Notes

CAUSES OF ACTION FOR FOREIGN VICTIMS OF ECONOMIC ESPIONAGE ABROAD BY U.S. INTELLIGENCE

There need be absolutely no dishonour in trying to ascertain what a potential or actual opponent is likely to attempt . . . . The risk of disrepute will depend on the extent to which the individual intelligence officer or his organization departs from the norms of morality in uncovering an opponent’s activities.

— R.V. Jones, former Director of British Intelligence

I. THE PROBLEM

The FBI defines economic espionage as “foreign power-coordinated intelligence activity directed at the U.S. . . . , which involves: (1) the unlawful or clandestine targeting or acquisition of sensitive financial, trade or economic policy information, proprietary economic information, or critical technologies; or (2) the unlawful or clandestine targeting or influencing of sensitive economic policy decisions.” In 1996 there were approximately 800 economic espionage matters under investigation by the FBI, directly implicating 23 foreign powers. The International Trade Commission estimated worldwide losses to U.S. industries at $23.8 billion in 1987 alone, and growing steadily—“Using the 1982 average loss ratio of $7 billion = 130,000 jobs, this would constitute a loss of about 450,000 U.S. jobs.” Further, in a report by the American Society for Industrial Security (ASIS) surveying 325 U.S. corporations, 700 incidents of proprietary loss were cited in 1995, an average of 32 incidents per month, with a

Copyright © 2001 by Michael Mosier.

4. Id.
total loss claimed for the 700 incidents at $5.1 billion.\textsuperscript{5} In 1997, ASIS reported those same losses to have exceeded $300 billion.\textsuperscript{6} Note also that any statistical margin of error should be presumed lower than actual numbers, due to the reluctance of companies to accurately report losses out of fear of investor backlash.\textsuperscript{7}

The effects of economic espionage are also less tangible in that they can stunt idea development. In testimony before the Select Committee on Intelligence, FBI director Louis Freeh noted in 1996 that the United States spends $249 billion on public and private research and development.\textsuperscript{8} Small companies who come up with unique ideas will quickly fold once larger foreign companies take each idea and mass produce it more cheaply.\textsuperscript{9} Companies lose incentive to develop technology when they have no way of protecting their creations and recouping their research costs.

With such significant national effects of economic espionage, national intelligence agencies have had to confront the issue vigorously. This entrance into the business arena has led to a vicious cycle of some national intelligence agencies corruptively spending billions of dollars each year in their economic espionage efforts, and counterintelligence agencies spending billions of dollars trying to thwart those efforts.\textsuperscript{10} During 1993 and 1994, the FBI “briefed nearly 250,000 persons at almost 20,000 companies, in addition to briefings at academic institutions, laboratories, and state and local governments” regarding economic espionage activities.\textsuperscript{11} The FBI reported that “its economic espionage caseload doubled from 400 in 1994 to 800 in 1995.”\textsuperscript{12} In 1996, the FBI had twenty agents assigned to trade secret theft investigations full time in Silicon Valley.\textsuperscript{13}

\textsuperscript{5} See id.
\textsuperscript{7} See Michael T. Clark, Comment, Economic Espionage: The Role of the United States Intelligence Community, 3 J. INT'L LEGAL STUD. 253, 255 (1997).
\textsuperscript{8} See Statement of Louis Freeh, supra note 3.
\textsuperscript{9} See, for example, Ellery Systems, Inc., developer of sophisticated communications software for NASA, who was undercut by a Chinese competitor who stole the trade secrets as Ellery was commercializing the proprietary information, and Dr. Raymond Damadian, holder of the first U.S. patent for an MRI device, who now has the smallest of all major companies in the MRI industry due to economic espionage by foreign competitors. For these, and other examples, see Clark, supra note 7, at 272-74.
\textsuperscript{10} Desmet, supra note 6, at 98.
\textsuperscript{11} Clark, supra note 7, at 270.
\textsuperscript{12} Desmet, supra note 6, at 97.
\textsuperscript{13} See Desmet, supra note 6, at 97.
The involvement of intelligence agencies also tends to raise the stakes of the game and worsen the situation as nations become more politically implicated. In February 1995, the French government publicly requested that five CIA operatives leave the country after having been caught allegedly stealing economic secrets in Paris.  

This cadre included one agent who allegedly paid approximately 100 dollars each time an aide to the Prime Minister provided information on French positions on matters being negotiated at GATT trade talks. Reports by France and Italy of industrial espionage by the United States have even sparked an inquiry in the European Parliament as to the actions of the CIA and its use of information from the global espionage system ECHELON. Given the dangerously growing problem of economic espionage and the involvement of national governments, we must make an affirmative movement toward reducing this trend.

Many of the papers cited herein already deal with federal criminal aspects of the issue. This Note aims to aid in the reduction of economic espionage by encouraging one of the most effective world actors, the United States, to clear its reputation so that it can lead with credibility. As a major industrial developer, the United States has an enormous stake in the issue. Whether it be the arms race, bankruptcy model law enactment, or bribery and other corruption prohibitions—for which the United States spearheaded combat with the Foreign Corrupt Practices Act—we have to get ourselves to a

---

14. See Clark, supra note 7, at 282-83.
15. See id.
16. See Answers to Frequently Asked Questions about Echelon, nn. 14, 16, 18, 25 & 28, and accompanying text (visited Aug. 24, 2000) <http://www.aclu.org/echelonwatch/faq.html> (citing sources including official reports of the European Parliament). Note that the NSA is actually the American intelligence agency behind ECHELON, but the CIA is being implicated for use of the information derived from ECHELON.
17. See UNCITRAL Model Law on Cross-Border Insolvency, 30th Sess., Report of UNCITRAL, U.N.Doc A/52/17 (1997), available at <http://www.un.or.at/uncitral/texts/insolven/mlinsolv.htm> (Model law to be enacted in the United States, rather than using an international treaty, with the reasoning that it would be quicker to take hold all around, for political reasons, than waiting for a requisite number of nations to ratify a treaty. Still pending before Congress.). See also 11 U.S.C. § 304, though, which has substantial aspects of the model law already in it, providing many rights for foreign creditors. In fact, the model law was based largely on U.S. Bankruptcy Code § 304, providing rights to foreign creditors in U.S. bankruptcy proceedings, subject to some comity discretion. See Prof. Steven L. Schwarz, Principles of Commercial and Bankruptcy Law class lecture, Duke University School of Law (Nov. 30, 2000).
18. “When the U.S. passed the Foreign Corrupt Practices Act, it was the only country in the world with a law that prohibits domestic companies and their agents from bribing foreign officials.” Clark, supra note 7, at 261-62.
moral high ground before we can legitimately and authoritatively entreat others to stop.

