Description of document:	Title of Thesis: Classified Information Leaks: The Need for New Tools in the Plumber's Tool Box 2007. Released by the Office of the Director of National Intelligence (ODNI)
Requested date:	2022
Release date:	20 December 2024
Posted date:	13-January- 2025
Source of document:	FOIA Request Director, Information Management Office ATTN: FOIA/PA Office of the Director of National Intelligence Washington, D.C. 20511 Email: ODNI_FOIA@odni.gov

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC

20 December 2024

Reference: ODNI Cases DF-2022-00310, DF-2022-00311, & DF-2022-00314

This letter provides an interim response to three of your Freedom of Information Act (FOIA) request to the Defense Intelligence Agency (DIA) requesting specific theses written by students at the National Intelligence University. As previously noted by DIA, DIA transferred these cases to the Office of the Director of National Intelligence (ODNI) in 2022.

ODNI is processing these requests under the FOIA, 5 U.S.C. § 552, as amended.

This interim response addresses eight of the theses. ODNI determined that one thesis, *Why the United States Needs a Domestic Intelligence Service and How to Make it Work*, falls under the purview of another government agency. It has been referred to them for review and direct response to you. *Non-Lethal Weapons of Mass Disruption* is provided in response to case DF-2022-00311 and *Hollywood Soldier Intelligence Support for SOFTWAR Operations* is for case DF-2022-00314. The other five these were requested under case DF-2022-00310.

During the review process of the seven documents being released directly to you, we considered the foreseeable harm standard and determined that certain information must be withheld pursuant to the following FOIA exemptions:

- (b)(3), which applies to information exempt from disclosure by statute. Specifically, the National Security Act of 1947, as amended:
  - Section 102A(i)(l), 50 U.S.C. § 3024(i)(1), which protects information pertaining to intelligence sources and methods; and
  - Section 102A(m), as amended, 50 U.S.C. § 3024(m), which protects the names and identifying information of ODNI personnel.
- (b)(6), which applies to information that, if released, would constitute a clearly unwarranted invasion of personal privacy.

Be advised, we continue to process your request. If you are not satisfied with this response, a number of options are available. You may contact me, the FOIA Public Liaison, at ODNI_FOIA_Liaison@odni.gov, or the ODNI Requester Service Center, at ODNI_FOIA@odni.gov or (703)-275-1313. You may also submit an administrative appeal to the Chief FOIA Officer, c/o Chief, Information Management Office, Office of the Director of National Intelligence, Washington, DC 20511 or emailed to ODNI_FOIA@odni.gov. The appeal correspondence should be clearly marked "Freedom of Information Act Appeal of Adverse Determination" and must be postmarked or electronically transmitted within 90 days of the date of this letter.

Lastly, the Office of Government Information Services (OGIS) of the National Archives and Records Administration is available with mediation services and can be reached by mail at 8601 Adelphi Road, Room 2510, College Park, MD 20740-6001; telephone (202) 741-5770; toll-free (877) 684-6448; or email at ogis@nara.gov.

Sincerely,

Erin Morrison
Chief, Information Review and Release Group
Information Management Office

ABSTRACT

TITLE OF THESIS: Classified Information Leaks: The Need for New Tools in the Plumber's Tool Box

STUDENT: (b) (6) [redacted]

CLASS NUMBER: PGIP-R Class 2006 **DATE:** January 2007

THESIS COMMITTEE CHAIR: (b) (6) [redacted]

COMMITTEE MEMBER: (b) (6) [redacted]

The unauthorized disclosure of classified information, or leaks, has been a continuing problem for the Intelligence Community (IC). While there have been some notable case examples, some classified and some not, which show the damage done to U.S. national security, there have been few federal criminal prosecutions of those leaking classified information. Indeed, the government has struggled to apply the existing set of laws and regulations, many designed for other purposes, to the problem. This thesis focuses on the gaps, inequities, and issues in existing federal law with regard to leaks and proposes alternatives to address the problem. This thesis analyzes the Shelby

Amendment to the Fiscal Year 2001 Intelligence Authorization Act, the British Official Secrets Act of 1989, and a proposed statute by the author.

This thesis reviews existing U.S. laws regarding unauthorized disclosures of classified information. This thesis surveys statutory, regulatory and decisional law and finds at least six unresolved legal issues regarding the application of the Espionage Act, 18 U.S.C. §§ 793 and 794 to the unauthorized disclosure of classified information. This survey includes a detailed analysis of recent leak cases to include President Clinton's pardon of Samuel Morison, one of the few persons prosecuted in the last 50 years for leaking classified information. Next comes a summary of recent legislative efforts including the history of the Shelby Amendment, the results of the 2002 interagency task force formed by the Attorney General, and the re-introduction of the Shelby Amendment by Senator Kit Bond on 2 August 2006. This legislative summary includes the positions taken by the Attorney General, the Director of Central Intelligence, media interest groups and President Clinton. Next follows a review of the British Official Secrets Act, to include the most recent 1989 amendment. This review shows that there are certain aspects of British law that would be useful to American legislators. Finally, the thesis includes a proposed statute by the author. This statute includes strict liability provisions for damaging leaks and is tailored to apply to both government employees who leak information and third-parties (i.e. journalists, academics and lobbyists) who receive leaked information.

In sum, this thesis concludes that existing U.S. law has gaps and fails to provide adequate tools to deter would be leakers and to prosecute culpable persons.

UNCLASSIFIED

CLASSIFIED INFORMATION LEAKS: THE NEED FOR NEW TOOLS IN THE PLUMBER'S TOOL BOX

by

(b) (6)
[redacted]
PGIP-R 2006

Unclassified thesis submitted to the faculty
of the Joint Military Intelligence College
in partial fulfillment of the requirements for the degree of
Master of Science of Strategic Intelligence

January 2007

UNCLASSIFIED

The views expressed in this paper are those of the author and
do not reflect the official policy or position of the
Department of Defense or the U.S. Government

CONTENTS

Chapter

Appendixes

CHAPTER 1

INTRODUCTION

The unauthorized disclosure of classified information, or leaks, has been a continuing problem for the Intelligence Community (IC).[1] While there have been some notable case examples, some classified and some not, which show the damage done to U.S. national security, there have been few federal criminal prosecutions of those leaking classified information. Indeed, the government has struggled to apply the existing set of laws and regulations, many designed for other purposes, to the problem. This thesis focuses on the gaps, inequities, and issues in existing federal law with regard to leaks and proposes alternatives to address the problem.[2] This thesis analyzes three alternative statutory proposals to tighten U.S. law using

[1] The term Intelligence Community is defined by 50 U.S.C. § 401(a) to include: the Central Intelligence Agency (CIA); the National Security Agency (NSA); the Defense Intelligence Agency (DIA); the National Geo-Spatial Intelligence Agency (NGA); the National Reconnaissance Office (NRO); Department of Defense offices for collection of specialized intelligence through reconnaissance programs; the intelligence elements of the military services, the Federal Bureau of Investigation (FBI), Department of the Treasury, Department of Energy and the Coast Guard; the Bureau of Intelligence and Research of the Department of State; and elements of the Department of Homeland Security. Under the National Security Intelligence Reform Act of 2002, the Intelligence Community now includes the Director of National Intelligence. 50 U.S.C. § 401 (2004).

[2] Classified information means information that has been determined pursuant to Executive Order No. 12958, or any successor order, Executive Order No. 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure. Executive Order 12958, § 1.1(d). There are three classification levels: "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe. "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe. "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe. Executive Order 12958, § 1.3.

both a legal and a policy analysis and makes specific recommendations for change in existing federal law.

This thesis considers the Shelby Amendment to the FY 2001 Intelligence Authorization Act, the British Official Secrets Act (BOSA) of 1989, and a proposed statute, and analyzes each in turn under U.S. constitutional case law. The First Amendment to the U.S. Constitution restricts the government's ability to limit the release of information to the public and its ability to restrain the media from publishing information that has been released in violation of the law without prior approval.[3] In fact, more than 35 years have passed since the government has tried through the courts to stop a publisher from printing classified information. The 1971 *New York Times Co.* (The Pentagon Papers) case marks the last time that the government tried to use the courts to restrain the press from publishing classified information.

An effective set of statutes should combine restraints on publication with subsequent criminal punishment. Moreover, any proposed change in the law must meet constitutional muster and avoid unnecessary policy complications. This thesis makes specific recommendations to tighten U.S. law and improve deterrence against leaks.

