OFFICIAL USE ONLY

Historical review of the problem and some remedial proposals.

THE PROTECTION OF INTELLIGENCE DATA

John D. Morrison, Jr.

The unauthorized exposure of classified information is a chronic problem for governments and intelligence agencies. Defense against the conscious agent of a foreign power is different from, and in some ways less difficult than, deterring revelations due to carelessness, malice, or greed on the part of government employees. The problem is particularly acute in a democratic society whose laws and courts must provide broad protection to criminal defendants. The deterrence provided by the espionage laws and related statutes is weakened by the difficulty of prosecution under them. This is especially true in cases involving disaffected or careless employees of intelligence agencies; the defenses usually include strong equitable pleas which may excite a sympathetic public response.

No legislation or administrative procedure can offer perfect protection. It is submitted, however, that both our laws and our administrative procedures could be improved so as to provide more effective deterrence. Some particular avenues that might be taken will emerge from the following discussion.

The Espionage Laws: An Incomplete Structure

A review of American legislation, in the field of criminal espionage shows that historically there has been limited legislative effort directed to the protection of intelligence data. As a result there is a startling lack of protection for a governmental function of growing importance and sensitivity. Perhaps the need for laws protecting intelligence data has reached significant proportions only in the relatively recent past.

The changes, technological and other, in the manner in which nations deal with each other have caused some improvements in legislation dealing with the protection of state secrets. Diplomatic communications have traditionally been protected. As early as 1807, the Supreme Court suggested that the legislature recognize and provide against crimes affecting the national security which "have

i

OFFICIAL USE ONLY

not ripened into treason." ¹ It was not until 1911, however, that Congress passed the first important statute dealing with the broad problem of espionage. In 1917 the language of the 1911 act was amended to read much as it does today. More recently congressional attention has been focused—and appropriate legislation enacted—on the problems involved in protecting atomic energy data² and communications intelligence.³ The Internal Security Act of 1950⁴ made it unlawful for a government employee merely to communicate classified information to a known representative of a foreign government.⁵

However, the espionage laws are still the basic statutory protection against unauthorized disclosure of intelligence materials and information. No legislation has yet been enacted to cover the new problems arising out of the chronic "cold war" status of international relations and the consequent need for a sophisticated, professional intelligence apparatus as an arm of the executive. The wartime concept of the military secret is inadequate to cover information about the personnel, activities, and products of such an apparatus, information whose extreme sensitivity is often not readily apparent even though its exposure may have a most damaging effect on the national security.

These shortcomings point to the need for new legislation establishing a category "Intelligence Data" and providing that anything so designated by an authorized official shall be judicially recognized as such solely on the basis of that designation. This would solve a vexatious and recurring problem for which there is no known cure in existing laws. That problem is the immunity enjoyed by an exposer of sensitive information when the information itself cannot for practical reasons be brought into the open for the purpose of prosecution.

The Official Secrets Acts

It has often been suggested that, if legislation is needed in this area, the British Official Secrets Acts with their broader protection offer a good example to be followed. It is not commonly understood

¹Ex parte Bollman and Ex parte Swartwout, 4 Cranch 75, 127, 2 L. Ed. 554, 571 (1807).

⁴² U.S.C. §2271 et seq.

^{* 18} U.S.C. §798.

^{&#}x27;50 U.S.C. §783(b).

^{*} See Scarbeck v. U.S., 317 F. 2d 546, cert. denied, 83 S. Ct. 1897 (1983).

^{* 18} U.S.C. §§791-798.

that the British acts are based on a different legal theory from that underlying our espionage acts. Under our system the information divulged must be shown to be related to national defense and security either by its very nature or as coming within statutory definitions such as those for communications intelligence and atomic energy data. The British acts are based on the theory of privilege, according to which all official information, whether or not related to the national defense and security, is the property of the crown. It is therefore privileged, and those who receive it officially may not divulge it without the crown's authority.

