

To eliminate a dilemma

DISCLOSURE PROBLEMS IN ESPIONAGE PROSECUTIONS

George W. Clarke

Enforcement of the principal provisions of the United States espionage laws often poses a serious problem for our defense and intelligence agencies. The statutes at issue, 18 U.S.C. §§793 and 794, are among the most often used in espionage prosecutions. Since these statutes actually or potentially necessitate damaging disclosures of national security information¹ to defense counsel and, through public trial, to foreign adversaries during the course of prosecution, the statutes should be reformulated to eliminate this dilemma unless such disclosures are required as a matter of law or for some other compelling reason.

Statutes

Title 18 U.S.C. §§793 and 794 (Appendix A), respectively, proscribe the gathering or obtaining of documents or information "relating to the national defense"² and the communication or delivery, or attempted communication or delivery of such documents or information to a foreign government or faction or an agent thereof. To be proscribed, such acts must be done with "intent or reason to believe" that the documents or information are "to be used to the injury of the United States or to the advantage of a foreign nation." These requirements are a problem because they impose upon the government the obligation to prove to a jury in open court that the documents or information at issue are related to the national defense and that the defendant acted with the requisite intent or knowledge.

Elements of Proof

To obtain a conviction under 18 U.S.C. §§793 and 794, the government must prove that the documents or information at issue in the case meet the statutory standard. In *United States v. Gorin*, 312 U.S. 19 (1941), the Supreme Court adopted a broad definition of what information relates to the national defense.

National defense, the Government maintains, is a "generic concept of broad connotations, referring to the military and naval establish-

¹ "National security information" is intended to mean information which would be subject to the various espionage statutes. As will be seen, as a practical matter this means classified information.

² 18 U.S.C. §793(a) uses the phrase "respecting the national defense" to describe the covered information and documents while 18 U.S.C. §§793(d)-(f) and 794(a) use "relating to the national defense" and §794(b) uses "relating to the public defense" (emphasis added). No distinctions were intended by the use of these differing formulations.

Prosecutions

ments and the related activities of national preparedness." We agree that the words "national defense" in the espionage act carry that meaning.³

Under such a broad definition, however, it would be difficult for a person to know what specific acts are proscribed, since many foreign communications, dealings, and relationships in the private and commercial sectors pertain to military-related matters. The Court disposed of such overbreadth objections in *Gorin*:

... we find no uncertainty in this statute which deprives a person of the ability to predetermine whether a contemplated action is criminal under the provisions of this law. The obvious delimiting words in the statute are those requiring "intent or reason to believe that the information to be obtained is to be used to the injury of the United States, or to the advantage of any foreign nation." This requires those prosecuted to have acted in bad faith. The sanctions apply only when scienter is established.⁴

Since the obtaining and transfer of national defense information is thus proscribed only when done with the requisite "bad faith," in the absence of self-incriminating statements or a confession by the defendant, about the only way to convince a jury on this element is to prove that the information is so important that the defendant had to have an intent or reason to believe that his acts would injure the United States or benefit a foreign state.

The cases subsequent to *Gorin* developed further what information was excluded from coverage and how the government could go about proving that information relates to the national defense. Thus, information released by the defense establishment or which is otherwise publicly available is not covered by the statutes, regardless of the defendant's intent.⁵ On the other hand, the fact that the information at issue is classified is admissible as evidence of defense-relatedness,⁶ although a jury would still have to determine as a separate matter that the defendant had an intent or reason to believe that the information would injure the United States or give advantage to a foreign nation.

Costs of Disclosure

A CIA General Counsel once stated that "nobody doubts the proposition that some prosecutions, and due to the elements of the relevant offenses, virtually all espionage prosecutions, cannot be maintained except at the price of disclosing information that otherwise would and should remain secret for

³ *Gorin v. United States*, 312 U.S. at 28.

⁴ *Id.* at 27.

⁵ *United States v. Heine*, 151 F.2d 813 (2d Cir. 1945), *cert. denied*, 328 U.S. 333 (1946).

⁶ *United States v. Soblen*, 301 F.2d 236 (2d Cir.), *cert. denied*, 370 U.S. 944 (1962).

Prosecutions

reasons of national security."⁷ While this statement was made broadly with respect to all prosecutions that in some manner may require the disclosure of classified information to enable the case to go forward, it clearly represents a judgment that espionage cases in particular exact a high price. While the Classified Information Procedures Act (CIPA)⁸ has established a statutory framework to obtain pretrial and trial rulings concerning the relevancy of classified information claimed to be necessary in federal criminal prosecutions, it is primarily of benefit in non-espionage cases where the defendant seeks broad discovery of sensitive classified matters (often unrelated to any real issue concerning the government's case or any defense) in order to force the government to drop the case rather than disclose the requested information. Obviously, when a central element of the offense involves classified information, as with 18 U.S.C. 793 and 794, or is claimed to be necessary to enable the defendant to cross-examine the principal government witness called to establish how documents or information will injure the United States or give advantage to a foreign adversary, CIPA is of limited or no utility.

