Dominguez, *supra* note 7.
46. ASIS INT'L, *supra* note 9, at 3.
47. ONCE REPORT, *supra* note 8, at iii.
48. ASIS INT'L, *supra* note 9, at 23. Respondents reported that foreign individuals, firms, and governments were the beneficiaries of information compromises in 357 incidents, compared to 155 incidents where the primary beneficiary was a U.S. individual or firm. *Id.*
49. *Id.*
50. ONCE REPORT, *supra* note 8, at ix.

link was established, the perpetrators often had ethnic connections to the non-U.S. country benefiting from the compromise.[51]

Perpetrators are becoming more skilled in disguising their intelligence operations.[52] Traditional espionage efforts are becoming less common as governments have learned to glean intelligence from the private sector.[53] Many governments establish organizations to track the activities of expatriates abroad in order to pump them for information upon their return home,[54] which precludes the monitoring of meetings on American soil by U.S. officials.[55] It is estimated that up to sixty percent of information collected by foreign intelligence agencies occurs on their own soil from foreign companies operating there.[56] Authorities may

---

51. ASIS INT'L, *supra* note 9, at 24.

52. *See* FEDERAL BUREAU OF INVESTIGATION, THE SPYING GAME: TRICKS OF TODAY'S TRADE (2007), http://www.fbi.gov/page2/july07/spying070907.htm. A recent posting on the Federal Bureau of Investigation's website describes common disguises, including:

- Representatives at supposed "research institutes,"
- Visiting business professionals and scientists who want to tour your state-of-the-art plants and operations worldwide (a great place to take pictures and make friends),
- Tourists or visitors on non-immigrant visas,
- Diplomatic officials, the standard cover,
- False front companies, and
- Students and educators.

*Id.*

The posting characterizes economic espionage as a state's long-term commitment:

- "You hire a foreign-born engineer who has been educated in this country. Over a 10-15 year period, she rises to mid-level management. Then, she returns to her home country—where she gets paid by that government to set up a business that competes with yours."
- "A series of university students and professors from overseas take jobs in research labs on campus and get involved in related military projects. Individually, they learn only bits and pieces. But collectively, when they pass that information back to their home country, it paints a telling picture of our country's defense initiatives."

*Id.*

53. ONCE REPORT, *supra* note 8, at 6.

54. *Id.* at iv.

55. *Id.*

56. Levon Sevunts, *A Spy in the Office*, INFOSEC NEWS, Aug. 2, 2000, http://www.infosecnews.org/hypermail/0008/2532.html.

attempt to deal for information, or they may extract it through coercion in countries in which the private sector remains influenced by security services, such as Russia or China.[57] The proliferation of foreign "front companies" in the United States is a concern.[58] The Federal Bureau of Investigation ("FBI") estimated in 2005 there were over 3000 such companies located in the United States designed to serve Chinese government interests.[59] Front companies are difficult to recognize. The number of valid commercial activities in which they participate makes it difficult to distinguish between legitimate and illegitimate transactions.[60]

The United States has been reluctant to publicly identify governments carrying out economic espionage campaigns, especially when the governments involved are considered allies.[61] The FBI, for instance, does not officially identify those states engaging in economic espionage against the United States.[62] This reluctance reflects the fact that relations between governments take place on a number of levels concurrently.[63] Publicly accusing

---

57. ONCE REPORT, *supra* note 8, at 6. An example of a government dealing for information allegedly occurred when an official French government program incentivized economic espionage by allowing its citizens to avoid mandatory military service by agreeing to work at U.S. high-tech companies, presumably to obtain trade secrets. *See* Craig L. Uhrich, *The Economic Espionage Act—Reverse Engineering and the Intellectual Property Public Policy*, 7 MICH. TELECOMM. TECH. L. REV. 147, 148 (2001).

An example of a government extracting information by coercion recently came to light at the Houston Offices of Shell Oil. A group of Chinese workers employed by Shell was caught stealing information to help China build oil infrastructure in Africa. China recently concluded agreements in the Darfur region of Sudan to develop such infrastructure. The perpetrators allege they have been threatened by the Chinese government that if they failed to obtain the information "things might not go well" for their relatives in China. *See* Kelly O'Connell, *Chinese Web Spies Steal Rolls Royce and Shell Oil Secrets*, INTERNET BUS. L. SERVICES, Dec. 10, 2007, http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1927.

58. ASIS INT'L, *supra* note 9, at 19–20.

59. *Id.* at 20.

60. ONCE REPORT, *supra* note 8, at 7.

61. Brenner & Crescenzi, *supra* note 31, at 399.

62. Hedieh Nasheri & Timothy J. O'Hearn, *High-tech Crimes and the American Economic Machine*, 13 INT'L REV. L., COMPUTERS & TECH., 7, 12 (1999).

63. Brenner & Crescenzi, *supra* note 31, at 399.

an ally of theft may heighten tensions between countries.[64]

## D. U.S. PARTICIPATION

The United States has steadfastly denied engaging in economic espionage; it claims to react to instances of economic espionage in a purely defensive fashion.[65] It is unlikely that the United States is merely a victim of economic espionage, as it, too, has been accused of such behavior. American officials have been expelled from both France and Germany following accusations of economic espionage.[66] Recently, it has been accused of using its "Echelon" surveillance system to monitor the conversations of European Union ("EU") companies[67] and also to eavesdrop on conversations between the Indonesian government and Japanese manufacturers in order to get a piece of a $200 million satellite contract.[68] EU nations have expressed concern that a U.S. program instituted post-September 11, 2001, allowing the United States to inspect international bank transfers taking place in the EU, is being used for economic espionage.[69] The growing size of Central Intelligence Agency ("CIA") stations located within the EU is a source of anxiety for some.[70]

These quarrels have not resulted in a lasting political rift for the United States.[71] However, feelings of suspicion and contempt for such alleged dishonesty doubtlessly linger.[72] It remains to be seen whether a "dual-track" approach[73]—the overlooking of

---

64. *Id.*

65. *See* Duncan L. Clarke & Robert Johnston, *Economic Espionage and Interallied Strategic Cooperation*, 40 THUNDERBIRD INT'L BUS. REV. 413, 423 (1998) (quoting former Director of Central Intelligence James Woolsey stating the CIA "is not in the business of . . . spying on foreign corporations for the benefit of domestic businesses").

66. Alan Cowell, *Bonn Said to Expel U.S. Envoy Accused of Economic Spying*, N.Y. TIMES, March 10, 1997, at A6.

67. Peter Goodspeed, *The New Space Invaders: Spies in the Sky,* NAT'L POST (Canada), Feb. 19, 2000, at B.1.

68. Vaknin, *supra* note 16.

69. Resolution on the Interception of Bank Transfer Data from the SWIFT System by the US Secret Services, EUR. PARL. DOC. (C 303) (2006). Such transfers may potentially indicate prices, supply, and consumer information—a concern to EU businesses.

70. Clarke & Johnston, *supra* note 65, at 424.

71. *Id.* at 428.

72. Cowell, *supra* note 66. The article quotes an unidentified German intelligence official lamenting that the U.S. looks upon Berlin as "their backyard where they can do anything they like." *Id.*

73. Clarke & Johnston, *supra* note 65, at 420.

economic espionage while remaining vigilant against military espionage—will be able to withstand public scrutiny.[74] United States participation in economic espionage risks retaliation from targeted countries, decreased credibility when promoting international agreements, and diminished respect for its IP.[75] Most U.S. officials recognize these costs outweigh the benefits of the activities.[76] To its credit, the United States does not appear to pass on information gathered from its activities to domestic businesses.[77]

### E. INTERNATIONAL ATTITUDES

Cases of economic espionage rarely make the news. Amongst the general public there exists the perception that economic espionage is not a pressing problem, but rather an inevitable consequence of globalization.[78] Internationally, there is a conspicuous lack of concern toward the practice.[79] No

---

74. *Id.* at 424.

75. Van Arnam, *supra* note 18, at 132.

76. Clarke & Johnston, *supra* note 65, at 423.

77. Schweizer, *supra* note 2, at 11. The author remarks the United States' alleged activities constitute economic espionage "at its most benign level" and asserts it is the passing on of information to domestic companies that harms the global marketplace. *Id.; see* Brandon J. Witkow, Comment, *A New "Spook Immunity": How the CIA and American Business are Shielded from Liability for the Misappropriation of Trade Secrets,* 14 EMORY INT'L L. REV. 451, 460 (2000) ("[T]here is a fine line between the collection, through open sources of information, of economic trends for policy-making purposes and the covert theft of proprietary business information for dissemination to competing American corporations."). Even those who believe U.S. law permits the collection of economic intelligence concede the passing on of such intelligence to domestic businesses is likely impermissible. Witkow, *supra* 77*,* at 482.

78. For example, in response to a recent blog posting describing how foreign citizens infiltrate U.S. companies to acquire information useful to their competition abroad, an individual remarked in response, "[s]ounds like global free enterprise to me." Posting of Luke O'Brien to Wired Blog network, http://blog.wired.com/27bstroke6/2007/07/fbi-warns-of-sp.html#previouspost (July 9, 2007, 4:00:50 PM).

79. Blood, *supra* note 22, at 233 ("[T]here appears to be little international will to recognize and address the problem of trade secret theft."). Former Director of Central Intelligence Dr. John M. Deutch believes the adverse effects of economic espionage to U.S. companies are far less significant than those resulting from violations of the Foreign Corrupt Practices Act. *Q&A Following Worldwide Threat Assessment Brief, Before the S. Comm.on Government Affairs*, 104th Cong. 26 (1996) (statement of John M. Deutch, Director of Central Intelligence), *available*

international agreement expressly prohibits it. This may be due to the fact that all states have an interest in conducting such activities.[80] It is generally accepted that states spy on one another to some degree.[81] In fact, many governments targeting the United States remain political or military allies.[82] These states do not see a "contradiction in maintaining a military alliance with the United States while at the same time using their intelligence services to target U.S. technologies."[83] In a 1991 interview, Pierre Marion, former head of the French spy agency Direction Générale de la Sécurité Extérieure ("DGSE"), acknowledged this dichotomy, stating that "[i]t would not be normal that we do spy on the (United) States in political matters; we are really allied. But in the economic competition, in the technological competition, we are competitors; we are not allied."[84]

It is disputed whether economic espionage violates international law at all.[85] An accepted way of determining the international legality of an act is to examine the general and consistent practice of states.[86] Those actions consistently

---

*at* https://www.cia.gov/news-information/speeches-testimony/1996/q-a-following-worldwide-threat-assessment-brief.html. The effects of economic espionage and FCPA violations are strikingly similar: both distort trade, undermine economic development, misdirect resources from more valuable uses, and confer benefits on undeserving parties. OCED Fighting, *infra* note 213.