In a British prosecution for unauthorized disclosure several consequences flow from the privilege theory. Portions of the trial can be held in camera if the court agrees. Under our constitution, while certain procedural aspects can be considered in camera, no part of the actual trial could be heard privately. In Britain certain presumptions may apply. For instance, if the defendant is known to have possession of privileged information and to have been in the company of a known foreign espionage agent, there is a presumption that he passed the information. The presumption is rebuttable; but our Supreme Court opinions indicate that such a presumption would not be permissible here. Most important, in the English system it is not necessary to prove that any item of information relates to the national defense and security.

A good example is the so-called Isis case in which two Oxford students published in their college magazine, Isis, the story of their experiences in the Navy, including technical intelligence operations in the Baltic. The prosecution merely testified that the article contained information which they had acquired in their official service and was, therefore privileged. After the verdict of guilty, the prosecution approached the court alone, without presence of defendants or defense counsel, and briefed the court, solely for purposes of sentencing, on the significance of each item of information to the government. Such a briefing, we believe, would be held error under our system.

In another case, that of an RAF officer named Wraight who defected to Russia and then returned, a government witness who had inter-

⁷ Jencks v. U.S., 353 U.S. 657, 668 (1957). But see post Jencks Statute 18 U.S.C. §3500(c) permitting in camera examination for relevancy and editing of pre-trial reports of government witnesses.

1

1

Ĺ

1000

1

1

1

OFFICIAL USE ONLY

viewed the defendant for the security services was allowed to testify without publicly identifying himself. His name was handed in writing to the court. Possibly this could be done here if the defense agreed to it, but it seems clear it could not be done over the defense's objection.

In short, the Official Secrets Acts would seem to be in important respects unconstitutional in this country and therefore cannot be relied on as examples of means by which we could protect intelligence data. In addition, despite the technical advantages which the British laws provide for the prosecution, experience has shown that these do not by any means give complete protection; they are only to some degree more effective than our system.

Intelligence Sources and Methods

The statutory authorities and responsibilities of the Director of Central Intelligence include the responsibility for "protecting intelligence sources and methods from unauthorized disclosure." 8 The Congress's use of the term "intelligence sources and methods" indicates its recognition of the existence of a special kind of data encompassing a great deal more than what is usually termed "classified intelligence information." The espionage laws and the statutes designed to protect communications and atomic secrets, though they specify in detail the kinds of information they seek to protect, nevertheless do not cover everything that might be defined as intelligence data whose exposure could be detrimental to the national interests. For example, knowing the identities of U.S. covert intelligence officers or the fact that U.S. intelligence is making a study of certain published unclassified materials might be of great value to a foreign intelligence agency, but there is some question whether such information would be considered by a court to be included among the things protected by existing statutes.

The Congress has also recognized the need for protecting intelligence sources and methods by enacting for CIA a number of special authorities and exemptions from legal requirements otherwise in general force throughout the government. The Agency is exempted from the "provisions of any . . . law which require the publication

National Security Act of 1947, \$102(d), 61 Stat. 495 50 U.S.C. \$403.

or disclosure of the organization, functions, names, official titles, salaries, or numbers of personnel employed by the Agency." Similarly, the Agency is authorized to expend the funds made available to it for objects of a confidential, extraordinary, or emergency nature, such expenditures to be accounted for solely on the certificate of the Director. It is exempted from statutory requirements regarding exchanges of funds and the performance rating of employees and from laws and executive orders governing appeals from adverse personnel actions.

Thus Congress has charged the Director of Central Intelligence with protecting intelligence sources and methods from unauthorized disclosure, has recognized that the term "intelligence sources and methods" encompasses an area not entirely covered in other statutes, and has affirmed the need for such protection by providing statutory authority for that purpose. The void in the statutory structure protecting intelligence sources and methods is the absence of sanctions against unauthorized disclosure which can be invoked without disclosing the very sources and methods whose protection is sought.