Recent leaks and criminal prosecutions highlight the need to deter the unauthorized disclosure of classified information by members of the Intelligence Community. Under current law, various statutes prohibit disclosures of certain information; namely, national defense information, intercepted communications or codes, certain restricted data, or intelligence

[3] *New York Times Co. v. United States*, 403 U.S. 713, 91 S. Ct. 2140, 29 L. Ed. 2d 822 (1971) (government effort to enjoin publication of the contents of a classified study); *Snepp v. United States*, 444 U.S. 507, 100 S. Ct. 763, 62 L. Ed 2d 704 (1980) (secrecy agreement signed by employee of the Central Intelligence Agency); and *United States v. The Progressive, Inc.*, 467 F.Supp. 990 (W.D. Wis. 1979) (preliminary injunction restraining publication of "do-it-yourself" guide for building an atomic device).

identities.[4] No comprehensive statute proscribes the unauthorized disclosure of classified information irrespective of the type of information or recipient involved. While unauthorized disclosures are a continuing and sometimes newsworthy problem, four recent events have highlighted the need for a change in federal law: President Clinton's veto of the Fiscal Year (FY) 2001 Intelligence Authorization Act (H.R. 4392) because of an anti-leak amendment offered by Senator Richard Shelby (Republican, Alabama), then Chairman of the Senate Select Committee on Intelligence (SSCI); the November 2005 leak to the *Washington Post* on the Central Intelligence Agency's overseas terrorist detention facilities; the December 2005 leak to the *New York Times* concerning the National Security Agency's (NSA) warrantless surveillance program; and the July 2006 government subpoena of a former NSA employee in an effort to compel disclosure of the source of that leak.[5] This thesis considers these issues not only from a legal perspective, but also from a policy perspective. For example, President Clinton vetoed the Shelby Amendment, a provision that would have made it a felony to disclose classified information, contending that it would have increased the likelihood that it would "unnecessarily chill legitimate activities."[6]

This thesis hypothesizes that existing U.S. law fails to provide an adequate criminal deterrent to the unauthorized disclosure of classified information and fails to provide adequate

---

[4] *See*, for example, the statutes prohibiting the disclosure of national defense information, intercepted communications or codes (18 U.S.C. §§ 793, 794, 797, 798 and 952) (2000); the statutes prohibiting the disclosure of restricted data (42 U.S.C. § 2274) (2000); Intelligence Identities Protection Act (50 U.S.C. § 421 et. seq.) (2000); or the Internal Security Act (50 U.S.C. §783) (1950) (repealed).

[5] Steve Chapman, "Have Leaks Crippled War on Terrorism?" *Chicago Tribune*, on line ed., 9 July 2006, URL: <http://www.chicagotribune.com/news/columnists/chi-0607090393jul09,1,1759071.column?coll=chi-navrailnews-nav>, accessed 8 September 2006.

[6] William J. Clinton, "Statement by the President to the House of Representatives," 4 November 2000, URL: <http://64.233.161.104/search?q=cache:n_stZ_BT6U0J:www.fas.org/irp/news/2000/11/irp-001104-leak.htm+clinton,+%22statement+by+the+president+to+the+house%22&hl=en&gl=us&ct=clnk&cd=1>, accessed 22 August 2006.

legal remedies that address unauthorized disclosures. This thesis addresses three key questions: What are the gaps, inequities and issues in existing law related to the unauthorized disclosure of classified information? What statutory alternatives might address these and be consistent with First Amendment case law? What policy concerns are associated with each proposed change?

Classic espionage, the act of selling secrets to a foreign power, is distinct from leaks, the unauthorized disclosure of classified information. While the damage caused to U.S. national interests by leaks may be equal or greater than that of espionage, leaks are typically made by government insiders to the press, lobbyists, or academics for other than pecuniary gain. Indeed, some leaks are made because the insider hopes to shape government policy to the advantage of the United States. Spies commit espionage, on the other hand, for either pecuniary gain or anti-U.S. sympathies. These distinctions are important in view of the scienter (or knowledge) requirements to support a conviction under existing law.

When facing a question about government limits to freedom of expression under the First Amendment, the U.S. Supreme Court has developed two tracks of case law under the First Amendment freedom of expression: content restrictions, and time, place and manner restrictions. The Court has recognized numerous limitations on that the government may regulate certain specific content conveyed by speech (also called anti-speech limitations). For example, courts allow speech limitations based upon defamation, copyright, attorney solicitation, and espionage. In the second line of cases, the Court considers time, place and manner limitations as non-speech restrictions.

The laws dealing with the unauthorized disclosure of classified information are based upon the content of speech in that the government seeks to restrain and punish certain expressive activity. The Supreme Court has ruled that the government may regulate the content of

otherwise constitutionally-protected speech in order to promote a compelling interest if it chooses the least restrictive means necessary to further the stated interest.[7]

This unclassified thesis assumes that the unauthorized disclosure of classified information poses a threat to U.S. national security. An analysis of the number, nature, identity, and specific damage caused by past leaks would be classified, and is beyond the scope of this project. This thesis is limited to existing U.S. law, including gaps, inequities and issues in U.S. law, and how U.S. law might be changed to provide a more effective deterrent. This thesis also assumes that the threat of subsequent punishment is an effective form of legislative prior restraint.

This thesis is unique in that it reviews gaps, inequities and issues in existing law with regard to the problem of unauthorized disclosure of classified information. Next comes a structured topic exploration involving legal analysis of U.S. statutes, regulations, and case law. With regard to statutes and regulations, this thesis analyzes proscribed activities, legal remedies and gaps in the law. With regard to case law, it analyzes the facts, issues and holdings, to include an analysis of the substantive weight of the case. This study then proceeds with a review of the legislative history of the failed Shelby amendment and provides a legal post-mortem, to include President's Clinton veto and the subsequent opinions of the U.S. Attorney General and the Director, Central Intelligence (DCI) on the need for changes in the law. It analyzes both the British Official Secrets Act (BOSA) and a proposed statute for comparison. With regard to the BOSA, it shows why an official secrets act would not be appropriate in the United States. Instead, this thesis proposes a statute that might remedy the problems in current law.

Chapter 2 reviews existing U.S. law with regard to the unauthorized disclosure of classified information. This chapter begins with a description of the First Amendment to the

[7] *Sable Communications of California v. Federal Communications Commission*, 492 U.S. 115, 126, 109 S. Ct. 2829, 106 L. Ed. 2d 93 (1989).

U.S. Constitution, as well as applicable statutes, case law and Executive Orders, followed by a discussion of how federal law has been applied to various cases. This chapter discusses some of the policy tensions between the need to prevent the unauthorized disclosure of classified information and the need for government agencies to share intelligence. Finally, this chapter discusses some of the problems involved in applying existing law to leakers.

Chapter 3 is an analysis of recent legislative efforts to amend existing law to include a legal post-mortem on the Shelby Amendment to the FY01 Intelligence Authorization Act. This chapter reviews recent legislative efforts to remedy the perceived patchwork of laws, both to provide consistency and to cover all the information that the government needs to protect from leakage. To close the perceived gaps, the 106th Congress passed an amendment to the FY01 Intelligence Authorization Act (the Shelby Amendment). President Clinton vetoed the measure. Subsequently, the 108th Congress considered an identical measure, but instead directed the Attorney General and other agency heads to review existing law and to issue a report recommending either legislative or administrative action.

Several subsequent documents show the differing positions of the DCI, and the U.S. Attorney General on the need for changes in federal law. An extensive report of the Attorney General to the U.S. Congress provides one example.[8] The Attorney General contended that existing law was adequate to address the problem involving the unauthorized disclosure of classified information. The DCI, however, did not agree.[9] In addition, the legislative history

[8] John Ashcroft, U.S. Attorney General, "Report to Congress on Unauthorized Disclosures of Classified Information," 15 October 2002, URL: <http://www.fas.org/sgp/othergov/dojleaks.html>, accessed 26 October 2005.

[9] George J. Tenet, Director Central Intelligence, Letter to U.S. Attorney General, Subject: "Draft Report of the Attorney General to the U.S. Congress," 11 May 2002. *See also* John Ashcroft, U.S. Attorney General, Letter to the Director Central Intelligence, Subject: "Reply to Letter, 11 May 2002," 15 July 2002.

provides some information on the policy concerns that lead to President Clinton's veto of the amendment. More recently, on 2 August 2006 Senator Kit Bond (Republican, Missouri) re-introduced legislation to target leaks. This chapter identifies useful lessons for U.S. policymakers in terms of future legislative efforts.

Chapter 4 summarizes, discusses and analyzes the British Official Secrets Act (BOSA). The United Kingdom has taken a different approach to the problem and certain aspects of the British approach might be useful to U.S. policy-makers.

Chapter 5 proposes a new U.S. statute. This chapter summarizes the proposal, discusses the legal adequacy of the proposal under constitutional law, and reviews how the proposal answers the gaps, inequities and issues identified in Chapter 2.

Chapter 6 concludes the thesis and makes recommendations for policymakers.

This thesis contains six appendices: a Table of Related U.S. Statutes, a Table of U.S. Leak and Espionage Cases, the Shelby Amendment, a Table of the British Official Secrets Act, and the Proposed Statute.

CHAPTER 2

CURRENT U.S. LAW

Those who disclose classified information without prior governmental authorization fall into four broad categories: Insiders (government employees) who provide information to an outsider (i.e. the press, lobbyists or academics) usually for non-pecuniary gain; insiders who provide information to a foreign power; persons who receive the information from inside sources; and persons who receive it, and then publish it. The government has used various legal remedies to restrain the expressive activity of both insiders and recipients, to identify the sources of information, and to prosecute the culpable parties. Current statutes have, however, been a clumsy tool for deterring and prosecuting non-espionage leak cases. As a principle of law, statutes dealing with the same topic should be read *in pari materia* to determine the overall legislative intent and applicability in any given case. Unfortunately, the accretion of laws has not been harmonized to meet the continuing problem posed by the unauthorized disclosure of classified information.

The U.S. Congress has repeatedly recognized the need to protect classified information, intelligence sources and methods, liaison relationships and intelligence identities.[10] Congress

[10] The President has arguable authority to protect information from misuse pursuant to Article II, U.S. Constitution. Under Article II the people imposed an obligation upon the President to defend the Constitution and protect the Nation from all enemies, foreign and domestic. The Congress has, however, imposed a statutory obligation upon the Director of National Intelligence to "protect intelligence sources and methods from unauthorized disclosure." 50 U.S.C. § 403-1 (i).

directed the President, pursuant to 50 U.S.C. § 435, to establish procedures to govern access to classified information. The President issued Executive Order 12958, which prescribes the current uniform standard for classifying, declassifying and safeguarding national security information.[11] The order recognizes not only the need to keep the public informed about the activities of government, but also that certain information must be protected against unauthorized disclosure. The order defines information as "any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government."[12] It further defines unauthorized disclosure as "a communication or physical transfer of classified information to an unauthorized recipient."[13] Executive Order 12958 provides instruction on the classification levels, classification authority, classification categories, duration of classification, identification and markings, classification prohibitions and limitations, declassification and downgrading. Both statutory law and federal regulations are subject to judicial scrutiny.