80. Commander Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F. L. REV. 217, 220 (1999).

81. Brenner & Crescenzi, *supra* note 31, at 400.

82. H.R. REP. NO. 104-788, at 5 (1996), *as reprinted in* 1996 U.S.C.C.A.N. 4021, 4024. "Unlike most espionage directed at military targets, economic espionage is as likely to be carried out by an ally as it is an adversary. The top twelve states placing economic spies in the United States are China, Canada, France, India, Japan, Germany, South Korea, Russia, Tawain, Great Britain, Israel, and Mexico." GLENN P. HASTEDT, ESPIONAGE: A REFERENCE HANDBOOK 60 (2003). A brazen example occurred when the French intelligence agency, DGSE, placed audio equipment in the business class of Air France flights between Paris and New York to eavesdrop on travelling U.S. businessmen. Jeff Augustini, Note, *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, 479 (1995).

83. H.R. REP. NO. 104-788 (1996), at 5, *reprinted in* 1996 U.S.C.C.A.N. 4021, 4024.

84. Merrill E. Whitney & James D. Gaisford, *Economic Espionage as Strategic Trade Policy*, 29 CAN. J. ECON. 627, 627 (1996).

85. Blood, *supra* note 22, at 233.

86. *See, e.g.*, RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 102(2)

practiced may become customary international law, either through explicit or tacit approval. By this measure, economic espionage may be tolerable under international law because many countries consistently practice it.[87] Others resist the classification of spying as a permissible activity under international law. Instead, it is alleged that spying is a "consistently practiced illegal activity."[88]

The domestic laws of many states, including the United States, do not prohibit the intrusion into foreign territories for the purpose of collecting economic intelligence.[89] U.S. law may in fact affirmatively support such activity.[90] Therefore, any inclination to adopt a "holier than thou" attitude towards another state's economic espionage practices may be perceived as hypocritical.[91] The "dual-track" notion helps explain why the United States has been reluctant to publicly accuse some of its traditional allies of information theft.

Economic espionage is perceived by offending states as a lesser offense than political espionage.[92] Many states consider the practice vital to their continued stability and success—to these states, economic spying is a matter of national security.[93] Further, the business ethics of developing states are often fundamentally different than those in the Western world. Western business ethics have formed primarily in response to legal considerations.[94] For instance, U.S. business ethics have been shaped by legislation such as the Foreign Corrupt Practices Act and the Federal Sentencing Guidelines.[95] Alternatively, Chinese business ethics

---

(1987).

87. Blood, *supra* note 22, at 235.

88. Scott, *supra* note 80, at 222.

89. Blood, *supra* note 22, at 233.

90. Scott, *supra* note 80, at 217. The question of whether the National Security Act of 1947 authorizes U.S. intelligence agencies to conduct economic espionage, to a limited extent, has been answered in the affirmative by at least one commentator. Witkow, *supra* note 77, at 459–60.

91. Brenner & Crescenzi, *supra* note 31, at 400.

92. Blood, *supra* note 22, at 246.

93. WERT, *supra* note 3, at 4.

94. Kristen Day, *Chinese Perceptions of Business Ethics*, INTERNATIONAL BUSINESS ETHICS INSTITUTE, http://www.business-ethics.org/iberpubback.asp (last visited Oct. 20, 2008) (link no longer functioning).

95. *Id.*

are rooted in a Confucian heritage.[96] Personal relationships, loyalty, and trust are often afforded greater significance than legal considerations.[97] The mind-set of developing states may be that ethics are a subordinate concern that should not be addressed until productive forces are maximized.[98] Finally, the significance of IP protection is not a universal value. Many states have been historically reluctant to protect IP and remain so.[99] For example, the inclusion of trade secrets in the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS") was staunchly opposed by developing states and was viewed as a concession to Western business interests.[100] States with minimal respect for IP impose their values on the developed world through the theft of such materials.

## II. EXISTING LEGISLATION AND AGREEMENTS TARGETING ECONOMIC ESPIONAGE

### A. THE ECONOMIC ESPIONAGE ACT OF 1996

Recognizing the damage that economic espionage was causing U.S. businesses, Congress passed the Economic Espionage Act, which became effective October 11, 1996.[101] Prior to its creation there was no federal statute that directly dealt with economic espionage.[102]

The Act criminalizes the copying or controlling of trade secrets with the intent to (1) benefit a foreign government, instrumentality, or agent,[103] or (2) with the intent to convert a trade secret for the economic benefit of a person other than the

---

96. *Id.*
97. *Id.*
98. *Id.*
99. Sepura, *supra* note 5, at 141.
100. Robin J. Effron, Note, *Secrets and Spies: Extraterritorial Application of the Economic Espionage Act and the TRIPS Agreement*, 78 N.Y.U. L. REV. 1475, 1511 (2003).
101. 18 U.S.C. §§ 1831-1839 (2000). American business lobbied vigorously for the creation of the Economic Espionage Act. IBM spent almost $2.7 million in the first six months of 1996 on such lobbying efforts. NOLAN, *supra* note 4, at 1–2.
102. Prior to the enactment of the Economic Espionage Act, the government principally relied upon mail fraud or fraud by wire statutes. The usefulness of these statutes was limited. *See* H.R. REP. NO. 104-788, at 6 (1996), *as reprinted in* 1996 U.S.C.C.A.N. 4021, 4025. The Act is codified at 18 U.S.C. §§ 1831–1839.
103. 18 U.S.C. § 1831.

DANIELSON MEA. Economic Espionage: A Framework for a Workable Solution. MINN. J.L. SCI. & TECH. 2009;10(2): 503-548.



rightful owner.[104] The first section, § 1831, prohibits economic espionage, while the second, § 1832, prohibits industrial espionage.[105] A "trade secret" is generally defined as business information which the owner has taken "reasonable measures" to keep secret and is not "generally known" or "readily ascertainable" to the general public through proper means.[106] Individuals found in violation of § 1831 are subject to maximum penalties of fifteen years in prison and fines up to $500,000.[107] Any organization that violates § 1831 is subject to a maximum fine of $10,000,000.[108] Further, the Act prescribes mandatory forfeiture of the fruits of the offense[109] and any property used to facilitate the offense[110] to the U.S. Government. The Act applies to conduct occurring outside the United States, but only in limited circumstances. The offender must be a citizen of the United States or an organization organized under U.S. laws, or an act in furtherance of the offense must be committed in the United States.[111]

Complaints that the Act's inherent limitations decrease its effectiveness have arisen.[112] Its language has been criticized as vague and difficult to interpret.[113] While the Act authorizes the U.S. Attorney General to obtain appropriate injunctive relief for

---

104. 18 U.S.C. § 1832.

105. The difference between "economic espionage" and "industrial espionage" turns on the lack of state involvement in industrial espionage activities. Industrial espionage typically takes place between private, non-government competitors looking to gain competitive advantage in the marketplace.

106. 18 U.S.C. § 1839(3)(A)-(B).

107. 18 U.S.C. § 1831(a).

108. 18 U.S.C. § 1831(b).

109. 18 U.S.C. § 1834(a)(1).

110. 18 U.S.C. § 1834(a)(2).

111. 18 U.S.C. § 1837(1)-(2).

112. *See, e.g.*, Sepura, *supra* note 5, at 140.

113. Van Arnam, *supra* note 18, at 116. See also Clarke & Johnston, *supra* note 65, at 428, where they highlight the following issue:

> [T]he statute defines trade secrets as information the "owner" has taken "reasonable measures" to keep secret. Who is the owner in a joint venture with a foreign partner? What constitutes reasonable measures to maintain secure facilities during site visits by foreign visitors? American companies must also determine whether their foreign national employees can be classified as "foreign agents" in the employ of a "foreign instrumentality", and, as such, whether they should handle trade secrets.

any violation of the Section,[114] it does not prescribe a private right of action for either damages or injunctive relief.[115] In 2002 the Attorney General elected to renew a requirement obligating prosecutors to seek the approval of the Attorney General before commencing a prosecution under § 1831.[116] Accordingly, "only the most egregious, clear-cut, or high-profile instances" are prosecuted.[117] The manner with which FBI and federal prosecutors have handled businesses' trade secrets has been concerning.[118] Businesses are reluctant to divulge trade secrets in court while prosecuting alleged offenders.[119] Prosecution may be counterproductive if it requires disclosure of the information sought.[120] Few cases involving economic espionage have been brought to trial, representing only a fraction of the many thought to exist.[121] Frequently, it is difficult to demonstrate a connection

---

114. 18 U.S.C. § 1836(a).

115. *See* Boyd v. University of Illinois, No. 96-9327, 1999 U.S. Dist. LEXIS 15438, at *11 (S.D.N.Y. Sept. 30, 1999) (holding the EEA affords no standing to private citizens); Brown v. Citicorp, No. 97-6337, 1998 U.S. Dist. LEXIS 9273, at *9 n.3 (E.D. Ill. June 17, 1998) (holding the EEA does not allow civil actions to be brought by private citizens).

116. Memorandum from the Attorney General on Renewal of Approval Requirement Under the Economic Espionage Act of 1996 (Mar. 1, 2002), http://www.usdoj.gov/criminal/cybercrime/eea1996.pdf.

117. A. HUGH SCOTT, COMPUTER AND INTELLECTUAL PROPERTY CRIME 212 (2001); *see also* Randall W. Schwartz, Comment, *Are Corporate Information Assets, in the Midst of Dynamic Technological and Infrastructural Advances, Best Secured by Legal or Self-Help Remedies?*, 26 HOUS. J. INT'L L. 163, 183 (2003).

118. *See generally* MacLean, *supra* note 11.

119. Van Arnam, *supra* note 18, at 115; *see also* MacLean, *supra* note 11, (quoting Steven Fink of Lexicon Communications Corp., that companies "feel they are more at risk for getting trade secrets exposed by coming forward than just sweeping it under the rug").

120. Gary E. Weiss & K. Alexandra McClure, *Trade Secret Prosecution Risks Further Losses of IP*, NAT'L L.J., June 21, 1999, at C6. The article describes methods which federal prosecutors use to ease business's concerns about trade secret disclosure during trial. Methods include the use of protective orders during pre-trial proceedings, seeking temporary courtroom closures, placing documents under seal at the conclusion of trial, or prohibiting jurors from seeing certain exhibits or requiring them to not to disclose information learned during the trial. The article notes that obtaining these orders can be difficult in a criminal trial due to the defendant's Fifth Amendment right to due process of law. *Id.*

121. Sepura, *supra* note 5, at 139–40. As of the time of writing, only three cases prosecuted have alleged economic espionage under § 1831 of the Act. *See* Press Release, Department of Justice, Chinese National Sentenced for Committing Economic Espionage with the Intent to Benefit China Navy Research Center (June 18, 2008),

between the perpetrator and the state suspected of directing the individual's activities.[122] Even when a connection is established, states have been reluctant to extradite citizens accused of economic espionage to face prosecution.[123] Because the Act does not prescribe any sanctions against a government found to have directed the activities, there is little reason to comply with an extradition request. Further, the Act is criticized for being ineffective against those sheltered by diplomatic immunity.[124] All things considered, while the Act may be useful to deter some forms of espionage, its value as a deterrent to state-sponsored espionage is limited.[125]

### B. PARIS CONVENTION FOR THE PROTECTION OF INDUSTRIAL PROPERTY

The Paris Convention[126] (the "Convention") was the first

---

http://www.usdoj.gov/criminal/cybercrime/mengSent.pdf.