In some relatively recent espionage cases, the government has avoided high disclosure costs that might have resulted had it not been for the tactics of defense counsel. For example, in *United States v. Moore*,⁹ a former CIA employee was prosecuted under 18 U.S.C. 794(a) for attempting to pass to the Soviet Union various documents relating to the national defense. Two of the charges upon which he was convicted concerned portions of classified CIA phone directories containing the names of numerous employees under cover. The defense counsel failed to cross-examine the government's principal witness who testified concerning the importance of the phone directories and the damage that passage to the Soviets would have caused. While it is doubtful that defense counsel could have persuaded the jury that the documents did not relate to the national defense, he could have increased the cost to the government by exploring in open court whether it had been disclosed publicly that persons listed in the directory worked for CIA or if any had been compromised to the Soviets in other ways.

Similarly, in *United States v. Kampiles*,¹⁰ another former CIA employee was prosecuted under 18 U.S.C. 794(a) for selling to an agent of the Soviet Union a top secret technical manual for the KH-11 satellite system. The government's principal witness concerning the importance of the compromised information was the CIA's Deputy Director for Science and Technology. The witness gave general testimony concerning the importance of the KH-11 system and how the technical manual would help the Soviets take countermeasures. Defense counsel did not seriously cross-examine on these points or press for a detailed explanation of how the manual would provide

⁷ *Espionage Laws and Leaks: Hearings before the Subcommittee on Legislation of the Permanent Select Committee on Intelligence, House of Representatives*, 96th Cong., 1st Sess. 18, (1979) (letter of Anthony A. Lapham to Philip B. Heymann, Assistant Attorney General, Criminal Division, Department of Justice) (hereinafter cited as *Hearings*).

⁸ 18 U.S.C. App. III.

⁹ Unreported. D. Md. 1978.

¹⁰ 609 F.2d 1233 (7th Cir. 1979) *rehearing and rehearing en banc denied* (1980).

Prosecutions

additional help to the Soviets if they already knew the United States had reconnaissance satellites, or whether the United States had noted any decrease in the KH-11 effectiveness since the manual was compromised. Such questions would have clearly been permissible and would almost certainly have led to the additional disclosure of classified information. While the defense tactics in both *Moore* and *Kampiles* may have resulted from conscious decisions not to contest the defense-relatedness of the information involved in order not to unnecessarily prejudice the jury against the defendant, these cases should make it clear that the current espionage statutes offer the government no assurances that it alone will be able to control the amount of sensitive information that will be disclosed at trial.

Possible Reformulation of Statutes

It should be possible to proscribe the conduct that is covered by 18 U.S.C. 793 and 794, at least insofar as those statutes are aimed at classical espionage, without requiring the United States to confirm specific damage to the national security or further exacerbate that damage. In their authoritative treatise on the espionage statutes, Professors Harold Edgar and Benno C. Schmidt, Jr. had the following to say about the broad manner in which classical espionage can be proscribed under our legal system:

The essence of classical espionage is the individual's readiness to put his access to information of defense significance at the disposal of agents of foreign political organizations. Granted that the harm that results from his conduct is a function of the importance of the information transferred, there should be no hesitation, regardless of the banal quality of defense information involved, to punish the citizen whose priorities are so ordered or foreigners whose job it is to risk apprehension. We believe, therefore, that the information protected against clandestine transfer to foreign agents should be defined broadly, probably more broadly than in current law. In this context, we see no dispositive objection to making knowing and unauthorized transfer of classified information to foreign agents an offense, without regard to whether information is properly classified. That a spy might earn complete immunity by stealing secrets so serious that their significance cannot be disclosed in court—a clear possibility under current law, and also under S.1 and S.1400—is an outcome that should be avoided, if possible.¹¹

In some contexts, the knowing passage of classified information to foreign agents is an offense under current law without regard to the propriety of the classification. Thus, under 18 U.S.C. 798, the passage to a foreign government of classified information concerning devices used for cryptographic or communications intelligence purposes is an offense without regard to whether the

¹¹ The Espionage Statutes and the Publication of Defense Information 73 Colum. L.R. 929, 1084 (1973). Professors Edgar and Schmidt would support a revision of the current law to streamline the proscription of classical espionage. See Statement of Harold Edgar and Benno Schmidt, Jr. in *Hearings, supra*, note 7, at 112-13.

Prosecutions

information is properly classified.¹² This is also the case under 50 U.S.C. 783(b) with respect to passage of classified information by employees of the United States to certain foreign representatives.¹³ Since it is difficult to see any First Amendment issues in such cases,¹⁴ the only concerns in drafting an appropriate statute to broadly cover communication of classified information to a foreign power and associated preparatory conduct should be the mental state or scienter needed to establish the offense and the sentencing process and severity of punishment to be imposed. Presumably, since the government would not have to prove the underlying significance of the information to the jury, it should be required to show that the defendant knew that the United States accorded a specific degree of protection to the information and that the defendant's action was intended to benefit some foreign organization. Finally, in order not to impose a severe penalty out of proportion to the offense, provisions for *in camera* proceedings prior to sentencing should be considered to allow the court to determine the importance of the classified information involved. A draft statute which contains these requirements is at Appendix B.