Current law provides for four levels of control over access to classified information. First, the government conducts extensive background investigations before the grant of a security clearance. This is to ensure that the "employment and retention in employment of any civilian officer or employee . . . is clearly consistent with the interests of national security."[14] Moreover, it is clear that government employees lack a property interest in a security clearance; judicial

---

[11] Executive Order 12958, 17 April 1995. The predecessor orders for Executive Order 12958 include E.O. 8381 (1940), E.O. 10104 (1950), E.O. 10290 (1951) and E.O. 12356 (1982). Louis Fisher, *In the Name of National Security: Unchecked Presidential Power and the Reynolds Case* (Lawrence, KS: University Press, 2006), 24-25.

[12] Executive Order 12958, § 1.1. (b).

[13] Executive Order 12958, § 1.1. (h).

[14] Executive Order 10450, § 2.

proceedings are not required for the revocation of a security clearance.[15] Second, government agencies typically require that employees sign non-disclosure agreements and agree to submit publications for review both during and after employment. Third, the government has a range of non-judicial sanctions that can be imposed against the miscreant employee. These sanctions include loss of access, revocation of security clearance, and the termination of employment. Finally, the government can proceed with either civil remedies or criminal prosecution. There are, however, drawbacks with judicial proceedings. The initiation of judicial proceedings can draw public attention to classified material has been improperly disclosed, exacerbating the problem. If the evidence against the miscreant employee is weak, the government runs a risk of losing the case, thereby undermining public confidence in the administration of justice and in government security practices. If the evidence against the miscreant employee is strong, defense counsel may use discovery to threaten the government with the disclosure of additional (and purportedly exculpatory) classified information. This practice, sometimes used to abort the government's decision to prosecute, is known as "gray mail."[16] Hence, the overall body of federal law should be structured for deterrent, as well as remedial, effect.

[15] *Department of the Navy v. Egan,* 484 U.S. 518, 108 S. Ct. 818, 98 L. Ed. 2d 918 (1988).

[16] The threat of disclosure by "gray mail" during a federal criminal prosecution has been greatly reduced by the Classified Information Procedures Act (CIPA), 18 U.S.C. App. 3, §§ 1-18 (2006). The CIPA permits the admission of classified documents in a federal criminal prosecution, to include discovery rights by defendants. The CIPA authorizes an adversary hearing to determine the relevance, admissibility and use of classified documents. If the Attorney General certifies that a public hearing would damage national security, the court is authorized to hold *in camera* proceedings. If a court determines that classified material is relevant and admissible, the government may move to submit a statement admitting relevant facts or provide an unclassified summary of the classified material. If the court refuses the substitution, the defendant may move for an adverse finding against the government on certain issues or for a dismissal of specified counts. The court may not, however, order the disclosure of classified information.

The power of the Executive branch to withhold documents from judicial review is known as the state secrets privilege.[17] The government has exercised this common law evidentiary doctrine to block discovery, with the result that critical evidence is sometimes denied to litigants in cases against the federal government.[18] Some argue that the doctrine has been used block the release of inculpatory evidence to plaintiffs, to block the release of embarrassing information, to shield criminal defendants and to obstruct judicial oversight of Executive action. The state secrets doctrine should not be confused with Executive privilege, a more limited doctrine that protects communication between the President and his advisers from predation by outsiders. Moreover, the state secrets doctrine operates as an absolute privilege, while the Executive privilege operates as a qualified privilege.

In *Reynolds*, the families were seriously handicapped in a tort action against the federal government and the families settled the claims at that time for a substantially lower value. In 2000, after the government declassified the accident report and other documents, the families obtained copies of the documents through the Freedom of Information Act and found that the documents apparently did not contain any classified material. In fact, the documents contained evidence that ascribed fault for the crash to the Air Force's failure comply with aircraft modification orders in the exhaust assembly and also reported that the Air Force had failed to brief the civilian contractors in proper emergency procedures. Did the government improperly

[17] *U.S. v. Reynolds,* 345 U.S. 1, 7 S. Ct. 582, 97 L. Ed. 727 (1953). In *Reynolds* the family members of personnel killed in the 1948 crash of a B-29 bomber filed a civil action under the Federal Tort Claims Act and sought discovery of a copy of the Air Force investigation report and statements from surviving crew members. The Air Force refused production, claiming that the material was classified and privileged against disclosure. The Supreme Court held that the material was privileged under the state secrets doctrine based upon the reasonable. possibility that military secrets were involved. It is, however, noteworthy that the Supreme Court sanctioned the lower court's decision to rely on government declarations without even an *in camera* review of the actual documents

[18] The state secrets doctrine was formerly used by the government to block discovery in civil and criminal cases, but the passage of the Classified Information Procedures Act has codified discovery in criminal cases leaving a problem for plaintiffs in civil litigation against the government.

classify or withhold documents to prevent disclosure of negligence? Unfortunately, the U.S. Supreme Court has declined further review of the case. One alternative to this conundrum would be to permit trial courts to make adverse inferences against the government in cases where the government invokes the state secrets doctrine to block discovery. In any event, the plaintiffs in civil litigation should not have to rely on either a leak or government largesse to obtain relevant, important information to prosecute an otherwise valid claim against the government in an Article III court.

THE FIRST AMENDMENT

The First Amendment provides that "Congress shall make no law . . . abridging the freedom of speech, or the press . . . ."[19] This seemingly direct command has spawned much case law as the federal judiciary has interpreted and applied it to cases with regard to unauthorized disclosures. Many contend that the government's efforts to restrain the expressive activity of either insiders or outsiders in possession of classified information impinge on protected constitutional rights. After Congress and Executive branch have acted to protected classified information, the federal judiciary responds to determine whether certain acts have been constitutional. The Supreme Court has not adopted an absolutist position, but has balanced the speech and anti-speech interests to minimize the abridgement of speech to the extent possible.

The Court decided many cases about information leaked from court proceedings or sources not open to the public. In so doing, the Court has devised a body of law regarding the prior restraint of free speech. The concept of prior restraint involves government restrictions

[19] *U.S. Constitution,* amend. 1.

imposed on speech or other forms of expression prior to publication or dissemination.[20] The Court has recognized that some prior restraint of content-based speech is appropriate in national security cases.[21] The Court has, however, also refrained from restraining publication in the *New York Times Co.* case.[22] Next, the Court has issued decisions regarding the confidentiality of reporters' sources.[23] Finally, the Court has ruled that once someone outside of government lawfully acquires official information, the government cannot, absent extraordinary showing, penalize that publication.[24]

In general, courts have minimized the reach of, or ruled unconstitutional, statutes that limit First Amendment freedoms if they are overbroad or vague. A law is considered unconstitutionally vague if it does not permit the ordinary citizen to determine with reasonable certainty whether his conduct is criminally punishable. For example, if a local ordinance proscribes cruising on city streets during hours of darkness, the ordinance will likely be held to vague because a person would be obliged to guess at the meaning and application of the ordinance - what is meant by "cruising". For example, if a local ordinance proscribes all

---

[20] "Prior Restraint and the Press Following the *Pentagon Papers* Cases - Is the Immunity Dissolving?" Note, 47 *Notre Dame Law* 927, 928 (1972).

[21] *Snepp*, 444 U.S. 507 (the Court awarded the government with a constructive trust under which all profits from a former CIA agent's unauthorized book went into the public treasury); *Progressive, Inc.*, 467 F.Supp. 990 (the Court enjoined publication of an article with nuclear weapons information, derived either from information in the public domain or declassified, even though the authors did not have access to classified information); and *U.S. v. Marchetti,* 466 F.2d 1309 (4th Cir. 1972) (injunction against publication, without government approval, of an ex-CIA agent's book).

[22] *New York Times Co. v. United States*, 403 U.S. 713, 91 S. Ct. 2140, 29 L. Ed. 2d 822 (1971).

[23] *Branzburg v. Hayes*, 408 U.S. 665, 92 S. Ct. 2646, 33 L. Ed. 2d 626 (1972); *Zurcher v. Stanford Daily*, 436 U.S. 547, 98 S. Ct. 1970, 56 L. Ed. 2d 525 (1978); and *Herbert v. Lando*, 441 U.S. 153, 99 S. Ct. 1635, 60 L. Ed. 2d 115 (1979).

[24] *Landmark Communications v. Virginia*, 435 U.S. 829, 98 S. Ct. 1535, 56 L. Ed.2d 1 (1978).

speeches in public parks, the ordinance will likely be held to be overbroad because it sweeps into its ambit activities that constitute an exercise of protected expressive or associational rights.

The most significant case in this area is the *New York Times Co.*, better known as the "Pentagon Papers" case. In the Pentagon Papers, the Supreme Court reviewed a petition for certiorari by the United States, seeking to enjoin the *New York Times* and the *Washington Post* from publishing the contents of a classified study (the *Pentagon Papers*) on the Vietnam War that had been by Daniel Ellsberg, who was a military analyst with the RAND Corporation. The issue in these cases was whether the government had the constitutional authority to enjoin the publication of the leaked study. The Court cited *Near v. Minnesota* for the proposition that the government "carries a heavy burden of showing justification for the imposition of such a prior restraint."[25] In the Pentagon Papers, the Court issued a short, delphic *per curium* opinion, with nine individual opinions, holding that the government had not met its burden. In sum, the value of this decision is limited by the unusual nine-way split of opinion among the Justices.