122. MacLean, *supra* note 11.

123. Brenner & Crescenzi, *supra* note 31, at 438; *see, e.g.,*

Press Release, Department of Justice, First Foreign Economic Espionage Indictment; Defendants Steal Trade Secrets from Cleveland Clinic Foundation (May 8, 2001), http://www.usdoj.gov/criminal/cybercrime/Okamoto_SerizawaIndict.htm .

Okamato was charged under § 1831 of the Economic Espionage Act for the theft of several hundred vials containing DNA and cell reagents from a U.S. research laboratory, Cleveland Clinic Foundation, where he was employed. Okamoto was simultaneously in the employ of a Japanese research institute, RIKEN. A Tokyo High Court refused extradition, concluding there was no conclusive evidence he had violated the Economic Espionage Act. *Court rejects U.S. request for extradition in industrial spy case, Okamoto's genetic materials didn't benefit Riken: judge,* JAPAN TIMES ONLINE, Mar. 30, 2004, http://search.japantimes.co.jp/cgi-bin/nn20040330a1.html.

124. Schwartz, *supra* note 117, at 183. Those with diplomatic status are often involved in the collection of economic information:

> An espionage relationship can start as simple friendship with someone who is actually an intelligence officer for an embassy whose goal is to recruit government or corporate insider(s) with access, knowledge and willingness to give information. The intelligence officer may cultivate the person for years, develop a relationship, start by asking for innocent information, e.g. an annual report, get to know the person's motivations and use them to get more information[.]

WERT, *supra* note 3, at 3.

125. Clarke & Johnston, *supra* note 65, at 429.

126. Paris Convention for the Protection of Industrial Property, Mar. 20, 1883, 21 U.S.T. 1583, 828 U.N.T.S 305 [hereinafter Paris Convention].

international agreement to protect IP.[127] It specifically focuses on industrial property.[128] The Convention requires that signatories provide the same IP rights to foreign nationals as those provided to their own citizens.[129] It was designed with flexibility in mind—signatories are afforded a level of discretion about how they must implement the Convention into their domestic law.[130] This flexibility has been criticized for "perpetuating weak national laws."[131] Further, economic espionage is not specifically addressed by the Convention. Article 10$^{bis}$ states "[a]ny act of competition contrary to honest practices in industrial or commercial matters constitutes an act of unfair competition."[132] Regrettably, the Convention does not clarify whether proprietary information theft would contravene this provision. The Convention is now over 100 years old and this provision has not proven useful in limiting economic espionage.

### C. AGREEMENT ON TRADE-RELATED ASPECTS OF INTELLECTUAL PROPERTY RIGHTS (TRIPS)

TRIPS establishes comprehensive minimum standards for the protection of IP.[133] It is administered by the World Trade Organization ("WTO") and was adopted during the Uruguay Round of the General Agreement on Tariffs and Trade ("GATT") in 1994. Article 39 grants perpetual trade secret protection, provided the secret is not "generally known or readily accessible" to the general public,[134] the secret has "commercial value because it is a secret,"[135] and the person controlling the secret has taken reasonable steps to prevent its disclosure.[136] Article 39(1) requires signatories to protect confidential information submitted to governments or governmental agencies.[137] This prevents foreign states from examining government records in the hope of finding

---

127. Van Arnam, *supra* note 18, at 118.
128. Paris Convention, *supra* note 126, art. 1.
129. *Id.* at art. 2.
130. Van Arnam, *supra* note 18, at 118.
131. Schwartz, *supra* note 117, at 184.
132. Paris Convention, *supra* note 126, art. 10$^{bis}$.
133. Agreement on Trade-Related Aspects of Intellectual Property Rights, art. 1(1), Dec. 15, 1993, 33 I.L.M 81 [hereinafter TRIPS].
134. TRIPS, *supra* note 133, art. 39(2).
135. *Id.*
136. *Id.*
137. TRIPS, *supra* note 133, art. 39(1).

useful information.[138]

TRIPS does not specifically address economic espionage. The fact that proprietary information theft is not among its enumerated activities "contrary to honest commercial practices" may imply trade secret protection is an ancillary concern in TRIPS' overall IP protection scheme.[139] Further, Article 8(1) of the Agreement provides a broad exception that allows governments to adopt contrary national laws "to promote the public interest in sectors of vital importance to their socio-economic and technological development."[140] This permits states to avoid prohibitions against economic espionage that are not forbidden by the agreement in specific terms.[141]

## D. NORTH AMERICAN FREE TRADE AGREEMENT (NAFTA)

The North American Free Trade Agreement ("NAFTA") operates between the United States, Canada, and Mexico[142] and entered into effect on January 1, 1994.[143] The treaty is the first international agreement to provide explicit protection for trade secrets.[144] The IP protections afforded under NAFTA generally reflect those in TRIPS, except that NAFTA defines "commercial value" in a manner protecting information with future or potential commercial value in addition to information with existing value. [145] Under NAFTA, a misappropriation of proprietary information is not actionable unless the acquiring party knew, or was grossly negligent in failing to know, its actions were illegal.[146] This is a higher standard than is required under U.S. tort law, which only requires one to prove an infringer's actual or constructive knowledge.[147] While NAFTA remains an important benchmark in international IP protection, it is operative, obviously, only between

---

138. HEDIEH NASHERI, ECONOMIC ESPIONAGE AND INDUSTRIAL SPYING 127 (2005). Although the specific reference is to NAFTA, the same logic applies to TRIPS.

139. Blood, *supra* note 22, at 235.

140. TRIPS, *supra* note 133, art. 8(1).

141. Van Arnam, *supra* note 18, at 120.

142. North American Free Trade Agreement, U.S.-Can.-Mex., Dec. 17, 1992, 32 I.L.M. 612 [hereinafter NAFTA].

143. NASHERI, *supra* note 138, at 127.

144. *Id.*

145. *See* NAFTA, *supra* note 142, art.1711.

146. NASHERI, *supra* note 138, at 127.

147. Van Arnam, *supra* note 18, at 121.

its signatories. Further, concerns have been raised about Mexico's ability to adequately fund and prosecute IP violations.[148]

### E. U.N. RESOLUTIONS 1236 AND 2131

There are two U.N. resolutions that may indirectly address economic espionage. Resolution 1236, "Peaceful and neighbourly relations among States," calls upon states to develop friendly and cooperative relations and mutually respect one another's sovereignty.[149] Resolution 2131, "Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty," states "[n]o State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State."[150] Further, it condemns the "interference . . . against the personality of the State or against its political, economic and cultural elements."[151]

On the surface, it would appear that both of these resolutions could be construed to prohibit economic espionage. However, resolutions of this kind are persuasive—not binding—resources that tend to be ignored by states.[152] They are not a manageable standard against which acceptable or unacceptable intelligence practices may be measured.[153] Finally, a number of states feel that Resolution 2131 conveys a political, rather than legal, view.[154] Consequently, general political pressure may be the only recourse in terms of enforcement.[155]

### F. OECD ANTI-BRIBERY CONVENTION

Bribing government officials or employees is a common way to

---

148. Neil Jetter, Comment, *NAFTA: The Best Friend of an Intellectual Property Right Holder Can Become Better*, 9 FLA. J. INT'L L. 331, 339–40 (1994).

149. Peaceful and neighbourly relations among States, G.A. Res. 1236 (XII) U.N. Doc. A/RES/12/1236 (Dec. 14, 1957).

150. Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, G.A. Res. 2131 (XX) Declaration 1, U.N. Doc. A/RES/20/2131 (21 Dec. 1965).

151. *Id.*

152. NASHERI, *supra* note 138, at 127–28.

153. Sepura, *supra* note 5, at 145.

154. *Id.*

155. NASHERI, *supra* note 138, at 177.

conduct economic espionage.[156] The OECD Convention on Combating Bribery of Foreign Public Officials (the "OECD Convention"),[157] effective since 1999,[158] has served as a minor setback for those seeking to engage in economic espionage. First, many instances of economic espionage do not involve bribery. Second, the OECD Convention only prohibits the bribery of *government* officials[159]—in many instances, bribes may be paid to individuals with no government affiliation. Finally, the OECD Convention has been ratified by only thirty-seven countries.[160] In many states there remain no laws prohibiting the bribery of foreign government officials.[161]

## III. PROPOSED METHODS OF TARGETING ECONOMIC ESPIONAGE

### A. IMPROVING CORPORATE SECURITY

Encouraging businesses to enhance corporate security targets the "supply side" of economic espionage.[162] Businesses are expected to protect their valuable assets to the utmost degree. Standard measures include the use of nondisclosure agreements, employee education and training, restrictive access controls, computer security, document creation/retention/destruction policies, and explicit markings of confidentiality on critical documents.[163] Businesses are encouraged to develop their

156. *Id.* at 128.

157. Organisation for Economic Co-Operation and Development, OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, Dec. 17, 1997, http://www.oecd.org/dataoecd/4/18/38028044.pdf.

158. Organisation for Economic Co-Operation and Development, OECD Anti-Bribery Convention: Entry into Force of the Convention, http://www.oecd.org/document/12/0,3343,en_2649_34859_2057484_1_1_1_1,00.html (last visited Mar. 18, 2009).

159. OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, *supra* note 157, art. 3(1).

160. Organisation for Economic Co-Operation and Development, *supra* note 158.

161. A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 620 (2007) (noting that many other states do not have statutes like the Foreign Corrupts Practices Act).

162. Marc A. Moyer, Comment, *Section 301 of the Omnibus Trade and Competitiveness Act of 1988: A Formidable Weapon in the War Against Economic Espionage*, 15 NW. J. INT'L L. & BUS. 178, 179 (1994).