To this end of accountable legitimacy, this Note will investigate causes of action for victims of economic espionage abroad by U.S. intelligence. If the reports to the European Parliament are true, and the CIA has given confidential information about European businesses to U.S. companies to exploit, is there any redress for the European victims? The inquiry will naturally include economic espionage by private actors, since the disclosure of the information to private U.S. companies will be subsumed in the offense. Therefore, the more basic action against private actors, without the necessary complications of sovereign issues, will be partially dealt with as well. While this practical approach will deal with many procedural considerations, issues will remain regarding proof of causation and other substantive evidentiary concerns too tied to specific situations to fall within the scope of this undertaking. The Note will conclude with an explanation of the cause of action that does seem to exist, though with many complications. It will then argue that there should be more effective and specific recourse against the government for economic espionage occurring abroad. For instance, note the anomaly created where a foreign national could rather effectively sue any other government in a U.S. court for such quasi-commercial activity under a Foreign Sovereign Immunities Act commercial acts exception, but could not sue the United States itself who provides such a forum to sue everyone else.

II. RE COURSE

A. Fora and Substantive Law Options

The first step is to identify laws that address the problem of economic espionage. Unfortunately, international laws and courts are still too weak in enforcement to provide much help. It may be possible to construe economic espionage as a violation of customary law or of Article 2 of the U.N. Charter, as a “threat or use of force against the territorial integrity . . . of any state, or in any manner inconsistent

19. See 28 U.S.C.S. § 1605(a)(2) (“A foreign state shall not be immune from the jurisdiction of courts of the United States . . . in any case in which the action is based upon a commercial activity . . . that causes a direct effect in the United States.”); see also Republic of Argentina v. Weltover, Inc., 504 U.S. 607, 617 (1992) (explaining and applying the commercial activities exception where the Argentinean government was engaged in activity that was not uniquely sovereign, but rather commercial, in issuing debt bonds for payment in the United States).
with the purposes of the United Nations” if the spying moves from passive observation to proactive influencing of events (specifically commercial) within the nation. But again, enforcement would probably reduce to general political pressure from the victim’s government, which is quite unpredictable. International agreements may actually point a plaintiff back to individual countries for recourse, though. Under NAFTA, “[m]ember countries must protect trade secrets from unauthorized acquisition, disclosure or use.” GATT/TRIPS provides the same misappropriation remedies requirements for member countries.

The next step is to turn to domestic laws of countries, as directed by NAFTA and GATT/TRIPS. Not only are there simply too many countries’ laws to effectively survey here, there are general disadvantages for any plaintiff to sue the United States itself or its citizens in a foreign court. As will be discussed below with regard to political question issues and justiciability, the more a plaintiff can keep the case internal to another country, the less likely it is to be turned into a political question. For example, if one sues the CIA in other country, the State Department would probably intervene with the foreign government. But if whole suit is in the United States, then the United States cannot appeal to a foreign government so readily to circumvent the court. Instead, it has to deal with its own domestic court, which should be less vulnerable to attempts to turn an otherwise justiciable case into a foreign relations event, given predefined tests U.S. courts have for political issues. Similarly, for collection, the more a plaintiff can keep the whole controversy internal to the country where the assets of the defendant are, the more likely it will get paid because of fewer judgment enforcement issues.

---

22. See id. (not citing specific provisions).
23. See discussion infra beginning p. 15.
24. See infra notes 70-72 and accompanying text for discussion of these tests.
25. See, for example, requirements of reciprocity and other factors for enforcing foreign judgments in Hilton v. Guyot and its progeny. 159 U.S. 113 (1895). See Kohn v. American Metal Climax, Inc., 458 F.2d 255, 302 (3d Cir. 1972) (summarizing the criteria for enforcing a foreign country judgment). Note also that absent federal statute or a treaty, state law controls foreign judgment recognition, and states vary on a reciprocity requirement. See LAWRENCE W. NEWMAN & DAVID ZASLOWSKY, LITIGATING INTERNATIONAL COMMERCIAL DISPUTES 165, 172 (West 1996).
Then there are the famous/infamous unique procedural advantages of U.S. litigation for a plaintiff. First, Federal Rule of Civil Procedure (FRCP) 26 provides for broad discovery, which gives the right to ask the other party for damaging information, often not granted in other countries. Next, under the American Rule, parties pay their own lawyers, not just that the loser pays both, therefore making it more realistic for a plaintiff to attempt a suit. The United States adds the help of contingent fees, so that the lawyer is only paid if the plaintiff wins, again making the suit a safer gamble in complex and risky litigation, such as suing a sovereign. There is also a willingness of the U.S. system to monetize injuries that many other systems would say a court just cannot put a price on (such as loss of consortium, or mental injury). The U.S. court will simply tell a jury to put a price on it.\textsuperscript{26} There is also a right to jury trial in civil cases, which can lead to very high awards, including punitive damages, as well some wild cards in general where a jury may be moved more by emotional issues than a lone professional judge. All these distinctively plaintiff-friendly features of the American judicial system make it a natural starting point for our hypothetical plaintiff.

U.S. courts can be approached from either federal or state law. Federal law applicable to economic espionage includes the Economic Espionage Act\textsuperscript{27} and the Foreign Corrupt Practices Act,\textsuperscript{28} among others.\textsuperscript{29} However, most of these federal laws are aimed at protecting the United States and its citizens, not foreign private actors. Consequently, they are criminal statutes, which can only be invoked by prosecuting U.S. Attorneys, not private actors themselves. Given the inherent complications of a foreign national inducing a federal prosecutor to bring a case against the United States, as well as the remedies being criminal penalties rather than civil damages, there is not much reason to explore these federal laws further.