Only two Justices, Justices Black and Douglas took an absolutist position. Justice Black issued a concurring opinion noting that the First Amendment makes an emphatic command that Congress could make no law abridging the freedom of the press. Justice Black maintained that "the press must be left free to publish news, whatever the source, without censorship, or prior restraint."[26] Justice Douglas also issued a concurring opinion, noting that Congress had not

---

[25] *New York Times Co.*, 403 U.S. 713 at 714, citing *Near v. Minnesota*, 283 U.S. 697, 51 S. Ct. 625, 75 L. Ed. 1357 (1931). In *Near* a newspaper published articles that purportedly exposed the malfeasance of public officials; the State of Minnesota petitioned the court to enjoin the newspaper from publishing as "a malicious, scandalous and defamatory newspaper." The Supreme Court opined (in dicta) that in national security cases that an infringement of First Amendment rights might be tolerated, suggesting that in time of war that it might be permissible to restrict publication of troop movements or obstruction of recruiting services. Cf. *Liberty Lobby, Inc. v. Pearson*, 129 U.S. App. DC 74, 390 F.2d 489 (1968) (the court denied a preliminary injunction against a former employee of Liberty Lobby, a political lobbying organization, who allegedly removed private materials belonging to Liberty Lobby; the court held that there was no showing of either ownership or an unlawful taking of the papers).

[26] *New York Times Co.,* 403 U.S. 713 at 717.

passed a statute barring the publication by the press of the material that the *New York Times* and the *Washington Post* sought to publish. Justice Douglas noted that Espionage Act, 18 U.S.C. § 793 did not apply to the press, explaining that the word "publish" is mentioned in only three of eight sections of the Espionage Act. Finally, Justice Douglas concluded that the serious impact of the disclosures did not provide a basis for sanctioning a prior restraint.

Justice Brennan also issued a concurring opinion, explaining that there was only a very narrow of class of cases in which the First Amendment's ban on prior restraint could be overcome. Justice Brennan explained that prior restraint could only occur during time of war, to prevent obstruction of the recruiting service or to prevent publication of troop movements.

A fourth justice concurred but held a different view. Justice Marshall questioned whether the Supreme Court or the Congress has the power to make law in this area. He explained that the President had the unquestioned authority to classify information, to discipline employees who leak classified information, and to take precautions to prevent leaks. He explained that the courts and the Executive Branch could not "make" law without regard to action by Congress. He noted that the Solicitor General failed to show whether there was probable cause that a crime had been committed or whether there was a conspiracy to commit a crime. He noted that the trial judge had found that 18 U.S.C. § 793 (e) had not made it a crime to publish the proscribed materials and that the legislative history of the statute indicated that it had been intended "only to prosecute those charged with ordinary espionage."[27]

Chief Justice Burger dissented from the Court's opinion, finding that the record had not been properly developed in the lower courts. He noted that it was undisputed that the *New York Times* had unauthorized possession of the documents. Justice Harlan also issued a dissenting

---

[27] *New York Times Co.,* 403 U.S. 713 at 745.

opinion. He raised numerous questions which should have been faced by the Court, including whether the newspapers were entitled to retain and use documents stolen from the government when the newspapers had knowledge they had been feloniously acquired. Justice Harlan seemed to suggest a route that has been rarely (if ever) traveled: The government could have prosecuted the newspaper under criminal laws. There are several ways that this could have been done under current law: First, under 18 U.S.C. § 793 (e), the *New York Times* could have been deemed in "unauthorized possession," and making an attempt to communicate information to others not entitled to receive it. Second, the government could have prosecuted the paper for willful retention of documents, also a violation under § 793 (e). Third, the government could have obtained a search warrant to recover the material, followed by a criminal prosecution for receipt of stolen property. In sum, the Court did not decide the issue whether the government had the constitutional authority to enjoin publication, but rather found that the government had failed to make a proper showing in this case leaving open questions about what the government could have done.

After losing the *New York Times* case, the government apparently took the Court's advice and attempted to prosecute Daniel Ellsberg and Anthony Russo for their role in disclosing the Pentagon Papers to the *New York Times*. Mr. Ellsberg was a military analyst with the RAND Corporation; he leaked the Pentagon Papers to the *New York Times* with the assistance of Mr. Russo, who was also a RAND analyst. Both Ellsberg and Russo were indicted for espionage, theft and conspiracy. Unfortunately, the federal district court was never able to rule on the propriety of prosecuting the press for publishing classified materials. The district court dismissed the case because the government had suppressed evidence, invaded the physician-patient relationship, conducted illegal wiretapping, destroyed relevant evidence and disobeyed

court orders. In short, when the dust settled on the whole Pentagon Papers case, there were two lingering issues: 1) Could the government prosecute a member of the media under the Espionage Act?; and 2) Could a more narrowly tailored statute permit such a prosecution even if the Espionage Act did not?

It is possible for the government to obtain a prior restraint on publication in a national security case, at least with a proper factual record. In the *Progressive, Inc.* case a federal district court considered the government's request for a temporary restraining order enjoining the publishers of a magazine from communicating or otherwise disclosing allegedly restricted data contained in an article entitled "The H-Bomb Secret; How We Got It, Why We're Telling It."[28] The defendants contended that the information was in the public domain and that the First Amendment barred prior restraint. The government maintained that the national security interest permitted it to impress classification upon material in the public domain that when drawn together threatened immediate, direct and irreparable harm to the United States. The district court held that the case was within the ambit of *Near* and was distinguishable from the *New York Times Co.* case.[29] It explained that the case was distinguishable from the *New York Times Co.* because the Pentagon Papers were primarily historical data already three years old, because the government in that case had failed to advance cogent reasons as to why the publication of the Pentagon Papers would impair national security, and because a congressionally enacted statute, § 2274 of the Atomic Energy Act, authorized the government's request for prior restraint. The court noted that § 2274 prohibited anyone from "communicating, transmitting or disclosing any restricted data" with reason to believe that it would injure the United States. The court held the statute neither overbroad nor vague. The court found that publication would likely be a violation

[28] *Progressive, Inc.*, 467 F.Supp. 990 (W.D. Wis. 1979).

[29] *Near v. Minnesota*, 283 U.S. 697 (1931).

of the Atomic Energy Act. The district court held that that the government had met its burden under § 2274 and met the test of two justices in *New York Times Co.* of "grave, direct, immediate and irreparable harm to the United States."[30]

Moreover, the Supreme Court has validated prior restraint on publication by former and current government employees. In *Marchetti* a federal court of appeals considered the issue of a Central Intelligence Agency (CIA) secrecy agreement that had been abrogated by a former employee.[31] That employee, Victor Marchetti, contended that the First Amendment foreclosed any prior restraint by the CIA. The government argued that his work contained classified information concerning intelligence sources, methods and operations. The court held that the agency's secrecy contract was constitutional and reasonable. The court noted that the U.S. Congress had imposed a duty upon the DCI to protect intelligence sources and methods pursuant to 50 U.S.C. § 403(d) (3). Moreover, the court noted that "the law would probably imply a secrecy agreement had there been no formally expressed agreement, but it certainly lends a high degree of reasonableness to the contract in its protection of classified information from unauthorized disclosure."[32]

The *Marchetti* court did note, however, a distinction between classified and unclassified information. The court explained that the CIA could impose a prior restraint on classified material: the CIA must have the opportunity to review proposed publications to excise classified information; the CIA must conduct any such review promptly; and Marchetti would be entitled to judicial review of any CIA disapproval. Moreover, the court noted that the burden would be

[30] *Progressive, Inc.*, 467 F.Supp. at 996.

[31] *Marchetti,* 466 F.2d 1309 (4th Cir. 1972).

[32] *Marchetti,* 466 F.2d at 1316.

upon Marchetti to seek judicial review. On the other hand, the court explained that the CIA could not prevent disclosure of unclassified information and that such restraint would be barred by the First Amendment. Finally, the court noted that "the classification [of documents] is part of the executive function beyond the scope of judicial review."[33]

After upholding the validity of a prior restraint agreement against the First Amendment in *Marchetti*, the Court expanded the reach of that ruling in *Snepp*. In *Snepp* the Supreme Court considered the binding nature of an agreement signed by a former CIA officer, Frank Snepp, not to divulge classified information and not to publish any information without prepublication clearance from the Agency.[34] After reviewing testimony from Admiral Stansfield Turner, Director of Central Intelligence (DCI), regarding the reluctance of foreign intelligence services to exchange information with the United States, the Court found irreparable harm to the government from Snepp's failure to obtain prepublication clearance for his book even though the CIA stipulated that the book did not contain classified information. The Court held that a showing of tortious conduct, needed to support an award of punitive damages, might force the government to disclose some of the very material it sought to protect. The Court held that Snepp's fiduciary obligation extended to both the non-disclosure of classified information and the requirement for prepublication clearance of unclassified material. The Court found that the imposition of a constructive trust upon the proceeds from Snepp's book was both an appropriate remedy and an effective deterrent to future such conduct.

Both the *Marchetti* and *Snepp* cases involved administrative pre-clearance, a form of prior restraint that has been traditionally disfavored under First Amendment case law. Indeed, it

[33] *Marchetti,* 466 F.2d at 1317.