The Judicial View of Intelligence

The courts have long recognized that the secret intelligence activities of the executive branch, though indispensable to the government, are by their nature matters whose disclosure would be injurious to the public. In the Totten case ¹⁰ compensation was sought under a secret contract with President Lincoln for espionage activities behind Confederate lines. The opinion of the Supreme Court stated:

If upon contracts of such a nature an action against the government could be maintained in the Court of Claims, whenever an agent should deem himself entitled to greater or different compensation than that awarded to him, the whole service in any case, and the manner of its discharge, with the details of the dealings with individuals and officers, might be exposed, to the serious detriment of the public. A secret service, with liability to publicity in this way would be impossible; and, as such services are sometimes indispensable to the Government, its agents in those services must look for their compensation to the contingent fund of the department employing them, and to such allowance from it as those who dispense that fund may award. The secrecy which such contracts impose precludes any action for their enforce-

^{*}Central Intelligence Agency Act of 1949, as amended, §6, 63 Stat. 208, 50 U.S.C. §403g.

¹⁶ Totten v. U.S., 92 U.S. 105 (1876).

1

OFFICIAL USE ONLY

ment. The publicity produced by an action would itself be a breach of a contract of that kind, and thus defeat a recovery.

It may be stated as a general principle, that public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential, and respecting which it will not let the confidence be violated. On this principle, suits cannot be maintained which would require a disclosure of the confidences of the confessional, or those between husband or wife, or of communications by a client to his counsel for professional advice, or of a patient to his physician for a similar purpose. Much greater reason exists for the application of the principle to cases of contract for secret services with the Government, as the existence of a contract of that kind is itself a fact not to be disclosed. [Emphasis supplied.]

The Totten case marks the beginning of the juridical idea—and judicial cognizance of it—that there is a kind of relationship to the state which is confidential, beyond judicial inquiry, and involving a trust of such nature that the courts cannot aid a breach of it, even in their solemn duty of administering justice.¹¹ A secret agent is almost impotent in his own cause; he literally cannot maintain an action in the courts where his secret activities are germane to the case.¹²

Judicial Access to Sensitive Data

Present espionage laws dealing with unlawful transmission or obtaining of information related to the national defense 13 have been interpreted as requiring proof of certain questions of fact; evidence on these questions must be submitted to the jury for consideration of its weight and sufficiency. For instance, the information betrayed must in fact be related to the national defense and must not have been generally available. 14 The courts have held that a jury cannot find on these facts unless it has access to the information allegedly related to the national defense and hears testimony regarding its use, importance, exclusiveness, and value to a foreign government or

¹¹ See Firth Sterling Steel Co. v. Bethlehem Steel Co., 199 Fed. 353 (1912), in which the court struck documents from the record on the ground that it was against public policy to disclose military secrets. See cases cited in note 18.

¹³ De Arnaud v. U.S., 29 Ct. 555, 151 U.S. 483 (1894); Allen v. U.S., 27 Ct. Cl. 89 (1892); Tucker v. U.S., 118 F. Supp. 371 (1954).

¹⁸ U.S.C. §§793, 794, and 798.

¹⁴ U.S. v. Heine, 151 F.2d 813, 816 (1945), citing Gorin v. U.S., 312 U.S. 19, 28, 61 S.Ct. 429, 85 L.Ed. 488 (1941).

potential injury to the United States.¹⁵ The defendant in a criminal proceeding must likewise have access to it, since the information itself may tend to exculpate him with respect to dealings in it.¹⁶ As Judge Learned Hand said in *U.S. v. Andolschek*, "The Government must choose; either it must leave the transactions in the obscurity from which a trial will draw them, or it must expose them fully." ¹⁷

These rulings have left the government in the position of having to reveal in court the very information it is trying to keep secret or else not prosecute those who steal information and use it to the injury of the nation. To invoke the law's protection of the secret, the secret must be told.