Instead the United States has generally left private actions in this sphere to the states to provide recourse, and the most applicable

\textsuperscript{26} Note that this feature is more a part of substantive tort law than procedure.
\textsuperscript{28} Pub. L. No. 100-418 (1988).
\textsuperscript{29} Under 18 U.S.C. § 1905 (2000), it is unlawful for any federal employee to disclose information acquired in the course of his employment that relates to “trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profit, losses, or expenditures of any person, or . . . [to permit] any income return or copy thereof . . . to be seen.” Under 26 U.S.C. § 7213(b) (2000) it is unlawful for a federal employee to disclose the operations “of any manufacturer or producer visited by him in the discharge of his official duties.”
cause of action is trade secret protection. Because it will be impossible to predict the most favorable state law in advance, the current discussion will be based on the Uniform Trade Secrets Act (UTSA)\(^\text{30}\) as a uniform proposed model, which many states have adopted.\(^\text{31}\) The UTSA creates a cause of action for both injunctive\(^\text{32}\) and monetary\(^\text{33}\) relief for misappropriation of trade secrets. “Misappropriation” is defined as

(i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (ii) disclosure or use of a trade secret of another without express or implied consent[,] by a person who . . . used improper means to acquire knowledge of the trade secret.\(^\text{34}\)

A “trade secret” consists of “information . . . that derives independent economic value . . . from not being generally known to . . . other persons who can obtain economic value from its disclosure or use.”\(^\text{35}\) “Person” includes a “governmental subdivision or agency, or any other legal or commercial entity.”\(^\text{36}\) Given that in the situation discussed herein the CIA has obtained the commercially useful information from a foreign business through espionage, we can reasonably consider that action “improper means.” Given the economic harm the disclosure to a U.S. competitor would cause, we can reasonably assume that any disclosure of the information would be without the implied consent of the foreign victim. Further, under the general principle that the CIA does not engage in commercial research for U.S. corporations, and moreover that it is known for foreign espionage, we can assume that any recipient U.S. corporation would have reason to know the information was “acquired by improper means.” Therefore, it should, in theory at least, be possible to hold both the CIA and the recipient U.S. corporation liable for their wrongdoing under most state trade secret laws. The question then becomes how to get to court and bring them with you.

33. See id. § 3.
34. Id. § 1(2).
35. Id. § 1(4).
36. Id. § 1(3).
B. Jurisdiction and Justiciability

1. General. Under the doctrine of comity, foreign nationals generally have a right to maintain actions that fall within the jurisdiction of the particular state or federal court without any special statutory authority. Further, the right to sue and the doctrine of comity generally apply to “artificial persons,” or corporations, in the same way as natural persons. The question then becomes how to obtain jurisdiction in the court to take advantage of comity.

The Federal Tort Claims Act (FTCA) grants federal court jurisdiction for tort actions against the government if a private party would have incurred liability under local law for the same actions. In fact, the FTCA is the exclusive mode of recovery for tort claims against the government. A plaintiff with a tort action under state law has a two-year statute of limitations from the time when the plaintiff “has or with reasonable diligence should have discovered the critical facts of both his injury and its cause” to file an administrative claim with the appropriate agency. Then, once administrative remedies are exhausted and relief still outstanding, a district court is conferred jurisdiction for the plaintiff to proceed with the action within six months of the denial.

37. See 3 C. AM. JUR. 2D Aliens and Citizens § 2564 (citing Dunlop & Co. v. Ball, 6 U.S. 180 (1804); Roberto v. Hartford Fire Ins. Co., 177 F.2d 811 (7th Cir. 1949); and Nizamuddowlah v. Bengal Cabaret, Inc., 399 N.Y.S.2d 854 (Sup. Ct. 1977)). Note that “[a]lthough Hilton v. Guyot, 159 U.S. 113, contains some broad language about the relationship of reciprocity to comity, the case in fact imposed a requirement of reciprocity only in regard to conclusiveness of judgments, and even then only in limited circumstances. Id., at 170-171. In Direction der Discontogesellschaft v. United States Steel Corp., 300 F. 741, 747 (D. C. S. D. N. Y.) [sic], Judge Learned Hand pointed out that the doctrine of reciprocity has apparently been confined to foreign judgments.” Banco Nacional de Cuba v. Sabatino, 376 U.S. 398, 411 (1964).

38. 36 A. M. JUR. 2D Foreign Corporations § 461 (citing Lathrop v. Commercial Bank of Scioto, 38 Ky. 114, 116, 8 Dana 114 (1839)).


43. Barrett v. United States, 689 F.2d 324, 326 (2d. Cir. 1982).

Misappropriation of trade secrets is a tort under state law, so we can begin with the FTCA.\(^{45}\) However, the FTCA specifies that the violation must “arise” in the United States, not abroad.\(^{46}\) This requirement is troublesome in the situation at hand because trade secret law consists of two violations: taking the secrets and then disclosing them to someone for use. The rub is that the secrets would be acquired abroad, but might be disclosed domestically in the United States. No reported cases have directly considered where trade secret cases fall for the purpose of establishing FTCA violation locus. However, we can look to how courts have resolved the issue of which state’s laws to use in these bifurcated actions, which should count heavily in a determination of where the claim arose for FTCA purposes.

Unfortunately, courts are somewhat divided as to the application of choice of law principles in trade secret cases. However, most courts surveyed tend to lean towards counting the principle place of business of the defendant (here, the United States) as the most significant factor rather than the principle place of business of the plaintiff (here, abroad), though the latter otherwise often weighs heavily in conflicts of law analysis of significant relationships.\(^{47}\) Courts use the defendant’s citizenship in trade secret cases because that is where the information was used or the benefit obtained, and therefore, where the wrong was committed.\(^{48}\) Courts have noted that in many other trade related cases the injury will “normally be felt most severely at the plaintiff’s headquarters . . . this place may have only a slight relationship to the defendant’s activities and to the plaintiff’s loss of customers or trade. [Also,] the plaintiff may have suffered no pecuniary loss but the defendant rather may have obtained an unfair profit,” such as where the defendant gains market advantage even where the


\(^{46}\) See 28 U.S.C.S. § 2680(k) (excepting the provisions of the FTCA from “Any claim arising in a foreign country.” Id.); see also id. at note 218 (citing Lassiter v. United States Lines, Inc., 370 F. Supp. 427 (E.D. Va. 1973)).