[34] *Snepp*, 444 U.S. 507 (1980).

could be termed a form of censorship. First, it should be noted that the secrecy agreements are in the nature of contract. In terms of classified information, Mr. Marchetti and Mr. Snepp lacked any pre-existing right to such information - each gained access only by virtue of his employment agreement. The government had, therefore, a reasonable expectation that each would comply with that employment agreement. Second, the Court in *Snepp* validated the agreement as to both classified and unclassified material. In *Marchetti* the court indicated that the agency had the right to review material, but could only withhold clearance for publication as to classified material. Third, the court in *Marchetti* provided helpful guidance, setting guidelines for the exercise of administrative discretion and an appeals process.

The CIA subsequently established a pre-publication review process that implements the *Marchetti* and *Snepp* decisions.[35] In fact, the *Marchetti* case became the benchmark for the agency's highly successful pre-publication review program: the agency limits the reviews to that necessary to protect agent cover, liaison relationships, and intelligence sources and methods. The review program facilitates publication of unobjectionable material while protecting intelligence activities. The result is a better informed public, but without the publication of information that can serve no legitimate purpose.

A 2006 case may test the limits of the government's power established in *Snepp* and *Marchetti*. Thomas Waters, a former CIA employee, submitted a manuscript to the agency for pre-publication review. Initially, the agency took over 90 days to respond to his submission, but

[35] John Hollister Hedley, "Secrets, Free Speech, and Fig Leaves," *Studies in Intelligence,* unclassified edition (Spring 1998): 75-83. On a historical note, in 1933 Herbert O. Yardley, a former governmnent code breaker for the U.S. governmnent, proceeded to publish a book about his experiences. Unfortunately, existing law did not permit action against him. The Department of Justice brought the publisher before a federal grand jury, but the Department did not pursue an indictment believing that the Espionage Act of 1917 would not block the publication. Instead, the U.S. Congress passed 18 U.S.C. § 952 which criminalizes acts involving diplomatic codes and correspondence. The *Marchetti* and *Snepp* decisions provide the governmnent with more effective tools for handling the modern Mr. Yardleys.

did so with an eight-page letter detailing information that had been determined to be inappropriate for disclosure. Waters made the changes and disseminated the text.[36] The Agency enjoined him from publishing. Waters subsequently filed a civil action for injunctive and declaratory relief asserting that the agency violated his First Amendment rights. Waters averred in his complaint that the agency reclassified a substantial amount of the previously approved text, failed to justify its actions, and refused to allow his attorney the opportunity to review the challenged manuscript sections.[37]

The CIA reportedly contends that the plaintiff's counsel lacks a need-to-know the document contents even when classification challenges are being litigated. Some persons, to include Mr. Waters' attorney, contend that the prepublication review process has recently become more time consuming and conservative, but this assertion has been denied by the agency.[38] This case raises several issues: What constitutes prompt review by the CIA's Publications Review Board? Did Waters disseminate the manuscript before final agency approval? Can the agency reclassify material that was previously approved for release? Does the plaintiff have a right to demand access by his attorney to the challenged material? The Waters case may cause the agency to alter the publications review process.

---

[36] Thomas J. Waters, *Class 11: Inside the CIA's First Post-9/11 Spy Class* (New York: Penguin Group, 2006). The rear jacket of the book states: "Filled with more information about the Clandestine Service Training Program than has ever been allowed into the public domain, *Class 11* is a fascinating and moving portrait of an extraordinary group of Americans with the courage and resolve to make a difference in the war on terror."

[37] *Waters v. CIA*, Civil Action No. 06-383 (D.D.C.) (RBW), URL: <http://www.fas.org/sgp/jud/waters030306.pdf>, accessed 22 October 2006.

[38] Scott Shane and Mark Mazzetti, "Moves Signal Tighter Secrecy Within C.I.A," *New York Times,* online ed., 24 April 2006, URL: <http://64.233.161.104/search?q=cache:iMX3NAcvnRoJ:www.thepowerhour.com/news2/secrecy_cia.htm+%22moves+signal+tighter+secrecy+within+C.I.A.%22&hl=en&gl=us&ct=clnk&cd=4>, accessed 1 November 2006.

PRIOR RESTRAINT

The prior restraint doctrine originated in early English common law. In 1501 Pope Alexander II issued a papal bull that prohibited unlicensed printing. In 1538 Henry VIII issued a proclamation that subjected the English press to licensing - all material had to be submitted to a censor for official approval prior to publication. The English Licensing Act of 1662 made it a criminal offense to publish without a license. The act was abandoned, primarily because of problems in administration. Blackstone, the preeminent scholar of the English common law, noted that the freedom of the press is based upon no previous restraint upon publication rather than freedom from censure for criminal reasons after publication.[39] Here stood matters when the U.S. Constitution was ratified.

Professor John Jeffries observed that the seminal case of *Near* invalidated an odd statute that authorized judicial abatement of newspapers under a vague standard.[40] Hence, the problem was with the standard for suppression, not in the form of the proceeding (i.e. a court sitting in equity issuing injunctive relief). Professor Jeffries found three coherent lines of case law under the prior restraints doctrine: the use of permit requirements to control distribution of literature; the use of injunctive relief as in *Near* and *New York Times Co.*; and the application of gross receipt taxes on newspapers as a guise to limit the circulation of information.

The laws proscribing the unauthorized disclosure of classified information can operate in the form and manner of a traditional prior restraint on publication. The *Progressive, Inc.* case

[39] Sir William Blackstone (July 10, 1723 – February 14, 1780) was an English jurist who produced an important treatise on the common law called *Commentaries on the Laws of England*, first published in four volumes over 1765–1769. It had an extraordinary success and is still an important resource on English common law.

[40] John Calvin Jeffries, "Rethinking Prior Restraint," 92 *Yale L.J.* 409 (1983).

involved a narrowly drawn statute and a likelihood of irreparable harm with a factual record that had been developed through an adversarial hearing in the trial court. The *Snepp* case operated as an application of a prior restraint, but the Court found it unobjectionable based upon Mr. Snepp's fiduciary obligation and the uncontroverted testimony of Admiral Turner concerning the harm caused to the government by his breach of duty. Mr. Snepp was, however, the source of the leaked material. In the case of journalists, lobbyists and academics who receive leaked material, the anti-leak laws can be best characterized as an indirect or secondary form of prior restraint.

There are two lines of prior restraint case law that have application to the unauthorized disclosure of classified material. The first line of case law involves injunctive relief as discussed in the *New York Times Co.* and *Progressive, Inc.* cases. In the case of either a temporary restraining order or an injunction, the decision to censor is made by a judge not an administrative official.[41] Moreover, injunctive relief runs less risk of over-breadth because of the focus on a specified person or organization ordering the non-publication of specified material, all with the opportunity for an adversary hearing. If, however, the court issues a temporary restraining order, the risk of overbreadth could be *de minimus* because of the order's limited duration. The *Progressive, Inc.* involves unclassified material and persons not bound by an employment agreement, but the application of a statute and a relatively high degree of harm that could ensue. Indeed, in the *New York Times Co.* case Justice Douglas indicated that he might have voted differently if 18 U.S.C. § 793 had contained the word "publish."[42] The *New York Times Co.* case should be interpreted as a problem involving the lack of an applicable statute, as well as the

[41] The use of an administrative official raises the specter of official censorship with a risk of arbitrary decision-making by an official biased in favor of the government.

[42] 18 U.S.C. § 793 is part of the Espionage Act of 1917. For example, § 793 proscribes various acts related to gathering, transmitting or losing national defense information, and § 794 proscribes various acts related to gathering or delivering national defense materials or information.

inadequate development of the record in the trial court as to the classification of the material, how it was procured by the newspaper and the potential harm that could ensue from publication.

The second line of case law involves administrative pre-clearance as discussed in *Marchetti* and *Snepp*. The case law shows that pre-clearance can be appropriate in national security cases, but the standards must be narrowly drawn, reasonable, and definite. If pre-clearance is to be applied to unclassified material, the employment agreement should set a standard for administrative review and an appeals process. In short, the application of pre-clearance to unclassified material could be unconstitutionally overbroad if it reaches substantially beyond the permissible reach of legislative regulation. Pre-clearance is appropriate where material can not enter the marketplace of ideas even for a single day.

While the courts have held that some form of prior restraint is appropriate in national security cases and that limited restraint can be imposed against persons with a fiduciary obligation to the government and against the media, more issues arise once that information has been disclosed to a third person and the government seeks the identity of the source. It is also noteworthy that the courts make an important distinction between prior restraint and subsequent punishment. In *Near* the court stated: "Liberty of speech, and of the press, is also not an absolute right, and that the State may punish its abuse."[43] A federal shield law for journalists does not currently exist, although at least 31 states have laws protect reporters from being compelled to testify or disclose sources.[44] Conceivably, a federal shield law would not protect reporters who receive national security information.

---

[43] *Near,* 283 U.S. at 708.

[44] Associated Press, "Bill to create federal shield law introduced in House," *Associated Press,* online ed., 2 February 2005, URL: <http://64.233.161.104/search?q=cache:lZ-VVPp2YQAJ:www.firstamendmentcenter.org/news.aspx%3Fid%3D14782+%22bill+to+create+federal+shield+law+introduced+in+house%22&hl=en>, accessed 19 January 2006.