163. DAVE DRAB, XEROX CORP., PROTECTION UNDER THE LAW:

investigative competencies and direct resources toward "identifying and mitigating" insider threats, such as dishonest employees.[164] Developing these skills is costly and the effects are frequently "messy."[165] Businesses may attempt to moderate their exposure to risk through their contracts entered into with other entities.[166] When working in other countries, a business should try to align its economic interests with those with whom they work so that information theft is equally damaging to each party.[167] However, these strategies are almost futile against state-sponsored economic espionage. No business has the resources to compete with a state determined to acquire its secrets.[168]

### B. COUNTER-ESPIONAGE

Some consider retaliation in kind the most appropriate response to economic espionage.[169] Former CIA Director under President Carter, Stansfield Turner, proposed that the United States imitate other states, such as France,[170] by establishing an offensive economic espionage program.[171] Advocates reason a tit-for-tat response is appropriate and may in fact be mutually productive.[172] They indicate that foreigners already spy on U.S. businesses and the only real concern is the risk of further retaliation by "spying even more."[173] Ultimately, these proponents

---

UNDERSTANDING THE ECONOMIC ESPIONAGE ACT OF 1996 at 8 (2003), http://www.xerox.com/downloads/wpaper/x/xgs_white_paper_drab.pdf.

164. ASIS INT'L, *supra* note 9, at 13.

165. WERT, *supra* note 3, at 2.

166. Problems typically arise through sub-contracting or outsourcing arrangements. Exposure to critical technologies should be minimized in these instances. *See* ASIS INT'L, *supra* note 9, at 33.

167. WERT, *supra* note 3, at 4.

168. 142 CONG. REC. S12, 211 (1996) (statement of Sen. Kohl).

169. Schweizer, *supra* note 2, at 14.

170. France developed its *Ecole de Guerre Economique* (EGE)—the "School of Economic Warfare"—in 1996. Allegedly, EGE "trains students to target U.S. technology and information." EGE's founder insists the school teaches methods of collecting economic intelligence which do not include the sort of espionage engaged in by the French DGSE. Communication Security Inc., Tilting the Playing Field: Economic Espionage Hasn't Gone Away Since 9/11, at 4 (Jan. 28, 2005), http://www.bugsweep.com/articles/jinsa-espionage.html.

171. Augustini, *supra* note 82, at 484.

172. *Id.* at 490 ("[F]oreign companies should be as vulnerable to penetration by U.S. intelligence as U.S. companies currently are to foreign intelligence. Mutual mistrust in this sense might be productive for all involved.").

173. *Id.* at 489–90.

believe the fear of reprisals in the form of U.S. spying will "level the playing field" for U.S. businesses more than legislation ever could.[174]

These notions have not had the requisite support from either corporate America or the intelligence community to come to fruition.[175] Former CIA Director Woolsey's predecessor, Robert M. Gates, referred to the plan as a "moral and legal swamp."[176] Opponents are concerned that victimized states will retaliate against U.S. businesses.[177] Such activities may damage "special relationships" with allies and harm valuable business associations.[178] There are difficulties in determining which companies are "domestic" and "foreign" in our increasingly interconnected world.[179] The arms-length relationship between firms and government in some countries, including the United States, may pose difficulties.[180] Once gathered, the allocation of information presents a problem—how is it to be distributed amongst competitors?[181] Who gets to "claim the prize"?[182] Such arrangements could cause relations between U.S. businesses to deteriorate to a point where fewer joint ventures are undertaken, ultimately decreasing U.S. competitiveness worldwide.[183] The biggest hurdle to such a plan may be the U.S. business ethic—Americans hold deep-seated moral views on how business is to be conducted.[184] Theft and deception likely conflict with these views. Ultimately, an offensive economic espionage plan would damage the credibility of the anti-economic espionage measures already in place and mark a reversal of U.S. policies up to this point in time.[185]

---

174. *Id.* at 491.
175. Schweizer, *supra* note 2, at 14.
176. William T. Warner, *Economic Espionage: A Bad Idea*, NAT'L L.J., Apr. 12, 1993, at 13.
177. Augustini, *supra* note 82, at 489.
178. *Id.*
179. Warner, *supra* note 176, at 13.
180. Whitney & Gaisford, *supra* note 84, at 628.
181. Warner, *supra* note 176, at 13.
182. *Id.*
183. Witkow, *supra* note 77, at 466–67.
184. Augustini, *supra* note 82, at 488.
185. Warner, *supra* note 176, at 13.

### C. UNILATERAL SANCTIONS

Unilateral sanctions have been proposed to address economic espionage.[186] Unilateral sanctions are most effective when imposed by a powerful state, such as the United States.[187] Powerful states usually possess the resources or other advantages which permit them to mitigate the costs of imposing sanctions and overcome collective action problems.[188] However, unilateral sanctions are often difficult to impose, even for the most powerful states.[189] As previously noted, relations between states may occur on different levels simultaneously,[190] making the issuance of such sanctions implausible due to geostrategic or political factors.[191] When imposed against international opposition, sanctions may damage important bilateral relationships and have the ironic effect of boosting the targeted state's international standing.[192] The imposition of unilateral sanctions often harms the sanctioning state more than the intended target[193]—punishing U.S. workers, suppliers, and shareholders.[194] The United States dominates few industries in the global market.[195] Targeted states are free to turn to foreign suppliers to replace the goods previously supplied by American companies.[196] The habitual use of unilateral economic sanctions causes U.S. businesses to be viewed as unreliable suppliers and harms long-term commercial

---

186. *See, e.g.*, Moyer, *supra* note 162. But note that the article was written prior to the enactment of the Economic Espionage Act. Further, Moyer merely advocated using Section 301 of the Omnibus Trade and Competitiveness Act of 1988 as an interim measure until more appropriate measures were devised.

187. Laurence R. Helfer, *Exiting Treaties*, 91 VA. L. REV. 1579, 1619 (2005).

188. *Id.*

189. *Id.* at 1621.

190. Brenner & Crescenzi, *supra* note 31, at 399.

191. Helfer, *supra* note 187, at 1620.

192. Adam Smith, *A High Price to Pay: The Costs of the U.S. Economic Sanctions Policy and the Need for Process Oriented Reform*, 4 UCLA J. INT'L L. & FOREIGN AFF. 325, 370 (1999-2000).

193. Daniel T. Griswold, *Going Alone on Economic Sanctions Hurts U.S. More than Foes*, CATO CENTER FOR TRADE POLICY STUDIES, Nov. 27, 2000, http://www.freetrade.org/node/216/print.

194. Harry Wolff, *Unilateral Economic Sanctions: Necessary Foreign Policy Tool or Ineffective Hindrance on American Businesses*?, 6 HOUS. BUS. & TAX L.J. 329, 362 (2006).

195. *Id.* at 361.

196. *Id.*

relations,[197] leading to residual losses from forfeited maintenance and replacement contracts.[198] These factors have caused most researchers to conclude that unilateral sanctions are ill-advised[199] and must satisfy strict conditions if utilized.[200]

### D. BILATERAL AGREEMENTS

Some propose bilateral agreements to address economic espionage.[201] Bilateral agreements are advantageous because they may be negotiated more rapidly than multilateral agreements and greater levels of protection are frequently achieved.[202] However, bilateral negotiations are difficult in the economic espionage context. Approaching states individually may have grave diplomatic consequences. A United States approach to China, for

---

197. Smith, *supra* note 192, at 340. The experiences of Caterpillar Tractor during the U.S. embargo of the Soviet Union illustrates this problem. Caterpillar was once the undisputed industry leader in heavy-construction equipment. In 1982 Caterpillar lost a $90 million pipe-laying contract after the U.S. declared sanctions in response to the Soviet declaration of martial law in Poland. The Soviets came to view Caterpillar as an erratic supplier. Japanese heavy equipment manufacturer Komatsu filled the vacancy left by Caterpillar and was able to "take over a new market without facing competition, and then leverage that monopolistic market to compete more effectively against Caterpillar in other markets." Peter S. Jordan, *Country Sanctions and the International Business Community*, 91 AM. SOC'Y INT'L L. PROC. 333, 338 (1997) (Remarks by R. Rennie Atterbury III); *The Crunch at Caterpillar*, TIME, Jul. 9, 1984, at 64, *available at* http://www.time.com/time/printout/0,8816,950102,00.html.

198. Wolff, *supra* note 194, at 362.

199. *See, e.g.*, Smith, *supra* note 192, at 354; *see also* Jordan, *supra* note 197, at 336 (remarks of Barry E. Carter) ("Cutting off U.S. exports . . . would seem to be the economic sanction of last resort.").

200. Craig Forcese, *Globalizing Decency: Responsible Engagement in an Era of Economic Integration*, 5 YALE HUM. RTS. & DEV. L.J. 1, 19 ("[S]anctions are most likely to be successful where the goal is relatively modest, the target is much smaller than the country applying the sanctions, there is substantial trade between the two nations, the sanctions are imposed rapidly and decisively, and the cost to the sanctioning country is low.").

201. *See, e.g.*, Dave McCurdy, *Glasnost for the CIA*, *in* AMERICAN DEFENSE POLICY 138, 140 (Peter L. Hays et al. eds., 1997); *see also* Melvin A. Goodman, *The Market for Spies*, ISSUES SCI. & TECH., Winter 1996–1997, at 95 (reviewing JOHN J. FIALKA, WAR BY OTHER MEANS: ECONOMIC ESPIONAGE (1997)).

202. Frank J. Garcia, *Protection of Intellectual Property Rights in the North American Free Trade Agreement: A Successful Case of Regional Trade Regulation*, 8 AM. U. J. INT'L L. & POL'Y 817, 824 (1993).

instance, could be taken as a formal accusation of the Chinese government's complicity in economic espionage efforts. Equally, it could be interpreted as an admission of guilt by the United States to intelligence-gathering in China. Tackling the problem through bilateral agreements could signal that economic espionage is, absent an agreement to the contrary, acceptable. The negotiation of a bilateral agreement could be prohibitively difficult. Bilateral agreements are unlikely to incorporate compliance-inducing mechanisms such as binding dispute resolution, monitoring procedures or provide for formal sanctions.[203] Finally, the potential for reputational harm is a greater deterrent in a multilateral context. Generally, a state that breaks an agreement between itself and multiple other states faces greater reputational harm than a state that breaks a bilateral commitment.

## IV. A WORKABLE SOLUTION

The concept of a convention prohibiting economic espionage has been discussed.[204] Most debate occurred as the *Economic Espionage Act* came into effect in 1996. There existed "little international will" to deal with the problem of trade secret theft at the time.[205] Some remarked that establishing a convention to deal with economic espionage would be difficult given "state involvement in that activity."[206] It was argued that detecting the surreptitious practice was not easy because of its passive nature, thus any prohibition would be difficult to enforce.[207] Further, many felt U.S. businesses needed less regulation, not more.[208]

---

203. Andrew T. Guzman, *The Design of International Agreements*, 16 EUR. J. INT'L L. 579, 605 (2005) (remarking that agreements with near-universal membership, such as the WTO, are more likely to provide for compliance-inducing mechanisms).