¹² *United States v. Boyce*, 594 F.2d 1246 (9th Cir.), *rehearing denied* (1979).

¹³ *Scarbeck v. United States*, 317 F.2d 546 (D.C. Cir.), *cert. denied*, 374 U.S. 856 (1963).

¹⁴ One of the main purposes of the freedom of speech and press clause of the First Amendment was to ensure the unfettered discussion of matters of importance and interest to the public. The public interest and the First Amendment, likewise, permit legislative efforts to prevent acts, be they characterized as speech or otherwise, which are harmful to the public. The Supreme Court recognized very early in its development of First Amendment law that there are "evils that Congress has a right to prevent." *Schenck v. United States*, 249 U.S. 247 (1919). In view of the unquestioned appropriateness of proscribing espionage, the only real issue becomes one of ensuring that no legitimate speech or press activities are swept within the proscription.

Prosecutions

APPENDIX A

Espionage Laws

18 U.S.C. 793

§ 793. Gathering, transmitting, or losing defense information

- (a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or
- (b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or
- (c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or
- (d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the

Prosecutions

injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

- (e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or
- (f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer—

Shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

- (g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

June 25, 1948, c. G16, 02 Stnt. 730; Sept. 23, 1950, c. 1024, Title I, § 18, GI Stat. 1003.

18 U.S.C. 794

§ 794. Gathering or delivering defense information to aid foreign government

- (a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States, or to the advantage of a foreign nation,

Prosecutions

communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life.

- (b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.
- (c) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

June 25, 1948, c. 645, 62 Stat. 737; Sept. 8, 1954, c. 1261, Title II, § 201, GS Stat. 1219.

APPENDIX B

Draft Statute

H.R. _____ / S. _____

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, that this Act may be cited as the "Espionage Prevention Act of 1984."

SEC. 2. Chapter 37 of title 18, United States Code, is amended by adding at the end thereof the following sections:

§ 800. *Espionage*

- (a) Whoever, without authorization, knowingly collects or attempts to collect classified information with the intent that such information be communicated to a foreign power or an agent of a foreign power shall be punished by imprisonment for any term of years or for life.
- (b) Whoever, without authorization, knowingly communicates, or attempts to communicate, classified information to a foreign power or an agent of a foreign power shall be punished by imprisonment for any terms of years or for life.
- (c) Prosecution under this section shall be barred unless, prior to the return of an indictment or the filing of an information, the Attorney General and the head of an appropriate department or agency responsible for the classified information jointly certify in writing to a court with jurisdiction that, at the time of the commission of the offense, the classified information involved was properly designated as classified information.

§ 801. *Defense to Espionage*

Whoever, in the course of official duties on behalf of the United States, engages in conduct described in Section 800 of this Chapter with a reasonable belief as to the authority to do so shall not be guilty of an offense under section 800.

§ 802. *Sentencing*

- (a) For purposes of sentencing an individual convicted of an offense defined in section 800, the court shall consider the nature of the classified information involved in the offense. Cases which involve classified information deserving a high degree of protection shall, absent especially mitigating factors, receive a greater sentence than cases which involve information requiring lesser degrees of protection.
- (b) Life imprisonment shall not be imposed except in time of war declared by Congress or when the court determines that the classified information involved poses an exceptionally grave danger to the national security or to the life of any person.

Prosecutions

- (c) For purposes of determining an appropriate sentence the court is authorized to conduct such *in camera* proceedings as it determines are necessary for a full understanding of the nature of the classified information involved in the offense. Upon request of the United States for good cause, such proceedings or portions thereof may be held *in camera ex parte*.

§ 803. *Definitions.* For purposes of section 800 of this Title—

- (a) The term "authorization" means having authority, right or permission pursuant to the provisions of a statute, executive order, directive of the head of any department or agency who is empowered to classify information, order of any United States court, or provisions of any rule of the House of Representatives or resolution of the Senate which governs release of classified information by the respective House of Congress.
- (b) The term "classified information" means information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or executive order (or a regulation or order issued pursuant to a statute or executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security.
- (c) The term "communicate" means to disclose, impart, transfer, convey or otherwise make available to another, but does not include publication by the media.
- (d) The term "foreign power" means—
- (1) a foreign government or any component thereof, whether or not recognized by the United States;
 - (2) a faction of a foreign nation or nations;
 - (3) an entity that is directed or controlled by a foreign government or governments;
 - (4) a group engaged in international terrorism or activities in preparation therefor; or
 - (5) a foreign-based political organization.
- (e) The term "agent of a foreign power" means any person who acts on behalf of a foreign power for the purpose of obtaining classified information.
- (f) The term "Attorney General" means the Attorney General of the United States (or Acting Attorney General) or the "Deputy Attorney General."

SEC. 3. The table of sections for chapter 37 of title 18, United States Code, is amended by adding at the end thereof the following:

- § 800. *Espionage*
- § 801. *Defense to Espionage*
- § 802. *Sentencing*
- § 803. *Definitions.*