Judicial experience with the privilege which protects military and state secrets has been limited in this country.¹⁸ British experience, though more extensive, is still slight compared to that with other evidentiary privileges.¹⁹ Nevertheless, it is clear at least from the civil precedents that the court itself must determine whether the circumstances are appropriate for the claim of privilege ²⁰ and yet do so without forcing a disclosure of the very thing the privilege is designed to protect.²¹ The latter requirement is the real difficulty. In dealing with it, courts have found it helpful to draw upon judicial experience

¹⁶ Gorin v. U.S., 312 U.S. 19, 30-31, supra note 14.

¹⁸ U.S. v. Reynolds, 345 U.S. 1, 73 S.Ct. 538 (1953); Jencks v. U.S., supra

[&]quot; 142 F.2d 503, 506 (1944).

²⁸ See Totten v. U.S., 93 U.S. 105, 23 L.Ed. 605 (1876); Firth Sterling Steel Co. v. Bethlehem Steel Co., 199 Fed. 353 (1912); Pollen v. Ford Instrument Co., 26 F. Supp. 583 (1939); Cresmer v. U.S., 9 F.R.D. 203 (1949). See also Bank Line v. U.S., 68 F. Supp. 587, 163 F.2d 133 (1947). 8 Wigmore on Evidence (3d Ed.) sec. 2212(a), p. 161, and sec. 2378(g)(5), pp. 785 et seq.; 1 Greenleaf on Evidence (16th Ed.) secs. 250-251; Sanford, Evidentiary Privileges Against the Production of Data Within the Control of Executive Departments, 3 Vanderbilt Law Review 73-75 (1949). See also Ticon v. Emerson, 134 N.Y.S. 2d 716, 206 Misc. 727 (1954).

¹⁹ Most of the English precedents are reviewed in *Duncan v. Cammel, Laird & Co., Ltd., A.C.* 624 (1942). For a thorough study of the history and application of the Official Secrets Acts see David Williams' *Not in the Public Interest* (London, 1965), reviewed in *Studies X 3*, p. 97.

[&]quot;Id. at 642.

ⁿ U.S. v. Reynolds, supra note 16, at 8, citing Duncan v. Cammel, Laird & Co., Ltd., supra note 19, and Hoffman v. U.S., 341 U.S. 479 (1951).

in dealing with an analogous privilege, that against self-incrimination. The Supreme Court said in U.S. v. Reynolds: 22

The privilege against self-incrimination presented the courts with a similar sort of problem. Too much judicial inquiry into the claim of privilege would force disclosure of the thing the privilege was meant to protect, while a complete abandonment of judicial control would lead to intolerable abuses. Indeed, in the earlier stages of judicial experience with the problem, both extremes were advocated, some saying that the bare assertion by the witness must be taken as conclusive, and others saying that the witness should be required to reveal the matter behind his claim of privilege to the judge for verification. Neither extreme prevailed, and a sound formula of compromise was developed. . . .

Regardless of how it is articulated, some like formula of compromise must be applied here. Judicial control over the evidence in a case cannot be abdicated to the caprice of executive officers. Yet we will not go so far as to say that the court may automatically require a complete disclosure to the judge before the claim of privilege will be accepted in any case. It may be possible to satisfy the court, from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged. When this is the case, the occasion for the privilege is appropriate, and the court should not jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers.

Of course Reynolds was a civil case, but the evidentiary difficulty in criminal cases is quite comparable. Thus, citing Reynolds, the Supreme Court stated in *Jencks v. U.S.*: ²⁴

It is unquestionably true that the protection of vital national interests may militate against public disclosure of documents in the Government's possession. This has been recognized in decisions of this Court in civil causes where the Court has considered the statutory authority conferred upon the departments of government to adopt regulations not inconsistent with law for . . . use . . . of the records, papers, appertaining to his department. The Attorney Ceneral has adopted regulations pursuant to this authority declaring all Justice De-

[&]quot;Supra note 16, at 8-10.