204. *See, e.g.*, McCurdy, *supra* note 201, at 140; Goodman, *supra* note 201, at 93; Michael T. Clark, Comment, *Economic Espionage: The Role of the United States Intelligence Community*, 3 J. INT'L LEGAL STUD. 253, 288–90 (1997); Todd A. Morth, Note, *Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter*, 30 CASE W. RES. J. INT'L L. 567, 581 (1998) (stating any prohibition on economic espionage would not be respected by the international community).

205. Blood, *supra* note 22, at 233.

206. Brenner & Crescenzi, *supra* note 31, at 455.

207. Morth, *supra* note 204, at 581.

208. Elaine Waldron, *Epidemic of Economic Espionage Takes Huge Toll on L.A. Companies*, L.A. BUS. J., Mar. 11, 1996, http://www.allbusiness.com/north-america/united-states-california-metro-areas/572231-1.html.

Businesses observed that the *Foreign Corrupt Practices Act* ("FCPA") already placed U.S. businesses at a significant disadvantage compared to their foreign competitors.[209] In much of the world, U.S. laws prohibiting the bribery of foreign government officials were seen as "quaint."[210] U.S. business craved a "leveling of the playing field" in relation to foreign competitors.[211]

The climate has changed considerably since the concept was dismissed. Recent developments suggest an improved global commitment to promoting ethical business practices. The "leveling of the playing field" sought by U.S. businesses arrived in the form of the OECD Convention.[212] U.S. anti-bribery laws once viewed as "quaint" have since become standard for thirty-eight countries that have implemented the OECD Convention in the form of domestic legislation. The OECD Convention has, for the most part, been successful in establishing an "anti-corruption culture" among members.[213] Along similar lines, the United Nations Convention against Corruption (the "U.N. Convention") entered into force in 2005.[214] Through its "four pillars" (prevention, criminalization, international cooperation, and asset recovery), the U.N. Convention strives to eliminate corruption in both the public and private sectors.[215] Further still, the United Nations Global Compact (the "Compact"), announced in 2000[216] and amended in

---

209. *Id.*

210. Schweizer, *supra* note 2, at 12.

211. Waldron, *supra* note 208.

212. Org. for Econ. Co-Operation & Dev., Convention on Combating Bribery of Foreign Public Officials, http://www.oecd.org/document/21/0,3343,en_2649_34859_2017813_1_1_1_1,00.html (last visited Apr. 8, 2009).

213. *See* Org. for Econ. Co-Operation & Dev., Fighting Bribery and Corruption: Frequently Asked Questions, http://www.oecd.org/document/18/0,3343,en_2649_37447_35430226_1_1_1_37447,00.html#how_works (last visited Feb. 10, 2008) [hereinafter OCED Fighting]; *see also* TRANSPARENCY INTERNATIONAL, PROGRESS REPORT 07 at 4, 21 (2007), *available at* http://www.transparency.org/content/download/21619/314761/file/3rd_OECD_progress_report_07.pdf.

214. Press Release, U.N. Information Services, United Nations Convention Against Corruption Enters Into Force on 14 December, U.N. Doc. CP/528 (Dec. 13, 2005), *available at* http://www.unis.unvienna.org/unis/pressrels/2005/uniscp528.html.

215. *Id.*

216. UN Global Compact Office, *UN Global Compact Annual Review 2007 Leaders Summit* 7 (July 5-6, 2007), *available at* http://www.unglobalcompact.org/docs/news_events/8.1/GCAnnualRevie

2004,[217] encourages businesses to conduct themselves in accordance with ten principles concerning human rights, labor, the environment, and corruption.[218] The Compact is not regulatory in nature; instead it relies upon public accountability, transparency, and the self-interest of participants to achieve compliance.[219] Among its many purposes, the Compact implores businesses to refrain from business practices which "discourage innovation and entrepreneurship"[220]—thus touching upon, tangentially, the practice of economic espionage.

These developments have elevated the role of ethics in global business. They indicate a readiness among the public and private sector to abandon individually-profitable activities in recognition of their larger destructive effects. However, these developments only deal with economic espionage in a marginal sense. Economic espionage remains to be explicitly addressed by any international commitment. Incidents will rise until joint efforts are made to solve the problem.[221]

Entrenching an agreement prohibiting economic espionage as a convention would subject its provisions to the Vienna Convention on the Law of Treaties, obliging parties to comply as a matter of international law.[222] Clarifying the status of economic espionage as an impermissible activity would ease management of the problem across different cultures.[223] A convention would spread the economic[224] and political[225] costs of responding to

---

w2007.pdf.

217. *Id.* at 37.

218. *Id.* at 6.

219. *Id.* at 4.

220. *Id.* at 6.

221. NASHERI, *supra* note 138, at 172.

222. *See* Vienna Convention on the Law of Treaties, art. 26, *concluded* May 23, 1969, 1155 U.N.T.S. 331, *available at* http://untreaty.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf [hereinafter VCLT] ("Every treaty in force is binding upon the parties and must be performed by them in good faith"). The VCLT is seen as an authoritative statement of the customary international law of treaties, even by non-signatories.

223. Philip M. Nichols, *The Myth of Anti-Bribery Laws as Transnational Intrusion*, 33 CORNELL INT'L L.J. 627, 642–43 (2000).

224. *See* Helfer, *supra* note 187, at 1616 (noting that an economic espionage convention would require financial contributions from members for expenditures such as support staff, facilities, and operations). Presumably, these costs would be lower in a multilateral context than if each state were to establish individual counter-espionage programs concentrating on economic espionage.

economic espionage amongst the membership base, making any response less costly for individual members. Further, a multilateral response would be more effective than one made unilaterally.[226] A convention would encourage transparency and promote the Western business ethic by encouraging fair competition.[227] Information sharing could lead to other cooperative opportunities, technical advances, and accelerate economic development.[228]

## V. CONVENTION FRAMEWORK

Commentary on a convention prohibiting economic espionage has been scarce. The structure of such an agreement remains unaddressed. The remainder of this article deals with this issue and discusses the potential barriers to implementation the proposed convention would face.

### A. MONITORING PROCEDURES

An economic espionage convention would require a monitoring procedure to ensure that parties face sanctions for their misbehavior. Monitoring would increase the information available to members, allowing them to better co-ordinate a response to an instance of economic espionage than in an information poor (i.e., convention-less) environment.[229] To satisfy

---

225. *See, e.g.*, Wolff, *supra* note 194, at 361. An accusation of, or response to, economic espionage has certain implications. Unilateral responses typically cause resentment for the imposing state in the target state. A multilateral response decreases resentment toward particular states and is more likely to be viewed as legitimate by the international community.

226. Jordan, *supra* note 197, at 339 (remarks by R. Rennie Atterbury III); *see also* Smith, *supra* note 192, at 370 ("Sanctions are most effective and least costly when they have broad support from the international community.").

227. *See, e.g.*, McCurdy, *supra* note 201, at 139 (warning that if the "world's major trading powers begin viewing each other with suspicion, hoarding economic breakthroughs like atomic secrets and monitoring each other like enemies, the world could easily slide into an economic version of the Cold War").

228. *Id.* at 140.

229. *See* Julian Oullet, *Monitoring of Agreements*, BEYOND INTRACTABILITY, Nov. 2003, http://www.beyondintractability.org/essay/monitoring_agreements (explaining the use of monitoring to ensure enforcement of international agreements).

this objective, transparency is of paramount importance in the monitoring process.[230] Monitoring standards should be objective and agreed upon in advance.[231] Important considerations include how, by whom, and for what purposes monitoring is conducted.[232] The skill and expertise of the monitors themselves is relevant.[233] Typical compliance monitoring methods include self-reporting, informal statements of state conduct, or formal compliance inspections by impartial observers.[234]

Self-reporting or informal statements of state conduct would not be reliable means of monitoring an economic espionage convention. Both represent "sunshine methods" of promoting compliance—that is, methods by which the potential reputational harm to a party promotes compliance.[235] Such methods are unlikely to ensure the compliance of all members in the absence of further coercive factors, such as direct sanctions.[236] The incentives for moral hazard in this context may be overwhelming.

States suspected of economic espionage are reluctant to disclose their participation and would not self-report given their prior decision to participate in the conduct. An obvious failure to report would antagonize other parties and undermine the agreement's credibility. Self-reporting should be encouraged, but could not be relied upon to an extent inconsistent with the proposed convention's underlying objective of transparency. Informal statements of state conduct would create a similar problem. Any response to an informal statement is discretionary;

---

230. *See id.* (listing transparency among generalized monitoring rules).

231. *See id.* (suggesting the use of "open and standardized measures for compliance" as a generalized monitoring rule).

232. Richard Locke, Fei Qin & Alberto Brause, *Does Monitoring Improve Labor Standards?: Lessons from Nike* 7 (MIT Sloan Research Paper No. 4612-06), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=916771.

233. The skill and experience of an agreement's monitors is a source of concern. Monitors may be experienced professionals, though they may also be "recent college graduates whose primary skill is . . . speaking a particular foreign language." *See id.* at 6.

234. Guzman, *supra* note 203, at 585.

235. Steve Charnovitz, *Rethinking WTO Trade Sanctions*, 95 AM. J. INT'L L. 792, 829 (2001).

236. *See* Andrew T. Guzman, *Reputation and International Law*, 34 GA. J. INT'L & COMP. L. 379, 387 (2006) ("The key point is to recognize that reputation acts at the margin, like all influences. If other relevant forces are sufficiently strong, they will swamp reputational concerns, but when other forces are less determinative, reputation can affect outcomes.").

therefore, the reliability of such measures is questionable.[237] A failure to comply would antagonize other parties and undermine the agreement's credibility.

Such informal methods may be justifiable when an agreement places onerous implementation costs on members. The proposed convention, however, has low implementation costs.

---

237. For example, the OECD Convention relies exclusively on such means. *See* Org. for Econ. Co-Operation & Dev., Country Reports on the Implementation of the OECD Anti-Bribery Convention and the 1997 Revised Recommendation, http://www.oecd.org/document/24/0,3343,en_2649_37447_1933144_1_1_1_37447,00.html (last visited Feb. 10, 2008)[hereinafter Country Reports]. Its reports do not initiate direct sanctions against member states that fail to effectively implement monitors' recommendations. Only recommendations are forwarded to the government of each participating country. OCED Fighting, *supra* note 213. Consequently, member states enforcement records have not improved and many have yet to bring charges under domestic anti-bribery legislation. *See generally* Country Reports, *supra* at 237. Transparency International's OECD Anti-Bribery Convention Progress Reports 2007 and 2008 list the investigations performed by signatories dating back to 2006. Many countries have either performed no investigations or have not made information available as is required by the Convention. *See generally* Transparency International, Global Priorities: International Conventions, http://www.transparency.org/global_priorities/international_conventions (last visited Apr. 26, 2009). The 2008 Report notes "the lack of enforcement in over half of the countries is very disturbing." TRANSPARENCY INTERNATIONAL: THE GLOBAL COALITION AGAINST CORRUPTION, PROGRESS REPORT 2008: OECD ANTI-BRIBERY CONVENTION 8 (June 24, 2008), http://www.transparency.org/global_priorities/international_conventions.