\(^{47}\) That is, often the jurisdiction of the plaintiff has the most significant relationship to the matter due to the court’s interest in protecting the harmed plaintiff.

\(^{48}\) See, e.g., Venango River Corp. v. NIPSCO Industries, 1994 U.S. Dist. Lexis 2700, *9 (N.D. Ill. Mar. 8, 1994) (Court also noted Restatement (Second) of Conflicts of Laws § 145 comment (f) (1971) that the principal location of defendant’s conduct is to be given the greatest weight in trade secret misappropriation cases.).
plaintiff was not yet doing business. Under this analysis, the court would consider the determinative damage to have occurred in the United States, where the CIA disclosed and the corporate defendant received and used the information. This outcome is justified because three of the four violating acts occurred in the United States: disclosure, knowing receipt of misappropriated information, and use of that information—whereas, only one act, the taking, happened abroad.

On the other side, however, there are still courts that stick to the “most significant relationship” test of §§ 6 and 145 of the Restatement (Second) of Conflict of Laws (1971). This analysis is tougher for our foreign plaintiff because of factors such as the interests of the various fora in the matter. The defendant would argue that the domicile of the foreign plaintiff would want to protect its businesses, and so would have a significant interest in taking the case. Indeed, in Victor Equipment Co. v. Armco Steel Corp., the court stressed the location of the plaintiff as the place where the injury was sustained. However, it is possible that this determination was partly driven by the desire to be able to litigate the issue in the United States to protect the plaintiff, rather than send the case to Mexico where the judicial system might have been less responsive to the American plaintiff, and where awards and enforcement might have been less reliable.

Finally, as some consolation, at least one FTCA case has suggested that where an issue of fact exists with respect to whether the acts proximately causing the damage occurred both in the United States and a foreign country, the case must at least survive summary dismissal. Another case denied summary judgment for the CIA defendant for drug experimentation that resulted from funding and supervision of experiments in the United States although the injuries were suffered by plaintiffs in Canada. Since misappropriation includes either acquisition “or” disclosure, one could probably sue only on the disclosure violation to avoid falling out of the “arising in the U.S.” requirement. However, from an evidentiary standpoint, the plaintiff will most likely be required to deal with the misappropriation


that occurred abroad in some fashion in order to show that the defendant should have known the information it received was misappropriated. The plaintiff’s problems may not end just because it can theoretically get into court past summary dismissal.

There also are venue complications with a nonresident alien suing in federal court, even though the action need only trigger state law. Case law has suggested that the FTCA is not limited to citizens of the United States; in fact, unlike actions by foreign nationals in the Court of Claims under the Tucker Act, the FTCA does not even have an explicit requirement of reciprocity. However, other cases have stated that

[since, in the case of individual plaintiffs, actions against the United States may be brought only in the judicial district in which the plaintiff resides, nonresident aliens who cannot be considered to be residents of any federal judicial district are unable to sue in the District Courts, and are limited to bringing actions in the U.S. Court of Federal Claims.

Because the U.S. Claims Court does not have jurisdiction over tort claims, specifically actions under the FTCA, this rule would preclude any action by a foreign plaintiff for trade secret misappropriation. At least one case directly disallowed an FTCA action by a Canadian corporation, though it had an agent in the state of New York, because it was not a citizen of the state so as to be within venue of the “district court within [the] meaning of 28 USCS § 1402(a) for purpose of maintaining [an] action against [the] United States under 28 USCS 1346.”

The text of the statute itself provides reason to be skeptical about the cases denying FTCA jurisdiction for nonresident aliens. While 28 U.S.C.S. § 1402(b) states that any tort claim against the United States under the FTCA “may be prosecuted only in the judicial district where the plaintiff resides,” it also provides the option of “or wherein the act or omission complained of occurred.” This latter provision implies that if a plaintiff in our discussion could show, as

55. See 3 C. AM. JUR. 2D Aliens and Citizens § 2581; United States v. South Carolina State Hwy. Dept., 171 F.2d 893, 899 (4th Cir. 1948).
56. 3 C. AM. JUR. 2D Aliens and Citizens § 2587 (citing 28 U.S.C.A. § 1402(a)(1) and Mala- jalian v. U.S., 504 F.2d 842 (1st Cir. 1974)).
60. (emphasis added).
discussed above with trade secret occurrence/injury analysis, that the act occurred in a particular district, venue should be available under 28 U.S.C.S. § 1402(b) for a federal court. The Supreme Court highlighted this opinion in *Smith v. United States*, in which it pointed out that Congress did not intend to create “venue gaps, which take away with one hand what Congress has given by way of jurisdictional grant with the other.” 61 The Court decried the anomaly created by rulings such as the case of the Canadian corporation above where the lower court held that the FTCA would create jurisdiction specifically for foreign nationals for tort claims against the United States, but that foreign plaintiffs would be denied venue unless they happened to reside in the United States. 62 Unfortunately for the plaintiff in that case, the Court used that reasoning to add to its decision to deny plaintiff’s argument that although the tort arose in Antarctica—which, though sovereignless, was still considered a foreign nation for the exception to the FTCA—she should still be able to bring the claim in her home state of Oregon.

Between the Supreme Court ruling and the statute, one would think that a foreign corporation would not be absolutely barred for lack of incorporation in the desired forum state; however, it is important to remember that some district courts have given foreign nationals some venue trouble. Further, according to the statute, they will probably be limited to the venue of the district in which the violation occurred. This requirement also precludes forum shopping for the most favorable state law to use under the FTCA and means that the plaintiff will be limited to the applicable misappropriation law of the state of the violation. Additionally, this limitation could cause personal jurisdiction issues for the unique tort involved here because there are two defendants. While this bifurcation may allow for two choices of venue, it also means that the chosen venue must have jurisdiction over both defendants. Depending on where the plaintiff claims the act occurred, if either of the defendants does not have sufficient minimum contacts with that state, the court may lack jurisdiction to adjudicate over that defendant. 63 So, the venue and choice of law problems for the plaintiff are not fully resolved by the statute and Supreme Court ruling.