In *Branzburg* the Supreme Court considered whether journalists could be compelled to appear before a federal grand jury and give testimony regarding persons who produced marijuana.[45] On November 15, 1969, a Louisville newspaper carried an article with photographs showing an unidentified person working at laboratory table with a substance identified as hashish. Apparently, the journalist had interviewed the person upon the express agreement that he would not reveal the identity of the hashish makers. The journalists contended that they could not be compelled to testify claiming that "the burden on news gathering resulting from compelling reporters to disclose confidential information outweighs any public interest in obtaining the information."[46]

The Court noted, however, that the case did not involve an intrusion on the freedoms of speech or assembly or a prior restraint on publication. To the Court a newspaper is not free to publish with impunity any and all that it desires. The Court explained "that the great weight of authority is that newsmen are not exempt from the normal duty of appearing before a grand jury and answering questions relevant to a criminal investigation."[47] The Court noted that grand juries are constitutionally mandated for the institution of federal criminal proceedings and have broad investigate powers precisely because they are tasked to inquire into the existence of possible criminal conduct. The Court clarified that while the theft of documents or private wiretapping could provide newsworthy information, "neither reporter nor source is immune from conviction for such conduct, whatever the impact on the flow of news. Neither is immune, on First Amendment grounds, from testifying against the other, before the grand jury or at a

[45] *Branzburg*, 408 U.S. 665 (1972).

[46] *Branzburg*, 408 U.S. at 681.

[47] *Branzburg*, 408 U.S. at 685.

criminal trial."[48] Next, the Court noted that agreements not to divulge the source of information could be construed as misprision of a felony.[49] In short, the Court held that reporters do not have a constitutional privilege against testimony in a grand jury proceeding.

Justice Douglas dissented, concluding that a newsman does have an absolute right not to appear before a grand jury. He believed that public discussion of public issues should be unabridged by the government. Justice Stewart "respectfully" dissented, taking swipes at the Court's "crabbed view" of the First Amendment and "disturbing insensitivity to the critical role of an independent press in our society."[50] He believed that government should be required to show that there was probable cause that the newsman had information clearly relevant to a specific probable violation; that the information could not be obtained by less intrusive means; and that the government had a compelling and overriding interest in the information.

The next issue is whether the First Amendment protects reporters who are witnesses to criminal activity from producing potentially relevant evidence. In *Zurcher* the Supreme Court reviewed the search, pursuant to an otherwise valid warrant, of the offices of the *Stanford Daily* newspaper for photographs of the persons involved in an assault on police officers trying to break up an on-campus demonstration on April 9, 1971.[51] On April 11, the newspapers printed an article with photographs showing the demonstration. Moreover, the article indicated that a Daily staff member had been in a position to photograph the assailants. The police then searched the newspaper officers and the newspaper claimed a constitutional violation of its rights. The

---

[48] *Branzburg*, 408 U.S. at 691.

[49] *Branzburg*, 408 U.S. at 696, citing 18 U.S.C. § 4. Misprision of a felony has been defined at common law as the concealment of a felony which a person knows of but fails to make known to a judge or other authority.

[50] *Branzburg*, 408 U.S. at 725.

[51] *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978).

Court noted that the state's interest in enforcing the criminal law and recovering evidence is the same whether the third party is culpable or not. The Court explained that the critical element in a reasonable search is whether "there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought."[52] The Supreme Court held that the First and Fourteenth Amendments do not bar a state from issuing a search warrant "because of the owner or possessor or the place to be searched is not reasonably suspected of criminal involvement."[53] Justices Stewart and Marshall dissented, noting that the protection of sources is an important aspect of the freedom of the press and the evidence was not contraband but material obtained in the normal course of business. The dissenting justices would have preferred the use of a subpoena *duces tecum* over a search warrant, thereby permitting a newspaper with an opportunity to bring a motion to quash with an adversarial hearing prior to production of the sought after material.

In *Landmark Communications* the Supreme Court considered a state criminal conviction of a newspaper editor who accurately reported on a pending judicial inquiry into the conduct of a named judge.[54] Moreover, the editor lawfully acquired the information pertaining to the judicial proceedings. The Court noted that the case did not involve prior restraint, but rather subsequent criminal punishment. The Court explained that a major purpose of the First Amendment is to protect the free discussion of governmental affairs. The Court saw the issue as not whether the confidentiality of the commission served a legitimate state interest, but whether those interests were sufficient to justify encroaching on First Amendment guarantees. The Court held that the

[52] *Zurcher*, 436 U.S. at 556.

[53] *Zurcher*, 436 U.S. at 560.

[54] *Landmark Communications v. Virginia*, 435 U.S. 829 (1978).

First Amendment does not permit the criminal punishment of third persons who are strangers to the proceedings before such a commission for disclosing truthful information about the confidential proceedings. On other hand, where a statute punishes the disclosure of information unlawfully obtained, the government's interests should prevail and the statute should be held constitutional.

EXISTING STATUTORY LAW

The U.S. Congress has passed a series of statutes relevant to the problem involving the unauthorized disclosure of classified information.[55] While the President has inherent powers under Article II, U.S. Constitution, to conduct foreign policy and to perform duties as Commander in Chief, the Court has ruled that Presidential power is maximized in areas where the Congress has passed enabling legislation.[56] The Court explained that Presidential power must be based upon either the Constitution or an act of Congress, but no such authority existed for the President's action. Hence, the Court held that the order could not stand.

This nature of Presidential power could, as an example, explain the difference in results between the *New York Times Co.* and *Progressive, Inc.* cases. In *New York Times Co.* three justices indicated they might uphold a prior restraint if there were a statute authorizing such a proceeding.[57] In short, *New York Times Co.* should not be cited for the proposition that injunctive relief is inappropriate in First Amendment cases. Moreover, statutes that focus on

[55] *See generally* Appendix A, Table of U.S. Statutes.

[56] *Youngstown Sheet & Tube Co. v. Sawyer,* 343 U.S. 579, 72 S. Ct. 863, 96 L. Ed. 1153 (1952).

[57] *New York Times Co.,* 403 U.S. 713 at 730 (Stewart, J., concurring), at 740 (White, J., concurring), and at 746-47 (Marshall, J., concurring).

subsequent punishment vice prior restraint stand on stronger constitutional grounds. Indeed, certain forms of expressive activity (i.e. libel and obscenity) have been the subject of subsequent punishment and have received reduced constitutional protection.

The Espionage Act of 1917

The most common statutes for criminal prosecution for espionage are under the Espionage Act of 1917, 18 U.S.C. §§ 793, 794, 798 and 952. The government has used these statutes to prosecute classic espionage cases; namely, those people engaged in selling secrets to agents of foreign powers (see Appendix B, Table of Leak and Espionage Cases). The key statutes for both espionage and leak cases have been 18 U.S.C. §§ 793 and 794. Robert Pelton and Wen Ho Lee were prosecuted under § 793, while traditional spies like Jonathan Pollard, Aldrich Ames, Harold J. Nicholson, Robert Hannsen and Ana Montes were prosecuted under § 794. There have been no reported prosecutions under 18 U.S.C. §§ 795-797 or 953. Under 18 U.S.C. § 3282 there is a five-year statute of limitations for most non-capital federal criminal offenses. It is noteworthy that both §§ 793 and 794 have an extended, ten-year statute of limitations and that most persons convicted under these sections have received lengthy prison terms. Under either § 793 (g) or § 794 (c) the recipient of leaked information can be prosecuted under a conspiracy theory.

Section 793 applies to acts of gathering, transmitting or losing national defense information. Section 793 (a) applies to all persons and proscribes the gathering of defense information "while upon places connected with national defense . . . ." Section 793 (b) applies to all persons and proscribes copying, taking, making or obtaining national defense information.

Section 793 (c) applies to all persons and proscribes the receipt or attempted receipt of material connected with the national defense, knowing or having reason to know that the material has been or will be illegally obtained. Section 793 (d) applies to persons who, having lawful possession of or access to national defense material, and it proscribes the communication of such material to persons "not entitled to receive it." Section 793 (e) applies to persons having unauthorized possession of national defense material, and who either communicate it to others not entitled to receive it or willfully fail to deliver it to a federal officer.[58] Section 793 (f) applies to persons, either entrusted with or having lawful possession of national defense materials, who permit the materials to be removed from the proper place of custody and lost, stolen or destroyed. The penalty for a violation of Section 793 is imprisonment for up to ten years or a fine or both, and forfeiture of any foreign proceeds. Clearly, the forfeiture provision is appropriate for espionage cases, but would be less useful in leak cases.

Section 794 is applicable to gathering or delivering national defense materials or information. Section 794 (a) deals with the transmission of national defense material "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." Under Section 794 (a) a person can be punished by death but only upon a finding that the offense resulted in the death of a covert agent, concerned nuclear weapons or involved certain elements of national defense. Unlike § 794 (b), § 794 (a) is not

[58] Recently, a federal prosecutor made a demand upon the American Civil Liberties Union (ACLU) for return of a classified document that the ACLU admittedly has. After the ACLU failed to return the document, a federal grand jury issued a subpoena on the ACLU for "any and all copies" of the document it received in an unsolicited electronic mail. The ACLU has moved to quash the subpoena, claiming that political advocacy groups are entitled to the same constitutional protections that journalists receive and that the document was not "related to the national defense." The federal district judge has not yet ruled on the motion to quash, but the government appears to have statutory authority for its action under 18 U.S.C. § 793 (e). Moreover, the government appears to be following a sound discovery strategy that could help identify leakers and reassert government control over leaked documents. Adam Liptak, "U.S. Subpoena Is Seen as Bid to Stop Leaks," *New York Times*, online ed., 14 December 2006, URL: <http://www.nytimes.com/2006/12/14/washington/14leak.html?_r=1&oref=slogin>, accessed 15 December 2006. The government has, however, mooted the issue by declassifying the document. ACLU, " Government Backs Down in its Attempt to Seize "Secret" Document From ACLU," 18 December 2006, URL: <http://www.aclu.org/safefree/general/27727prs20061218.html>, accessed 30 December 2006.

limited to wartime.[59] Section 794 (b) applies to persons who, "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 military movements. Under § 794 (b) a person can be punished by imprisonment for years or a fine or death.