In contrast, the WTO has adopted a comparatively formal monitoring procedure. Its Dispute Settlement Body ("DSB") generally adopts the decisions of the body's primary internal monitors, its "panels." *See* WORLD TRADE ORG., UNDERSTANDING THE WTO: SETTLING DISPUTES 55–56 (2007), *available at* http://www.wto.org/english/thewto_e/whatis_e/tif_e/utw_chap3_e.pdf. WTO panels consist of three or five experts from different states who examine evidence. The experts are fully independent. They cannot serve in their individual capacities, nor can they receive instructions from any government. *Id.* Panel reports may only be rejected by a DSB consensus, thus panel reports are difficult to overturn. This procedure has resulted in a positive compliance record among members. *Id* at 58; *see also* Guzman, *supra* note 236, at 387 ("The key point is to recognize that reputation acts at the margin, like all influences. If other relevant forces are sufficiently strong, they will swamp reputational concerns, but when other forces are less determinative, reputation can affect outcomes."); Bruce Wilson, *Compliance by WTO Members with Adverse WTO Dispute Settlement Rulings: The Record to Date*, 10 J. INT'L ECON. L. 397, 397 (2007).

Implementation would consist of a mere pledge to refrain from conducting economic espionage. The simplicity justifies a higher standard.

This discussion suggests formal compliance inspections would be required to effectively monitor the proposed convention. Further discussion concerning the formal compliance mechanism follows in the section titled "Dispute Resolution Processes."

### B. SANCTIONING PROCEDURES

Sanctions are coercive means of altering a targeted state's behavior. In the context of an international agreement, they are imposed as a result of a party's infringement.[238] Most international agreements do not employ sanctions as a compliance measure. When sanctions are called for, they are usually prospective and not strict enough to ensure compliance.[239] The imposition of sanctions almost always represents a net welfare loss for the parties to the transaction—not just the targeted party.[240] Nevertheless, sanctions are a popular deterrence measure, as a failure to impose sanctions may lead to a reputation as a "pushover."[241] Sanctioning authority would increase a convention's standing amongst governments and international organizations.[242] Further, the drawbacks of sanctions are greatly reduced if applied as part of a multilateral regime.[243] Sanctions may include financial or trade restrictions, monetary damages, withdrawals of intelligence-sharing privileges, formal diplomatic protests, or threats to cease other cooperative arrangements.[244]

Trade restrictions should generally be avoided to the extent possible, as they negatively affect both the target and sanctioning party.[245] They shift production to less efficient producers, restricting global output while raising prices for consumers.[246]

---

238. Guzman, *supra* note 203, at 595–96.
239. *Id.* at 589.
240. Andrew T. Guzman, *The Cost of Credibility: Explaining Resistance to Interstate Dispute Resolution Mechanisms*, 31 J. LEGAL STUD. 303, 323 (2002).
241. *Id.*
242. Charnovitz, *supra* note 235, at 809.
243. Jordan, *supra* note 197, at 339.
244. Goodman, *supra* note 201, at 95; *see also* Helfer, *supra* note 187, at 1618.
245. Guzman, *supra* note 240, at 323.
246. *Trade Restrictions and their Effects*, ECONOMIC EDUCATION WEB –

DANIELSON MEA. Economic Espionage: A Framework for a Workable Solution. MINN. J.L. SCI. & TECH. 2009;10(2): 503-548.



Worse still, trade restrictions are often met with retaliatory restrictions imposed by the target state.[247] If trade restrictions are utilized, they are best imposed selectively.[248] For example, tariffs or quotas could be placed on a target's exports to correct unacceptable behavior without resorting to a comprehensive embargo. Provisional restrictions could be imposed on the product or services targeted by the espionage attempt in appropriate circumstances. Restricting visiting students' and researchers' landing rights or access to facilities would selectively target a popular intelligence gathering method, while limiting private investment by a target state's citizens could frustrate foreign front companies' attempts to establish a domestic foothold. Further still, a state's eligibility for foreign aid or export finance programs could be affected by a decision to participate in economic espionage.

Historically, states have been reluctant to include provisions calling for damages in their agreements.[249] This is due in part to the difficulty in assessing damages in the context of most international agreements. This problem does not arise in the context of economic espionage. The damages arising from economic espionage are the losses attributable to the spying state's activities.[250] Monetary damages are preferable to trade retaliation because the obligation to pay the fine falls on the target and mitigates the harm to the sanctioning party.[251] Further, pecuniary measures in the form of a fine are desirable. A fine penalizes a violation of law and is distinct from a monetary judgment awarded against a tortfeasor.[252] Fines are rarely used as

---

UNIVERSITY OF NEBRASKA OMAHA, http://ecedweb.unomaha.edu/lessons/foegactivity1.htm (last visited Feb. 27, 2009).

247. *Id.*

248. *See, e.g.*, State Secretariat for Economic Affairs SECO, Smart Sanctions, http://www.seco.admin.ch/themen/00513/00620/00639/index.html?lang=en (last visited Dec. 2, 2008) (noting that targeted sanctions restrict "collateral damage" to civilian populations in target states).

249. Guzman, *supra* note 203, at 609.

250. *See id.* at 610 (stating that the use of monetary damages may be appropriate in those situations where "the harm is closely tied to economic harms").

251. Charnovitz, *supra* note 235, at 827.

252. *Id.* at 825.

a compliance measure in international agreements,[253] yet fines provide considerable incentive for parties to refrain from participating in economic espionage. Absent a fine, a party may weigh the potential reward of committing economic espionage against the prospect of accounting to the victim and accept the risk—a fine mitigates the prospect of scofflaws "breaking even" through their activities.[254] To this end, a provision authorizing an assessment of double or treble damages may be advisable.

Persistent disregard for the proposed convention's terms would lead to expulsion.[255] A threat of expulsion improves the likelihood parties would accept other compliance-inducing mechanisms.[256] An expelled party would be unable to participate in negotiations, make use of a convention's information-sharing network, or utilize its dispute resolution mechanisms.[257] Further, any expulsion would be heavily publicized, thus promoting compliance by appealing to states' reputational concerns.

### C. DISPUTE RESOLUTION PROCESSES

Dispute resolution processes ("DRPs") facilitate compliance[258] by providing a mechanism through which monitoring and sanctioning procedures may be given effect. Such a mechanism would be essential to a convention prohibiting economic espionage. To start, the standing requirements under the proposed convention are addressed. Subsequently, the importance of a binding, expeditious DRP is discussed. Standing requirements vary widely among international DRPs. Options include (i) state espousal of a victim's claim, (ii) a private right of action ("PRA"), or (iii) regulatory enforcement. Each is examined below.

---

253. *Id.*

254. *See* Andrew T. Guzman, *A Compliance-Based Theory of International Law*, 90 CAL. L. REV. 1823, 1860–61 (2002).

255. Many international agreements contain provisions that limit or deny membership privileges to non-complying members, but such provisions are rarely invoked. Charnovitz, *supra* note 235, at 827.

256. Guzman, *supra* note 254, at 1872.

257. Helfer, *supra* note 187, at 1614.

258. *See* Guzman, *supra* note 203, at 601. Despite this fact, only around half of international agreements include DRPs. *See* Barbara Koremenos, *If Only Half of International Agreements Have Dispute Resolution Provisions, Which Half Needs Explaining?*, 36 J. LEGAL STUD. 189, 190 (2007).

### 1. State Espousal

State espousal is a process by which a state effectively adopts a citizen's claim and asserts his rights on his behalf.[259] The decision to assert a claim is discretionary.[260] Given states' reluctance to publicly accuse others of economic espionage, state espousal could not reliably enforce the proposed convention. Businesses lacking the influence of more powerful lobbies may have difficulty persuading their government to respond to offenses.[261] The process could lead to mutual non-enforcement, as diplomatic concerns may influence the decision to assert a claim. This is not a marked departure from the status quo. Ultimately, the process would undermine the proposed convention's transparency and credibility.

### 2. Private Right of Action

A PRA would give economic espionage victims standing to assert a claim.[262] When appropriate, a PRA may grant standing to an entity unconnected with the activities, such as an NGO, to seek redress for a public harm (a "public PRA").[263] PRAs obviate the mutual non-enforcement problem by removing prosecutorial discretion from the state.[264] PRAs enhance the credibility of agreements by improving the prospect that a state will be penalized for noncompliance.[265] On the other hand, PRAs restrict states' sovereignty, which may cause states to resist compliance or abstain from participation.[266] A PRA may limit opportunities to establish strategic direction and could slow the DRP by encouraging repetitive claims.[267]

---

259. Philip M. Moremen, *Private Rights of Action to Enforce Rules of International Regimes*, 79 TEMP. L. REV. 1127, 1174 (2006).

260. *Id.*

261. Alan O. Sykes, *Public Versus Private Enforcement of International Economic Law: Standing and Remedy*, 34 J. LEGAL STUD. 631, 648 (2005).

262. Philip M. Moremen, *Costs and Benefits of Adding a Private Right of Action to the World Trade Organization and the Montreal Protocol Dispute Resolution Systems*, 11 UCLA J. INT'L L. & FOREIGN AFF. 189, 197 (2006).

263. Moremen, *supra* note 259, at 1133.

264. *Id.* at 1141.

265. *Id.*

266. Moreman, *supra* note 262, at 201.

267. *Id.* at 194. Moremen states that decentralized enforcement mechanisms, such as PRAs, are more efficient in some circumstances, "but centralized mechanisms [like regulatory enforcement,] may . . . take advantage of coordinated decision-making and . . . avoid the transaction

Such considerations must be balanced to determine whether a PRA would benefit the proposed convention. Philip Moremen suggests a PRA is most effective when (a) states desire increased enforcement, (b) plaintiffs are adequately incentivized, and (c) sovereignty costs are minimal.[268] In the absence of one or more of these factors, he suggests a PRA may still be beneficial if (d) the advantages of strict enforcement exceed the disadvantages or states want to make a credible commitment.[269] This framework applies to the proposed convention as follows:

(a) The desire for increased enforcement of an economic espionage convention would vary among states. Habitual practitioners would likely resist a PRA, while those most victimized by the practice would be motivated to limit it. Support for increased enforcement would be strong amongst the Western states likely to comprise a convention's initial membership.

(b) Whether private plaintiffs are adequately incentivized to assert claims is debatable. Adjusting the incentives to encourage them to do so is difficult.[270] Victims appear highly motivated to bring claims, as their proprietary information has been compromised. However, as discussed, economic espionage victims are often reluctant complainants. The creation of a public PRA would seemingly target this problem. However, public PRAs are most effective when there is an active NGO community willing to bring claims.[271] As will be discussed, NGOs have been indifferent towards economic espionage to date. Providing for anonymity in the process could also target this problem, though doing so would undermine the proposed convention's transparency objectives. A state may look to capitalize on its citizens' anonymity, complicating the task of linking a state to its questionable conduct.