62. See id.
In addition to these technicalities for the particular laws involved, we must also deal with general justiciability for the action to proceed in federal court,\(^{64}\) even though it is based on state law claims.\(^{65}\) First there is the constitutional “case or controversy” requirement\(^{66}\) that there must be a real controversy between parties having adverse legal interests,\(^{67}\) not a request for a mere advisory opinion,\(^{68}\) but an “injury in fact” to the actual plaintiff bringing the case, caused by the defendant’s actions, and which could be redressed by the requested relief from the court.\(^{69}\) These requirements should not be a problem in our discussion action. We have the actual victim, not a third party, bringing the case, with a specific economic injury caused by the misappropriation and disclosure of its trade secrets by the CIA to a U.S. corporation co-defendant. The injury already happened, so the decision is not hypothetical or advisory, and the administrative remedies failed to rectify the situation, so the case has not become moot. One final case or controversy issue remains, however.

The case must not involve a nonjusticiable political question with “a textually demonstrable constitutional commitment” to another branch of government or “a lack of judicially discoverable and manageable standards for resolving the issue.”\(^{70}\) This requirement “[e]xcludes from judicial review those controversies which revolve around policy choices and value determinations constitutionally committed for resolution to the halls of Congress or state legislatures or to the confines of the executive branch”\(^{71}\)—for example, foreign policy issues such as immigration-related claims.\(^{72}\) First, in our case there are clear standards for resolving the issue, provided by the FTCA and state trade secret law. Second, it is perhaps a policy choice to collect information, but it is not a valid choice to disseminate in violation of our own U.S. law.

\(^{64}\) See U.S. Const. Art. III, § 2.
\(^{65}\) See 32A AM. JUR. 2D Federal Courts § 674 (noting that “the jurisdictional constraints of Article 3 do not apply to the state courts.”) (citing ASARCO, Inc. v. Kadish, 490 U.S. 605 (1989) and U.S. Dept. of Labor v. Triplett, 494 U.S. 715 (1990)).
\(^{71}\) See 32A AM. JUR. 2D Federal Courts § 674 (citing Japan Whaling Ass’n v. Am. Cetacean Soc, 478 U.S. 221 (1986)).
\(^{72}\) See, e.g., Padavan v. U.S., 82 F.3d 23 (2d. Cir. 1996).
Three documents address the limits of foreign intelligence collection: Executive Order 12,333,\(^73\) the Intelligence Authorization Act (IAA),\(^74\) and the Foreign Intelligence Surveillance Act (FISA).\(^75\) While Executive Order 12,333 generally permits the collection and dissemination of “[i]nformation constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations,”\(^76\) it specifies absolutely that “[n]othing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.”\(^77\) Therefore, while the CIA may be authorized to collect commercial data, as it relates to the “areas of national defense and foreign relations,”\(^78\) it would violate trade secret statutes to disseminate the information to U.S. companies. The general authorization in § 2.3 of dissemination is superceded and limited by the preservation of statutory prohibitions in § 2.8, which may still allow some intergovernmental dissemination, but certainly not to U.S. companies for business use. Similarly, the IAA states unequivocally that “authorization of appropriations by this Act shall not be deemed to constitute authority for the conduct of any intelligence activity which is not otherwise authorized by the Constitution or laws of the United States.”\(^79\)

FISA goes further into detail in authorizing a court or the Attorney General to approve surveillance only if “solely directed at . . . communications used exclusively between or among foreign powers [or their agents] . . . ; or technical intelligence . . . from property or premises under the open and exclusive control of a foreign power.”\(^80\) An “agent of a foreign power” is “any person other than a United States person, who . . . acts for or on behalf of a foreign power which engages in clandestine intelligence activities.”\(^81\) All variations of the definition include some requirement of clandestine or criminal activities under U.S. statutes, thus ruling out our hypothetical plaintiff, which is conducting an ordinary business. FISA defines “foreign

\(^76\) Exec. Order 12,333, supra note 73, § 2.3.
\(^77\) Id. § 2.8.
\(^78\) Id. § 2.1 (setting out the purposes of intelligence gathering, with no mention of commercial or economic interests).
\(^79\) Intelligence Authorization Act, supra note 74, § 402.
\(^80\) 50 U.S.C.S. § 1802(a) (for Attorney General authorization); see also 50 U.S.C.S. § 1805(a)(3)(B) (for court authorization, with equivalent language).
\(^81\) 50 U.S.C.S. § 1801(b).
power” as “a foreign government or any component thereof . . . ; [or] an entity that is directed and controlled by a foreign government.”

So, arguably, we might be able to consider any government business, like a state-owned bank or utility industry, a foreign power for authorized surveillance. However, other sections limit what can be done with that acquired information, and dissemination of it to U.S. corporations in violation of trade secret law would be prohibited since “[n]o information acquired from an electronic surveillance pursuant to this title may be used or disclosed by Federal officers or employees except for lawful purposes.”

All three delineations of foreign surveillance contain overriding provisions specifically prohibiting use of collected information in violation of U.S. law.

Therefore, the policy choice and value determination that could be committed to the executive have already been made. Similarly, the legislatures have already addressed the issue by making such dissemination of commercial secrets illegal under trade secret laws and setting the general standards for addressing torts by the government under the FTCA. Therefore, it is left to the judiciary to rule on actions outside the prescribed limits of intelligence activities of the executive or the legal limits of activity set by the legislature, unless the government defendant can invoke other shields to adjudication.

2. **Trumping Wildcards.** The initial affirmative defense that must be considered is that of sovereign immunity, since the CIA is a government agency and “[a]bsent a congressional waiver, this sovereign immunity shields the Federal Government and all its agencies.” However, the “FTCA is a broad waiver of federal sovereign immunity, . . . [granting] jurisdiction to federal district courts to hear . . . tort suits against the United States.” Therefore, the complete bar of sovereign immunity is not a problem.