The *Gorin* case demonstrates the vagueness problem in §§ 793-94 cases.[60] *Gorin* is also a "classic" espionage case and the only case in which the Supreme Court has considered the constitutionality of the Espionage Act. Gorin, a covert Soviet agent, collected wartime information concerning local Japanese activities from an employee in the San Pedro branch of the Office of Naval Intelligence. Both persons were indicted under §§ 793-94 for obtaining counterintelligence documents, and for delivering and inducing the delivery of the documents to Gorin. Both Gorin and his accomplice were convicted on each count. On appeal to the Supreme Court, Gorin argued that the term "related to the national defense" as used in § 793(b) and § 794(a) had to be read in conjunction with § 793(a) that defined "national defense" in terms of protected places. The Court reviewed the statutory language to determine whether the language "connected with the national defense" was overbroad and whether the issue was properly left to the jury. The Court explained that in each section of the Espionage Act the document or other protected thing, in addition to the places, must be "connected with the national defense." The

[59] By contrast, a member of the Armed Forces can be convicted of espionage by general court martial and sentenced to death if "the accused knowingly created a grave risk of substantial damage to national security" or if "the accused created a grave risk of death to another person." In short, a member of the Armed Forces can be punished by death for the same offense that a case officer in the National Clandestine Service could not be. Article 106 (c), *Uniform Code of Military Justice*, URL: <http://www.au.af.mil/au/awc/awcgate/ucmj2.htm>, accessed 8 November 2006.

[60] *U.S. v. Gorin*, 312 U.S. 19, 61 S. Ct. 429, 85 L. Ed. 2d 488 (1941).

Court found "no uncertainty in this statute which deprives a person of the ability to predetermine whether a contemplated action is criminal under the provisions of the statute."[61]

The most troublesome aspect of *Gorin* is the Supreme Court's treatment of the relationship between secrecy and the statutory standard of defense-relatedness. The Court answered the culpability problem: "Where there is no occasion for secrecy . . . there can, of course, in all likelihood be no reasonable intent to give an advantage to a foreign government."[62] Thus, the *Gorin* court read a classification requirement into the statute and held that the statute's culpability requirement was adequate to fend off the dangers of over-breadth. Moreover, the court's reading of a classification requirement into the statute is contrary to both a plain reading of the statute and the legislative history. This case may, however, be an example of the Court's self-imposed "duty to construe a federal statute to avoid constitutional questions where such a construction is possible."[63] In short, the *Gorin* court narrowed a statute that is probably facially over-broad.

The Court's willingness to read a secrecy requirement into statute is somewhat remarkable in view of the legislative history. The earliest version of § 794 is contained in Senate Bill 8148, as part of the overall history of the passage of the 1917 Espionage Act. Senate Bill 8148 contained a proviso that authorized the President to designate protected information so that

---

[61] *Gorin*, 312 U.S. at 27.

[62] *Gorin*, 312 U.S. at 28. The reasoning of the *Gorin* court was followed in *U.S. v. Heine*, 151 F.2d 813, *cert. denied*, 328 U.S. 833 (1946). The *Heine* case involved German-born, naturalized U.S. citizen who collected open source information on the U.S. aircraft industry and sent that information back to Germany before the United States declared war on Germany. While the information obviously concerned national defense and was to be used to advantage a foreign nation, the court concluded that it was "obviously lawful to transmit any information about weapons and munitions of war which the services had themselves made public." *Heine,* 151 F.2d at 816. The court concluded that the wording "related activities of national preparedness" created a "penumbra of some uncertainty," but cited *Gorin's* reliance on secrecy in determining the applicability of the Espionage Act to the case at bar. *Heine,* 151 F.2d at 817.

[63] *Arnett v. Kennedy*, 416 U.S. 134, 162, 94 S. Ct. 1633, 40 L. Ed.2d 15 (1974).

only authorized persons might receive it, but this terminology was defeated because opponents feared granting the President broad rule-making authority.[64] In effect, this rule-making authority would have accomplished two things: it would have established a classification system that defined material "connected with the national defense" and also clarified persons entitled to receive that material. In other words, this grant of authority would have provided the President with authority to prescribe categories of defense information that were protected from disclosure and avoiding the dangers of statutory over-breadth. As it turned out, the United States did not establish a classification system until 1951 and then did so by Executive Order. Unfortunately, a classification finding is still not dispositive of defense-relatedness under the statute: The statute does not address either the problem of embarrassing information that is improperly classified to prevent public release or the problem of unclassified defense information that should not be released for otherwise legitimate reasons.

In *Boyce* the Defendant contended that documents pertaining to America's satellite program did not relate to national defense within the meaning of 18 U.S.C. §§ 793-94 and that the documents were not classified within the meaning of 18 U.S.C. § 798.[65] The court cited *Gorin* for the proposition that "national defense" has a broad, generic meaning that includes more than the military establishment. The court also concluded that the propriety of the classification is irrelevant under § 798. The fact of classification is enough to satisfy that element of the offense.

---

[64] Harold Edgar, "The Espionage Statutes and Publication of Defense Information," 73 *Columbia Law R.* 929, 947-952 (1973).

[65] *U.S. v. Boyce*, 594 F.2d 1246 (9th Cir.), *cert. denied*, 444 U.S. 855 (1979).

Subversive Activities Control Act

In 1950, in response to the perceived threat of communist subversive activities, the U.S. Congress passed the Subversive Activities Control Act (50 U.S.C. § 781 et. seq.). This act required members of the Communist Party to register with the Attorney General, mandated that certain organizations register printing equipment with the government, and directed named organizations had to provide certain information to the government. This act was a clear restraint of protected First Amendment activity and many aspects of the act were later ruled unconstitutional by the U.S. Supreme Court. Table A includes §§§ 781, 782 and 783, although all three sections were terminated on September 14, 1978 pursuant to 50 U.S.C. § 1601.

Theft Statute

In general, the government has tried to apply 18 U.S.C. § 641 to the unauthorized disclosure of government information based upon two separate theories. The first theory is based upon the larceny of property, a theory that has validity in terms of tangible documents such as the *Morison* or *Tobias* cases. Here, the property could be either the photograph itself or the government supplies that were used to make an illicit duplicate copy. In either case, the government would have to prove the market value for the final, leaked product. The second theory is based upon the common law action of trover, the conversion of property that occurs when someone interferes with an owner's rights to the extent that compensation is justifiable. Here, the interference could be the unauthorized disclosure of information. The argument is that the misuse of information is akin to theft because the government has been deprived of the

benefits of ownership. The opposing argument is that where the intermeddling falls short of a substantial deprivation of possessory rights in the property (such as in the reproduction of documents), the tort committed is not conversion, but rather the lesser wrong of trespass to chattels.[66] Under either theory, the government must prove that the information had some value and the leak diminished that value, that the accused acted with criminal intent, and that the disclosure was affirmatively prohibited by federal law. In cases where a leaker sells classified information for a financial gain, the government has to prove the value of the information. In the more typical case, where information is not sold, the government faces a challenge trying to prove the independent value of the information.

There have been some prosecutions under the Theft Statute, 18 U.S.C. § 641, but this statute is an odd tool for prosecutors to be using in disclosure cases. The Theft Statute has been used in the prosecutions of Christopher Boyce, Truong Dinh Hung, Ronald Humphrey, Samuel Morison, Michael Tobias and Jonathan Randel; of the six, only Christopher Boyce and Michael Tobias received lengthy prison sentences. Randel pled guilty to theft for disclosing Drug Enforcement Administration (DEA) sensitive material and was sentenced to one year.[67] It is not, however, clear whether the Theft Statute is properly applied to the unauthorized disclosure of classified information and, in some cases, the appellate courts have declined to rule on the propriety of a § 641 conviction based upon rules of judicial economy. In *Boyce*, for example, the Defendant also contended that § 641 was inapplicable to intangible interests, but the court

[66] Melville E. Nimmer, "National Security Secrets v. Free Speech: The Issues Left Undecided in the Ellsberg Case," 26 *Stanford Law Review* 311, 319 (1974).

[67] Robin R. McDonald, "DEA Employee Gets Prison Term for Leaking to Reporter." Law.Com, 15 January 2003, URL: http://www.law.com/jsp/article.jsp?id=1042568651135>, accessed 29 August 2006.

declined to consider that argument under the concurrent sentence doctrine.[68] The U.S. Court of Appeals for the 9th Circuit has declined to apply 18 U.S.C. § 641 to intangible property.

In *Hung* the court considered the convictions of Robert L. Humphrey and Truong Dinh Hung and the Theft Statute.[69] Humphrey was an employee of the United States Information Agency who passed classified information to Hung, who was a Vietnamese agent. Both were convicted of conspiracy to convert classified government documents and conversion, in violation of 18 U.S.C. §§ 371 and 641, as well as violations of the 18 U.S.C. § 793(e). The Court of Appeals for the Fourth Circuit found that the defendants had been properly convicted under the Espionage Act, but concluded that the case should be remanded for consideration of potential exculpatory statements under the Jencks Act. The court noted that the defendants had been convicted under the Theft Statute, 18 U.S.C. § 641, on the theory that they had converted government property. The defense theory was that information could not be converted because the common law tort of conversion requires that the legitimate owner be deprived of possession and that information is an intangible not encompassed by § 641, which speaks of "tangible" things of value. The Fourth Circuit suggested, in dictum, that national defense information is not government property within the meaning of § 641. The majority concluded that the defense contentions need not be considered under the concurrent sentence doctrine; Judge Hall dissented on that issue.