(c) Sovereignty costs are lower in matters of low politics (e.g., economic matters) than high politics (e.g., state security).[272]

---

costs of piecemeal enforcement by private parties." *Id.* at 193.

268. Moreman, *supra* note 259, at 1130.

269. *Id.* at 1177.

270. Moremen, *supra* note 262, at 225.

271. Moremen, *supra* note 259, at 1177.

272. *Id.* at 1178; *see generally* Norrin M. Ripsman, False Dichotomy: When Low Politics is High Politics (Mar. 17, 2004) (unpublished manuscript presented at the annual meeting of the International Studies Association, Le Centre Sheraton Hotel, Montreal, Quebec, Canada (Feb. 6, 2009), *available at* http://www.allacademic.com/meta/p73388_index.html) (distinguishing between matters of low and high politics).

Economic espionage is a matter of high politics. Its practice is considered by many to be vital to state security. The fact that no minimum obligations regarding economic espionage exist at the international level suggests states are reluctant to relinquish sovereignty in this area, as they have not previously done so.[273] The role of state secrets privilege in the process is problematic. States concerned about exposure to spurious claims or disclosure of sensitive information may favor a regulatory body, though enabling a secretariat to screen claims for their legitimacy could manage the former concern.[274]

(d) The benefits of strict enforcement exceed any disadvantages. Because the proposed convention prescribes an absolute prohibition, flexibility, leading to uneven application, would damage its credibility. States require a credible commitment. This would minimize the prospects of non-compliance by others, reducing the opportunity cost of participation. The likelihood of states' indiscretions going unpunished, while compliant states look on, would be decreased. A PRA would signal a state's intention to take an obligation seriously.[275]

### 3. Regulatory Enforcement

Alternatively, a convention could be enforced through the establishment of a regulatory body to investigate and prosecute violations.[276] The body, as opposed to private parties, would have standing to commence an action.[277] In regulatory systems, matters are usually referred to an internal administrative body or an independent tribunal for adjudication.[278]

A regulatory mechanism addresses the problems of mutual non-enforcement and private party reluctance by assigning prosecutorial discretion to the regulator. More often than not,

---

273. *Cf.* D. Daniel Sokol, *Order Without (Enforceable) Law: Why Countries Enter Into Non-Enforceable Competition Policy Chapters in Free Trade Agreements*, 83 CHI.-KENT L. REV. 231, 260–61 (2008) (considering inadequate minimum economic espionage obligations in the context of the lack of international antitrust commitments, but the same reasoning applies).

274. Moremen, *supra* note 262, at 222.

275. Moremen, *supra* note 259, at 1177.

276. *Id.* at 1136.

277. *Id.*

278. *Id.*

regulators possess greater resources and investigative powers than do private parties,[279] and benefit from economies of scale.[280] While private parties possess an informational advantage over regulators when the offender's identity is known, they are comparatively disadvantaged when it is unknown.[281] Alas, this is often the case in circumstances of economic espionage.

Regulators have a wide discretion in terms of both enforcement decisions and options.[282] This flexibility could present states more opportunity to influence the enforcement process, counteracting the proposed convention's transparency objectives.[283] To be effective, a convention would require provisions limiting the discretion of its regulators. Predictable, uniform enforcement would be critical.

Private party participation in the enforcement process is not limited to PRAs. Regulatory mechanisms may permit participation directly, through the right to observe proceedings, or indirectly, through the use of amicus briefs.[284] Such measures would improve transparency while avoiding the problems associated with multiple plaintiffs that may arise under a PRA.

A final consideration is whether non-member states should have standing to assert claims under the proposed convention. At first glance, a PRA is helpful. Denying any victim of economic espionage standing seems unfair, given the proposed convention's goal of eliminating the practice. This is particularly so if the perpetrator is a member state. Regardless, access to the DRP is an incentive to participate in the proposed convention. If non-member states could access the DRP in these circumstances, the incentive for membership is diminished. Also, domestic pressure on non-member governments to join an economic espionage convention would presumably intensify as citizens increasingly demand redress. A regulatory regime would strike a balance between punishing non-compliance and promoting convention participation.

### 4. Recommendation on Standing and Other Considerations

This analysis suggests a regulatory enforcement mechanism

279. *Id.* at 1143.
280. Moremen, *supra* note 262, at 201.
281. Moremen, *supra* note 259, at 1141.
282. *Id.* at 1130.
283. *Id.*
284. Moremen, *supra* note 262, at 214.

is preferable. The advantages of a PRA could be reasonably approximated by a carefully-crafted regulatory mechanism. This conclusion is supported by the remarks of others.[285] There remain further aspects of the DRP that must be considered.

The DRP must bind parties to any dispute. Referred or submitted disputes must produce a final decision that cannot be unilaterally avoided by any member.[286] In agreements with strict sanctions, such as the proposed convention, this is particularly important. Historically, states have been reluctant to submit to binding dispute adjudication,[287] particularly when the stakes are high.[288] This reluctance may stem from states' desire to preserve control of disputes or may be due to the fear of losing a binding verdict.[289] However, states are more willing to submit to binding dispute resolution in the multilateral context and when the relevant tribunal's accuracy is recognized.[290] The bias against binding dispute resolution is waning and the practice is gaining a broader appeal.[291] Significantly, the Western states likely to compose a convention's initial membership are traditionally proponents of binding dispute resolution.[292]

Also, the DRP must operate expeditiously. The slow pace of DRPs in international agreements is a frequent complaint.[293] In

---

285. *See, e.g.*, Michelle Sandilands, *Key Laws Governing the Practice of Competitive Intelligence in Global Business, in* COMPETITIVE INTELLIGENCE AND GLOBAL BUSINESS 82–83 (David L. Blenkhorn & Craig S. Fleisher eds., 2005) ("[O]nly international agreements that include an enforcement agency will be able to penalize violators and thus reduce government involvement [in economic espionage].").

286. Anne Peters, *International Dispute Settlement: A Network of Cooperational Duties*, 14 EUR. J. INT'L L. 1, 4 (2003).

287. *Id.* at 30; *see also* Guzman, *supra* note 240, at 304 ("A survey of 100 treaties registered with the United Nations and published in the United Nations Treaty Series yielded 80 treaties without a mandatory dispute settlement mechanism and only 20 with such a mechanism.").

288. Guzman, *supra* note 240, at 303.

289. Guzman, *supra* note 203, at 593–94.

290. Guzman, *supra* note 240, at 303.

291. Peters, *supra* note 286, at 30.

292. *Id.*

293. *See, e.g.*, *International Union, United Automobile, Aerospace and Agricultural Implement Workers of America: Hearing on Accession of China to the WTO Before the H. Comm. on Ways and Means,* 105th Cong. (2000) (statement of Alan Reuther, Legislative Director for the International Union, United Automobile, Aerospace and Agricultural Implement Workers of America), *available at*

this context, quick resolution is important, as stolen information may be swiftly assimilated into a competing product or service and leveraged into a sustained competitive advantage.[294] Prompt decisions could prevent or mitigate the damage to victims of economic espionage.[295] To this end, distinct timeframes for resolution would be prescribed by the agreement.

### D. ADMISSION & EXIT

Successful "public goods" agreements encourage participation.[296] Therefore, a convention should deal strictly with economic—not industrial—espionage. Recall that economic espionage has an element of state participation, while private parties commit industrial espionage. By limiting the proposed convention's scope to a matter directly within each state's control—the decision to commit economic espionage—membership is made available to a broader range of parties. States lacking the resources to effectively police industrial espionage would agree to refrain from participating in the practice. States would be responsible for contributing to the monitoring and enforcement of a convention, but the costs of policing economic espionage would be minimal, as states' involvement would be reduced. At worst, industrial thieves would have fewer willing buyers to pay for their information. This is significant, as governments are often the only suitors for stolen information.[297]

The proposed convention would prohibit all state involvement in the processes of economic espionage, including the passive receipt of information. As discussed, states are increasingly making use of information gathered by the private sector. Refraining from economic espionage while making use of unsolicited information would be incongruous with the purpose of

---

http://waysandmeans.house.gov/legacy.asp?file=legacy/fullcomm/106cong/5-3-00/5-3reut.htm.

294. Moyer, *supra* note 162, at 189.

295. *Id.* at 204.

296. Laurence R. Helfer, *Nonconsensual International Lawmaking*, 2008 U. ILL. L. REV. 71, 99 (2008).

297. *See, e.g.*, *Economic Espionage: Information on Threat From U.S. Allies, United States General Accounting Office Testimony Before the Select Committee on Intelligence* (statement of David E. Cooper, Associate Director, Defense Acquisitions Issues, National Security and International Affairs Division), 1–5, *available at* http://www.hanford.gov/oci/maindocs/ci_r_docs/gao96ee.pdf.

the proposed convention. A single purchase of such information would undermine its integrity and signal to industrial thieves the state implicitly encourages such behavior. Member states would be unable to utilize information one should reasonably suspect was obtained through suspect tactics. Conceivably, states might engage in a "final" economic espionage venture prior to seeking membership. To deter such conduct, a state would require a record of compliant behavior for a period of time prior to membership.

Reservations entitling states to exclusive benefits would be impermissible. Such measures transform agreements into "kaleidoscope[s] of a la carte legal commitments"[298] and would be incompatible with the required uniform application of the proposed convention. There is a rebuttable presumption at international law prohibiting exit from an agreement that does not permit withdrawal.[299] The proposed convention would not permit withdrawal. This would "weed out states that are less serious about future compliance."[300] To conclusively put an end to economic espionage, the proposed convention would be permanent. This would help ensure the cooperation of all states into the future.[301] As discussed, persistent disregard for its terms would lead to expulsion. Expelled states would be unable to reclaim membership status for a prescribed period of time. This would discourage opportunistic behavior by precluding member states from accepting the consequences of a one-time violation and then subsequently reapplying for membership.

## VI. OBSTACLES TO IMPLEMENTATION

Participation poses a dilemma for some states. Ultimately, all states would reap the benefits of an economic espionage convention in the long-term by way of improved global stability and an accelerated rate of innovation. However, "public goods" agreements encounter a unique problem. States that do not participate in the production of a public good (i.e., join the

298. Helfer, *supra* note 187, at 1640–41.

299. VCLT, *supra* note 222, art. 42.

300. Helfer, *supra* note 187, at 1591; *see also id.* at 1600 (stating that treaties which permit easy exit usually impede future cooperation as states may seek exit "whenever economic, political or other pressures make compliance costly or inconvenient").