There are also built-in statutory exceptions to the FTCA, however, providing subject matter jurisdiction dismissal for “[a]ny claim . . . based upon the exercise or performance or the failure to exercise or perform a discretionary function or duty on the part of a federal agency or an employee of the Government, whether or not the discre-

---

82. 50 U.S.C.S. § 1801(a).
83. 50 U.S.C.S. § 1806(a).
tion involved be abused.” Courts have used a two-part test “to determine whether the challenged conduct falls within the exception.”

First, they look “to the nature of the conduct itself, rather than the status of the actor,” then to “whether the action is a matter of choice for the acting employee.” Further, however, “the discretionary function exception does not apply if ‘a federal statute, regulation, or policy specifically prescribes a course of action for an employee to follow’ or if ‘the acts complained of do not involve the permissible exercise of policy discretion.’” Since the Executive Order 12,333, IAA, and FISA all prohibit illegal disclosure of information obtained in surveillance, it would seem quite difficult for the CIA defendant to claim any discretion involved in its decision to act contrary to the three controlling authorities for its actions. However, as with any discretionary test to be applied in courts, “one thing is sure: the Supreme Court, with all due respect, by its undulations from Dalehite to Indian Towing and Rayonier to Varig Airlines to Berkowitz [sic] provides anything but a predictable certitude on what is, or is not, within a discretionary function.” Therefore, while the issue looks favorable for our plaintiff, it is hardly certain.

A similar affirmative defense outside of the FTCA itself is qualified immunity, which shields an administrative officer from liability for activities that are “within the scope of her office, are in objective good faith, and do not violate clearly established statutory or constitutional rights of which a reasonable person should be aware.” However, courts have stated that “[i]f the law was clearly established, the immunity defense ordinarily should fail, since a reasonably competent public official should know the law governing his conduct.” In our hypothetical situation, we have already ruled out the discre-

86. Kelly, 924 F.2d at 359-60 (citing 29 U.S.C. § 2680(a)).
87. Id. at 360.
90. Kelly, 924 F.2d at 360 (quoting Berkovitz v. United States, 486 U.S. 531, 546 (1988)).
91. See supra notes 73-83 and surrounding text.
97. Kelly, 924 F.2d at 364 (Brown, S.J., concurring in the judgment).
98. 2 A M. JUR. 2D Administrative Law § 653 (citing Harlow et al. v. Fitzgerald, 457 U.S. 800 (1982)).
tionary option above. Further, that dismissal notwithstanding, given that trade secret law is well established in the United States, including the federal criminal Economic Espionage Act, with which intelligence agencies deal more than most people, there should be little room for a CIA defendant to claim objectively reasonable ignorance of the state of the law.

If no complete bars keep the defendant out of court, the defendant may still be able to keep significant information out of court under state secrets privilege. “[M]atters the revelation of which reasonably could be seen as a threat to the military or diplomatic interests of the nation . . . are absolutely privileged from disclosure in the courts.” There is no balancing of interests; no necessity can overcome the claim of privilege once “the court is satisfied that the information poses a reasonable danger to secrets of state.” However, a second inquiry then arises as to whether the case is to proceed as if the privileged matter had simply never existed, with the parties bearing the consequent disadvantages (or advantages) of this sudden disappearance, or instead should proceed under rules that have been changed to accommodate the loss of the otherwise relevant evidence. Such changes could compensate the party ‘deprived’ of his evidence by, for example, altering the burden of persuasion upon particular issues, or by supplying otherwise lost proofs through the device of presumptions or presumptive inferences.

There is reason to be skeptical, rather than hopeful for such compensation, however.

For instance, in the landmark national security case Halkin v. Helms, the court declined to alter the parties’ burdens in any way, despite a broad denial of information involving primarily domestic CIA activities during the Vietnam War era, twenty years prior to the case. Though the plaintiffs only requested information regarding “the identities of the plaintiffs [themselves] who were subjected to surveillance,” not CIA operatives or liaison services, the court opined that it would not force disclosure of any information from which one could deduce in anyway an embarrassing connection with a foreign

102. Id. (citing United States v. Reynolds, 345 U.S. 1, 11 (1953)).
103. Id.
104. Id.
nation or the identity of a past operative. The court noted that “the identity of particular individuals whose communications have been acquired can be useful information to a sophisticated intelligence analyst.” Therefore it seems unlikely that the privilege will be denied once invoked, given the deference to err on the side of protection. Further, it seems accommodation will rarely be granted, given that even facts only relating to the plaintiff itself can be absolutely barred without any balancing, since it is possible for an intelligence expert to deduce information about past U.S. intelligence activities simply through knowing the names of Vietnam protesters who were spied on during the 60s. Indeed, the court was even willing to presume not necessarily that the CIA had anything to hide, but “that it wishes to hide from our adversaries the fact that it has nothing to hide.”

So the CIA could block evidence that would show it actually did engage in economic espionage because of the effects on the diplomatic relationship with the victim nation. Additionally, it could claim general national security privilege in the military interest of the nation because divulging information about the espionage activities of the CIA needed for the case would give away too much and threaten national security. Note that there is little chance of helpful compensation for the deprived party in our situation, because the information needed from the CIA is fundamental to the action itself, rather than ancillary proof to drive the point home. It is quite unlikely that a court would make presumptive inferences or shift the burden of proof outright on a basic element of the claim, akin to forcing the defendant corporation to prove that it did not receive the information from the CIA, who did not acquire it through economic espionage. Such a fundamental shift to guilty until proven innocent seems too much the antithesis of the American legal process to occur.