In Kaiser Aluminum & Chemical Corp. v. U.S., 157 F. Supp. 939 (1958), the Court of Claims held that judicial examination of a document for which executive privilege has been asserted should not be ordered without a definite showing by plaintiff of facts indicating reasonable cause for requiring such a submission. Otherwise, said the Court, at 949, the executive determination would be merely preliminary and "the officer and agency most aware of the needs of government and most cognizant with [sic] the circumstances surrounding the legal claim will have to yield determination to another officer (the Court) less well equipped."

[™] Supra note 7, at 670.

partment records confidential and that no disclosure, including disclosure in response to subpoena, may be made without his permission.

But this Court has noticed, in U.S. v. Reynolds, the holdings of the Court of Appeals for Second Circuit that, in criminal causes "... the Covernment can invoke its evidentiary privileges only at the price of letting the defendant go free. The rationale of the criminal cases is that, since the Covernment which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense.

The loophole afforded by this evidentiary difficulty has not been overlooked by the thief who limits his trade to information too sensitive to be revealed. Nor is it ignored by the more imaginative among those accused of other crimes when they claim that their offenses were committed at the behest of an intelligence agency which uses its statutory shield to protect itself at the expense of its agent.

Judicial Evaluation of Sensitive Data

It must be emphasized that undesired disclosure is only one difficulty in the submission of intelligence data to a jury. There is another great problem, the capability of the jury to evaluate such data, often complex and technical and often meaningful only in the context of other sensitive information not otherwise bearing on the case. 26 It can of course be argued that juries often have to grapple with technical facts and that the law provides for assistance in such instances in the form of expert witnesses. But in a case dealing with secret information, resort to these legal devices merely increases the amount of sensitive data which must be shorn of its usefulness by disclosure, increasing the government's reluctance to prosecute and thwarting the protective congressional intent expressed in legislation.

Some Avenues for Action

The courts have recognized that intelligence activities are confidential per se and not subject to judicial inquiry. Congress, in the National Security Act, has charged the Director of Central Intelligence with the protection of intelligence sources and methods and has given

The quoted material from the Reynolds case appears at 345 U.S. 12.

²⁶ Compare the holding in the Kaiser case, supra note 23, on the competence of the court to evaluate the contents of a document for which there has been a claim of executive privilege.

OFFICIAL USE ONLY

him certain statutory authority and exemptions to assist him in meeting this obligation. Yet the espionage laws and related statutes enacted for the same or a similar purpose can often not be put to work just when the offense represents the greatest potential threat to the public welfare.

There are three steps which would go far toward solving the problems which still exist in this area. Two of them would seem to require new legislation; the third might be accomplished, at least with respect to CIA, by regulation under the DCI's existing authority. First would be a criminal statute defining what is to be protected and providing punishment for exposure. Second, this statute should also confer injunctive authority, because prevention of exposure is more to the point than punishment for violation and in many cases an injunction might offer greater deterrence than the penal provisions for violation. In addition, the act might provide that persons convicted under it would forfeit retirement benefits; precedent for this exists in 5 U.S.C. §8312, the so-called "Hiss Act."

The third step would be a requirement by the Director that all employees, agents, consultants, and others who enter into a relationship with CIA giving them privity to intelligence data agree in writing to assign as of that time to the Agency all rights in anything intended by them for publication based on information received in the course of their official duties. Perhaps a similar step could be taken by other intelligence agencies. Such agreements, along with appropriate regulations governing the dissemination of intelligence data, could in themselves serve as a basis for injunctive relief, apart from or as an alternative to the statutory provision for injunctions against the criminal act of exposure.

Some such steps are necessary if we are to overcome the shortcomings in laws protecting intelligence information which limit prosecution to cases where intent is clear and where divulging information in open court is not detrimental.