301. *Id.* at 1632–33.

proposed convention) would nonetheless benefit from its production.[302] Less-Developed States ("LDSs") have little incentive to participate given that economic espionage is profitable to participants[303] and saves the time and the financial resources required to develop technologies independently.[304] A movement for change will not come from states desperate to catch their more successful neighbors. LDSs may ignore reputational concerns to engage in economic espionage and free-ride off the gains made publicly available by a convention.[305] This would be rational for a LDS already suffering from a poor reputation for corruption or integrity. Under such circumstances, it is anticipated many states would abstain from membership.

This problem is solvable. It may be confronted by offering member states privileges unavailable to non-complying members and non-members.[306] For example, members would have access to the information-sharing network and DSP previously described, in addition to other cooperative opportunities. Another equally important incentive would reveal itself over time. In due course, states may covet the reputational benefits of membership. The international community would view states that subscribe to the proposed convention in a positive light. A positive reputation enhances the credibility of a state's promises,[307] providing greater leverage in international negotiations and broadening the range of available cooperative opportunities.[308] Reputational concerns have been shown to be an important factor in a state's decision to

---

302. Once a "public good" is established, the cost to producers to prevent others from consuming the good is cost-prohibitive. Those that have not contributed to a good's development still reap the benefits of its production. Some regard products of international cooperation, like the proposed convention, as equivalent to pure public goods. *See* John K. Setear, *An Iterative Perspective on Treaties: A Synthesis of International Relations Theory and International Law*, 37 HARV. INT'L L.J. 139, 174–76 (1996).

303. *See, e.g.*, Schweizer, *supra* note 2, at 12 ("That so many states practice economic espionage is a testament to how profitable it is believed to be."); *see also* NOLAN, *supra* note 4, at 2 ("It doesn't take the President of the World Bank to figure out that if you spend $500,000 bribing a research scientist in the United States to get the trade secret or proprietary information that an American company has spent $750,000,000 developing, the intelligence operation has just netted $700 million.").

304. Sepura, *supra* note 5, at 133.

305. *See* Setear, *supra* note 302.

306. Helfer, *supra* note 296, at 101.

307. Guzman, *supra* note 240, at 383.

308. *Id.* at 385.

comply with its obligations.[309] LDSs striving to improve international reputations may find non-membership too costly to endure. Further, LDSs have more to lose to economic espionage as they develop. As development takes place, it is anticipated that states will increasingly seek to protect their assets through international law.[310] Further still, as more states subscribe to the proposed convention, the more conspicuous non-members would become. A shrinking pool of non-members would immediately be suspected in the event of any economic espionage incident. Thus, a convention benefits from a kind of virtuous cycle.

Another factor that must be considered is that the success of "public goods" agreements is frequently contingent on the level of participation.[311] In other words, a convention's success could turn depending on how many states subscribe to the agreement. If states doubt one another's willingness to comply with a convention, participation may be a problem from the outset. This difficulty may be confronted in two ways. First, the proposed convention would adopt strong compliance measures that would increase the prospects of cooperation by making misbehavior more costly.[312] It is not uncommon for a state to adopt an agreement as a means of compelling its own compliance while signaling to others its intention to adhere to its terms.[313] Second, a convention could require a ratification threshold taking into account a prescribed number of states, their size, or their relative financial contributions, before entering into force.[314] Such measures have been shown to create "treaty bandwagons" which facilitate the cooperative process.[315] This compromise may help resolve a stalemate between states reluctant to bind themselves until others do likewise.

## VII. GAINING MOMENTUM

A convention would need the backing of the U.S. Government, businesses, and NGOs to gain momentum. The Government has acknowledged, through the creation of the *Economic Espionage*

309. Guzman, *supra* note 203, at 595–96.
310. WERT, *supra* note 30, at 4.
311. Helfer, *supra* note 296, at 99.
312. Guzman, *supra* note 203, at 605.
313. Moremen, *supra* note 259, at 1141.
314. *See* Helfer, *supra* note 187, at 1638.
315. Helfer, *supra* note 296, at 99.

*Act*, that economic espionage is a serious problem. The FBI has stated that economic espionage is a priority second only to terrorism.[316] U.S. businesses, which have had to bear the cost of these thefts, have voiced their frustrations. Commentators, appreciating the shortcomings of domestic law, have observed that further steps to combat economic espionage may have to occur at the international level. However, NGO support for this notion is lacking. NGOs play a crucial role in the establishment of international norms[317] and the development and implementation of international agreements.[318] NGO support is a prerequisite to establishing a consensus among the international community that economic espionage is an unwelcome practice.

There are various reasons for this lack of support. Most NGOs are concerned with monitoring domestic practices and do not possess the resources or mandate to think globally.[319] The symbiotic relationship[320] between NGOs and the media compels them to focus on hot-button issues that generate public interest and garner support for their cause.[321] This is worrying, as problems lacking journalistic appeal may be nonetheless damaging. Further, a dependence on funding or the preferences of members may determine the issues with which NGOs deal.[322] Finally, while NGOs are less encumbered by the difficulties states encounter in publicly accusing other states of misconduct,[323] they must still consider the consequences of publicly accusing states of misconduct versus the benefits of working "behind the scenes" to modify states' behaviors.[324] Like inter-state relationships,

316. WERT, *supra* note 3, at 5.

317. Ellen Gutterman, *NGO Activism and State Compliance, with Three Anti-Corruption Treatises: The Role of Transparency International* 2 (Mar. 5, 2005) (paper presented at the annual meeting of the International Studies Association, Hilton Hawaiian Village, Honolulu, Hawaii), http://www.allacademic.com/meta/p_mla_apa_research_citation/0/7/0/4/2/p70423_index.html.

318. OLIVER MEIER & CLARE TENNER, VERIFICATION RESEARCH, TRAINING, AND INFORMATION CENTER, NON-GOVERNMENTAL MONITORING OF INTERNATIONAL AGREEMENTS 207 (2001) (U.K.), *available at* http://www.vertic.org/assets/VY01_Meier_Tenner.pdf.

319. *Id.* at 217.

320. NGOs depend on the media to publicize their work and thus are obliged to focus their efforts on issues of interest to journalists. *See id.* at 219.

321. *Id.* at 218.

322. *Id.*

323. *Id.* at 216.

324. *Id.* at 220.

relations between NGOs and states may occur on different levels simultaneously. This may help explain why certain NGOs, which ostensibly would be opposed to economic espionage, have been reluctant to address it.[325] Abstaining from publicly criticizing a state may be provident for an NGO working "behind the scenes" to improve a state's compliance in other areas. Fresh allegations may embarrass the state and hurt the relationship the NGO has worked to foster. As the norms these NGOs are working towards become universally accepted, attention may shift to combating the problem of economic espionage.

## VIII. CONCLUSION

Superficially, economic espionage has a zero sum outcome: one state's loss is another's gain. A broader examination reveals otherwise. It discourages innovation[326] by eroding businesses' hard-earned competitive advantage.[327] It reduces profitability,[328] forcing businesses to recoup losses by raising costs to consumers.[329] Businesses, already undercut by lower production costs overseas, may not be viable after factoring in the cost of these thefts. Economic espionage unquestionably raises tensions between states[330] and challenges the security and stability of sovereign states.[331]

Disturbingly, the practice is on the rise globally. Domestic legislation has not adequately addressed the problem. This is evidenced by the fact that despite the escalation of economic espionage, the number of prosecutions under the EEA can be counted on one hand.[332] Governments have placed the burden on

---

325. It is curious that those NGOs that are the catalysts behind anti-bribery and corruption movements have been silent regarding economic espionage. The effects of these practices and economic espionage are strikingly similar: both distort trade, undermine economic development, misdirect resources from more valuable uses, and confer benefits on undeserving parties. *See* OCED Fighting, *supra* note 213.

326. Sepura, *supra* note 5, at 138.

327. ASIS INT'L, *supra* note 9, at 41.

328. Vaknin, *supra* note 16.

329. Thierry Olivier Desmet, *The Economic Espionage Act 1996: Are We Finally Starting to Take Corporate Spies Seriously?*, 22 HOUS. J. INT'L L. 93, 95–96 (1999).

330. Brenner & Crescenzi, *supra* note 31, at 399.

331. *Id.* at 449.

332. As of the time of writing, only three cases prosecuted have alleged economic espionage under § 1831 of the Act. *See* Press Release,

businesses to secure their assets to the utmost degree, which is laudable. However, no business possesses the resources, financially or otherwise, to continuously fend off a state intent on stealing its valuable secrets.[333] Economic espionage is unregulated at the international level; the only level where it can be effectively enforced.[334]

This deficiency could be corrected by establishing a convention prohibiting economic espionage. The prevalent view is that economic espionage cannot be effectively regulated due to states' inherent interest in conducting the activity and the difficulty in detecting such a surreptitious practice. These positions are debatable. First, states are increasingly willing to jointly endeavor to eliminate destructive business practices that are independently profitable. The contemporary business environment is more hospitable to agreements that challenge the status quo. Second, enforcement difficulties would be addressed through the strength of the commitment. The consequences of non-compliance would be sufficient to deter transgressions at the outset. Further, the surreptitious nature of other undesirable business practices, like bribery, has not discouraged regulation efforts.

The proposed framework has been informed by the structure of other international agreements. A convention would feature swift and binding dispute resolution with regulatory oversight. Independent monitors who are not merely relegated to an advisory role would inform the body. Targeted sanctions would be imposed against non-complying states, with monetary damages and fines providing the primary incentive for compliance. Ultimately, the measures adopted should make economic espionage not worth the risk. Stern measures are justified by the fact that economic espionage is deliberate; transgressions would not arise by mistake or by a lack of capacity to comply.

Given that domestic prosecutions have been disproportionately low to the level of activity, a proposal to address the problem at the international level would presumably generate interest. So far, this has not been the case. Economic

---

Department of Justice, Chinese National Sentenced for Committing Economic Espionage with the Intent to Benefit China Navy Research Center (June 18, 2008), http://www.usdoj.gov/criminal/cybercrime/mengSent.pdf.

333. 142 CONG. REC. S12, 211 (1996) (statement of Sen. Kohl).

334. *See, e.g.*, WERT, *supra* note 3, at 5 ("National laws mean nothing without international protection and multi-lateral agreements.").

espionage has not been made a priority by any NGO, and as such, the practice continues unabated. My purpose is not to rebuke those remaining dormant, but to question why the problem has not received attention. Economic espionage is as destructive and costly as other undesirable business practices that have garnered attention of late, yet no more difficult to address.

Solving the underlying causes of economic espionage—corruption, poverty, and resource disparity—is not easy.[335] It is intuitively obvious theft is not the answer. The proposed convention would not eliminate the risk of industrial theft, though it would go a long way towards ensuring that governments do not remain accomplices to such activities.

335. *Id.* at 3.