C. Remaining Procedural Issues: Joinder and Subpoenas

Given the complications with involving the government as a defendant, we must consider the possibility of proceeding with the suit against the recipient company defendant alone, and the accompanying complications of such a strategy. Federal Rules of Civil Procedure provide that “[a] person who is subject to service of process and

105. Id. at 991-93 (emphasis in original).
106. Id. at 993 (quoting itself in Halkin I, 598 F.2d 1, 8 (D.C. Cir. 1976)).
107. Id. at 994.
whose joinder will not deprive the court of jurisdiction over the subject matter of the action shall be joined as a party in the action if . . . in the person’s absence complete relief cannot be accorded among those already parties.”108 Will it deprive the court of jurisdiction to add the CIA? No, it will not affect the diversity jurisdiction because both defendants are domestic and the plaintiff is foreign. Also, the FTCA waives sovereign immunity. The question is whether the actions against the CIA will be justiciable, though, based on political question issues.109 Can complete relief be accorded among those already parties? Perhaps adequate relief can be achieved, as discussed in the following paragraph, but not really complete relief because one type of defendant will be missing (i.e., the acquirer) under the trade secret law. Also, as discussed previously,110 the plaintiff needs to be able to satisfy personal jurisdiction contact requirements in order to call the defendants to the court. So it may not be possible to bring both defendants to court, based on personal, not subject matter, jurisdiction problems.

The rules further stipulate that

[i]f a person . . . cannot be made a party, the court shall determine whether in equity and good conscience the action should proceed among the parties before it, or should be dismissed, the absent person being thus regarded as indispensable. The factors to be considered by the court include: first, to what extent a judgment rendered in the person’s absence might be prejudicial to the person or those already parties; second, the extent to which, by protective provisions in the judgment, by the shaping of relief, or other measures, the prejudice can be lessened or avoided; third, whether a judgment rendered in the person’s absence will be adequate; fourth, whether the plaintiff will have an adequate remedy if the action is dismissed for nonjoinder.111

Looking at the factors in order, first, the judgment would probably not be prejudicial to the CIA because if not joined the CIA will have to be brought to trial separately and will have its own host of special defenses as a sovereign. If anything, the CIA has the information the plaintiff needs, and will not get without it, so a case without the CIA will not significantly prejudice the CIA in any way. Not joining the CIA will be beneficially prejudicial for the corporate defendant because the plaintiff will have problems without the CIA’s supply of

109. See supra notes 70-72 and surrounding discussion.
110. See supra note 63 and surrounding text.
evidence. However, the continued adjudication of the case will be prejudicial against the plaintiff for the same reasons. Second, the prejudice to the plaintiff could be lessened by allowing inferences of evidence in the plaintiff’s favor that are reasonably shown. Third, the remedy with just the corporation might be adequate because it would stop the passing of trade secrets if corporate recipients could be brought to court, even if the CIA could not. But the plaintiff would probably have causal problems bringing a case against a recipient if could not show the defendant acquired the information inappropriately from the CIA. So the plaintiff would really need the CIA as a party to prove the transitive offense, though the plaintiff would need enough evidence of misappropriation by the CIA to get past summary dismissal from the beginning either way. Fourth, there is probably no adequate remedy for the plaintiff without the action, because there is not much legal recourse left for the plaintiff to use, especially in U.S. courts. So the fourth factor weighs heavily in the plaintiff’s favor. In conclusion, the bad news is that the CIA may not be joined; however, at least the factors weigh in favor of the case proceeding even if the CIA cannot be joined.

For further illumination of the issue, consider the following case. A complaint against the Burmese government and its state-owned oil company was dismissed based on sovereign immunity, but not dismissed as to the U.S. corporate defendant, Unocal, for failure to join an indispensible party under FRCP 19. Though Unocal argued that the absence of the state defendants meant that the case could not be fully and fairly adjudicated, as required under Rule 19, the court refused, maintaining that the plaintiffs could obtain the core relief they sought of cessation of the corporate enterprise while the human rights abuses continued, from the remaining corporate defendant. In our case, relief of damages and cessation of use of the trade secrets could theoretically be obtained simply from the corporate defendants. The issue is more that evidence rather than relief itself cannot be obtained without the CIA. The actual relief of damages could come from either defendant, and in fact the corporate defendant is arguably the more appropriate compensator because it benefited economically from use of the trade secrets.

Fortunately, there may be some possibility of evidentiary help from the CIA even if it is not joined as a defendant because one of the bars to joinder or jurisdiction. In a case brought by the father of

Dodi al Fayed requesting information from the CIA relating to the death of his son and Princess Diana, the court referenced an appellate holding that the broad defense of sovereign immunity was not applicable to a federal court subpoena issued to a government agency that was not a direct party to the lawsuit.\footnote{See \textit{In re Application of Mohamed al Fayed}, 91 F. Supp. 2d 137, 138 (D.D.C. 2000).} The court in the \textit{Fayed} case, however, ultimately denied the subpoena because it must have subject matter jurisdiction over the subpoena in question.\footnote{See \textit{id.} at 139.} Mr. Fayed relied solely upon 28 U.S.C. § 1782 for his action to issue the subpoena and that statute only applies to a “person” rather than to an entity such as a federal agency.\footnote{See \textit{id.} at 140.} Without a proper statute conferring subject matter jurisdiction for the federal court to adjudicate, it was without authority to issue the subpoena. The court left it open as to whether another statute might confer the proper subject matter jurisdiction to issue a subpoena to a government agency, though specifically hinted that it was not ruling on the matter of whether a particular officer might be called, as a person, distinct from a federal agency.\footnote{See \textit{id}.} In fact, though the subpoena was ultimately denied on other grounds of undue burden and state secrets privilege, another federal court in the process of its decision at least gave a general indication, by even getting to those bars, that it considered itself to have authority to issue the subpoena to the FBI and CIA merely through the discovery provisions of the Federal Rules of Civil Procedure.\footnote{See \textit{Linder v. Calero-Portcarrero}, 180 F.R.D. 168, 173 (D.D.C. 1998).} Therefore, while a court can enforce a subpoena against a sovereign regardless of sovereign immunity, it may not have the jurisdictional authority to issue such a subpoena. In further complication, the \textit{Fayed} court also cited a split of circuit decisions on the issue of the authority to issue a subpoena to a sovereign entity at all, including specific officers themselves.\footnote{See \textit{Fayed}, 91 F. Supp. 2d at 139.} Therefore, the authority for a court to issue a subpoena to a sovereign at all remains in question until the Supreme Court takes up the issue. Further, this subpoena power is also subject to state secrets privileges and traditional subpoena limitations such as undue burden. Therefore, it is unclear how much help the possibility of a subpoena really would be, and evidentiary issues remain unsettled for our foreign victim.
III. CONCLUSION

Some cause of action does in principle exist for foreign nationals who are victims of economic espionage by U.S. intelligence, through the FTCA and state trade secret law. However, so many complications accompany that cause of action that there is a question whether any cause of action really exists in practice. For instance, no court has directly ruled on how to resolve where exactly the trade secret violation will be considered “arising” for purposes of the FTCA under the dual actions of acquisition and disclosure. Further, the closest analysis of the issue in the context of conflict of laws presents a split of decisions. The statute and Smith v. United States\(^\text{119}\) seem to provide some resolution of the court divide on the issue of whether a foreign corporation with no residency in any federal district can sue in district court at all, other than Federal Claims Court. However, the FTCA statute limits forum choices for the plaintiff to wherever the court deems the violation to have occurred—again bringing us back to the problem of the bifurcated trade secret misappropriation law. This limitation on venue choices also leads to personal jurisdiction problems because there are two defendants, the original acquirer/discloser and the recipient, and the court must satisfy personal jurisdiction requirements to call either one. The venue restriction, resulting personal jurisdiction limitations, and separate sovereign issues of immunity and political question lead to joinder issues where the court may dismiss the case if an “indispensable” party cannot be properly joined. There are discretionary exceptions within the FTCA itself, as well as omnipresent qualified immunity exceptions for any administrative agency actions. Additionally, the broad state secrets privilege may bar disclosure of important evidence for the plaintiff’s case. Finally, if the government cannot be joined, but the case is to proceed, there is a court split regarding whether the sovereign can be subpoenaed for evidence, and even if it can, the subpoena is subject to limitations of state secret privilege and undue burden. With all these variables, it is nearly impossible not to be skeptical of any claimed recourse provided for victims of economic espionage abroad by U.S. intelligence.

Given these limitations, then, there are several reasons why a more reliable and genuine means of redress should be provided for such victims, not just for their benefit, but for the benefit of the

\(^\text{119.} 507\text{ U.S. 197 (1993).}\)
United States. Note that under the applicable laws,\textsuperscript{120} even a U.S. company whose branch or subsidiary abroad was a victim of economic espionage by the CIA (presumably not intentionally, but negligently perhaps) may not have a satisfactory cause of action simply because the violation technically arose abroad, rather than in the United States. Our own subsidiaries abroad or indirect partnerships could unwittingly be victims and they may have no recourse due to many of the same problems here, such as the “arising abroad” exception and other sovereign immunity and evidentiary bars. As writers in this area of the muddied interaction between private enterprise and intelligence have pointed out, “given the fragmentation of ownership, management, and employment of most international firms, defining a strictly American or strictly Canadian firm[,] for example[,] . . . becomes problematical.”\textsuperscript{121} A former Director of the CIA queried whether an “American corporation” covers one which is “headquartered in New York, but does most of its manufacturing in Canada . . . [or] a Canadian corporation that manufactures largely in Kentucky? Who knows.”\textsuperscript{122} Further, as U.S. citizens, we want to avoid the likely conflicts of interest and corruption resulting from U.S. intelligence possessing inside information that is useful to multiple competing companies in the United States. This situation would lead to at least the temptation for compromises in the integrity of the U.S. intelligence community as companies vie for the information. We could end hypocrisy while helping our nationals at the same time simply by applying our own Foreign Sovereign Immunities Act exceptions\textsuperscript{123} to ourselves instead of only to every other sovereignty.

This Note is not directed against the United States or CIA. It is really in our best interest to be able to push for stronger economic espionage laws everywhere because we are spending billions of dollars fighting it,\textsuperscript{124} and we happen to be creating a large percentage of the

\textsuperscript{120} The same FTCA, needed to sue the government for a tort, and state trade secret law.
\textsuperscript{121} Robert David Steele, \textit{Private Enterprise Intelligence, in Intelligence Analysis and Assessment} 212, 219 (David A. Charters et al. eds., 1996).
\textsuperscript{123} See 28 U.S.C.S. § 1605(a)(2) (“A foreign state shall not be immune from the jurisdiction of courts of the United States . . . in any case in which the action is based upon a commercial activity . . . [and] that act causes a direct effect in the United States.”); see also Republic of Argentina v. Weltover, Inc., 504 U.S. 607, 617 (1992) (explaining and applying the commercial activities exception where the Argentinean government was engaged in activity that was not uniquely sovereign, but rather commercial, in issuing debt bonds for payment in the United States).
\textsuperscript{124} See Desmet, supra note 6, at 98.
technology falling prey to such espionage. If the United States does not offer a satisfactory cause of action for these crimes, it will be nearly impossible for our nationals to get similar relief for the same crimes committed against us abroad, whether unwittingly by our own intelligence agencies (due to procedural and sovereign issues) or by foreign intelligence (due to politics of reciprocity and judgment enforcement). If we are not doing anything wrong, we have nothing to worry about in opening ourselves to accountability. Meanwhile, France and Israel have been notorious offenders in this area, so it would be beneficial to have a cause of action against them in their own courts, where seizure of assets and judgment enforcement may be more practicable, rather than trying to bring over a foreign judgment from FISA exceptions used in the United States. Former CIA Director, R. James Woolsey, bluntly made the point about our greater need to protect ourselves from others than worrying about our own liability: “True, in a handful of areas European technology surpasses American, but, to say this as gently as I can, the number of such areas is very, very, very small. Most European technology just isn’t worth our stealing.” Meanwhile, we risk chilling creative output in Woolsey’s grand United States for lack of idea protection. As leading world developers, we really do have more to lose than to gain by lax economic espionage laws, even if we have to get down from our raft of immunity to pull others into the pool.

Michael Mosier

125. See Statement of Louis Freeh, supra note 3.
126. See, e.g., comments in note 25 regarding requirements of judgment enforcement.