Judge Hall persuasively explained that the legislative history of 18 U.S.C. § 641 does not mention the application of the statute to the theft of government information. He did note,

---

[68] The concurrent sentence doctrine provides that where a defendant receives concurrent sentences on plural counts of a criminal indictment and where one conviction is found to be valid, a reviewing court need not pass on the validity of the concurrent sentence. In effect, the doctrine is a means of avoiding the expenditure of judicial resources on the unnecessary decision of an issue. *U.S. v. Hung,* 629 F.2d 908, 931(4th Cir. 1980), *cert. denied*, 454 U.S. 1144 (1982).

[69] *Hung,* 629 F.2d at 931.

however, that Congress intended the § 641 to be all-inclusive and that the leading decisions of the Supreme Court have held that the statute sweeps broadly, avoiding inconsequential distinctions that the culpable could use to avoid criminal liability. He explained that § 641 must be applied to the theft of government information with extreme care: First, "Section 641 is not carefully crafted to specify exactly when disclosure of government information is illegal" - impinging on First Amendment rights. Second, there exists a "potential for this statute to conflict with other statutes specifically addressed to the disclosure of government information."[70] He noted that § 641 does not contain a stringent scienter requirement and would encompass a broad class of persons. He would have held that the "thing of value" language in § 641 could not be read to include classified information.

In *Tobias* the Court of Appeals for the Ninth Circuit reviewed the propriety of a conviction under § 641 for theft of classified cryptographic cards and espionage; he was convicted under 18 U.S.C. §§ 371, 641, 793 and 798.[71] Tobias took cryptographic cards that had been marked for destruction and tried to sell them. The court noted that the Ninth Circuit had declined to apply § 641 to intangible goods like classified information because of First Amendment concerns. The court concluded that the cards were not without value because they could still be useful to a foreign power. The court found the cards to be tangible goods and affirmed the conviction.

[70] *Hung,* 629 F.2d at 925.

[71] *U.S. v. Tobias,* 836 F.2d 449 (9th Cir. 1988).

Signals Intelligence Statute

The United States does have something akin to an official secrets act, but it applies only to signals intelligence (SIGINT). Section 798 criminalizes the disclosure of classified information regarding codes, ciphers or cryptographic or communications intelligence systems by anyone who "knowingly and willfully communicates, furnishes, transits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interests of the United States" to any unauthorized person. Moreover, a violation of this statute is punishable by 10 years imprisonment. This statute broadly proscribes leaks and further publication of SIGINT material and information. Note, however, the scienter requirement makes it applicable only to intentional leaks. Leaks due to carelessness fall outside the statute.

Invention Secrecy Act of 1951

The Commissioner of Patents has statutory authority pursuant to 35 U.S.C. § 181 to place a patent under a secrecy order if, in the opinion of the interested government agency, the publication or disclosure of either the application or the grant of the patent would be detrimental to national security. If the Commissioner imposes such a secrecy order upon a patent in which the government lacks a property interest, the owner has the right of appeal to the Secretary of Commerce. If, however, a person willfully publishes or discloses the invention, with knowledge of the secrecy order, that person may be punished by a fine of $100,000.00, imprisonment for up to two years, or both.

Unauthorized Retention Statute

Any federal officer, employee or contractor, who comes into the possession of classified documents or materials and who "knowingly removes such documents or materials without authority and with the intent to retain such documents or materials" shall be punished fine or imprisonment for up to one year or both, according to U.S.C. § 1924. This code section closely parallels 18 U.S.C. § 2071 which proscribes the willful concealment, removal or mutilation of any record, proceeding, map, book, paper, document or other thing filed or deposited in any public office. Section 2071 is clearly a broader statute and is punishable by a fine of up to $2000.00 or imprisonment for three years or both. Moreover, a person convicted under § 2071 forfeits any office under the United States, an additional penalty not available under § 1924. Thus it is a misdemeanor to remove classified documents from government facilities providing there was an intent to retain the documents. Leakers could be prosecuted under this statute.

The Atomic Energy Act

The Atomic Energy Act, 42 U.S.C. §§ 2274-2277, has been an effective prosecutorial tool in unauthorized disclosure cases relating to nuclear material. Sections 2274-2276 have an extended ten-year statute of limitations. The broad language of this statute was used to good advantage in the *Progressive, Inc.* case to justify injunctive relief against the periodical.

Intelligence Identities Protection Act

On 23 June 1982 President Ronald Reagan signed the Intelligence Identities Protection Act (IIPA) (50 U.S.C. § 421 et. seq.) into law. This statute was the product of several years of work by the Central Intelligence Agency to provide legal protection for Directorate of Operations personnel serving under cover. This legislation came about, at least in part, because a former CIA officer, Philip Agee, and others had been publicizing the names, addresses and biographical information of CIA officers serving overseas. Mr. Agee and Louis Wolf, both U.S. citizens, disclosed this information in periodicals such as *Counterspy, Quicksilver Times* and the *Covert Action Information Bulletin*. Mr. Agee also wrote a book, *Inside the Company: CIA Diary*, which was published in 1975 in England. The public disclosures led to the 1975 murder of Richard S. Welch, the CIA Station Chief in Athens, and the 1980 attack on N. Richard Kinsman, the CIA Station Chief in Kingston, Jamaica. Unfortunately, there existed no law at the time that would have permitted the prosecution of those responsible for the disclosure of the officers' names.

In July 1980 the House Permanent Select Committee on Intelligence (HPSCI) passed a bill to outlaw the publication of information that identifies a covert agent. Despite some pressure from media organizations about the constitutionality of the proposed legislation, the bill eventually passed through the U.S. Congress and was signed into law as the Intelligence Identities Protection Act (IIPA) of 1982. The law has had some positive effect, but limited effect since it was signed into law: Sharon Scranage was prosecuted and sentenced in 1985 after she revealed the names of CIA assets in Ghana, and Sergeant Clayton Lonetree was convicted in 1987 after he disclosed the names of CIA officers serving in Austria. Finally, there is the

pending investigation into the public disclosure of Valerie Plame as a CIA officer. It is noteworthy that the statute applies to persons "as a result of having authorized access to classified information" who disclose such information to persons not authorized to receive it. Under § 421(c) the statute also applies to news organizations who engage in a pattern of activities intended to identify and expose covert agents, but this standard raises difficult problems of proof. In fact, persons need not have had authorized access to classified information to be prosecuted under this section.

Section 421 (a) applies to persons, having or having had authorized access to classified information that identifies a covert agent, who intentionally disclose any information identifying that agent to any individual not authorized to receive classified information. A violation of this sub-section is punishable by a fine or imprisonment for not more than ten years or both. Section 421 (b) applies to persons, having or having had authorized access to classified information and who learn the identity of a covert agent, who then intentionally disclose any information identifying that agent to any individual not authorized to receive classified information. A violation of this sub-section is punishable by a fine or imprisonment for not more than five years or both. Section 421 (c) applies to persons who disclose the identity of a covert agent learned through a pattern of activities intended to identify and expose covert agents. A violation of this sub-section is punishable by a fine or imprisonment for not more than three years or both. For the purposes of this statute, the term covert agent applies only to persons serving outside the United States within the preceding five years.

There has also been some question raised as to whether the IIPA is constitutional. Susan Charkes notes that the Act is divided into two distinct conceptual categories: disclosure by

intelligence community insiders and disclosures by members of the public.[72] Ms. Charkes notes that sub-sections 421(a) and (b) apply to insiders and concluded that those sub-sections were probably constitutional if applied to insiders being punished for the effective disclosure of classified information learned through inside access. She also notes that sub-sections 421(a) and (b) required fewer elements of proof and imposed harsher sanctions than sub-section 421(c). She contends that a statute, here sub-section 421(c), cannot constitutionally punish the disclosure of classified information obtained lawfully by an outsider without proof of significant harm. She maintains that disclosures pertaining to illegal activities are protected under the First Amendment. In sum, she contends that sub-section 421(c) is over-broad.

On the other hand, one can argue that the reasoning of the Supreme Court in *Landmark Communications, Inc.* is inapposite because the government identified a narrow category of information (names of covert officers), severely limiting the encroachment on First Amendment guarantees. Moreover, the legislative history of the IIPA provides ample evidence of significant harm that can befall a named agent as well as a strong national interest in protecting his identity. The U.S. Congress crafted the IIPA to meet a "substantive evil [that is] extremely serious and the degree of imminence extremely high …."[73] The reach of the Act is limited, however, by its own strict definitions including who is a "covert agent" under the Act.[74] The IIPA likely meets the standards for constitutionally valid content-based restrictions under *Sable Communications.*[75]

---

[72] Susan D. Charkes, "The Constitutionality of the Intelligence Identities Protection Act," 83 *Columbia Law Review* 727 (1983).

[73] *Landmark Communications*, 435 U.S. at 845.

[74] 50 U.S.C. § 426 (4).

[75] *Sable Communications of California*, 492 U.S. at 126.

PROSECUTIONS UNDER CURRENT LAW

Morison

One case in particular illustrates the need for changes in federal law with regard to the unauthorized disclosure of classified information.[76] Samuel L. Morison, the grandson of the renowned naval historian Samuel E. Morison, was convicted of providing classified information to *Jane's Defence Weekly*, an English publication that publishes news on international naval developments. Morison was convicted under the Espionage Act, 18 U.S.C. § 793(d) and (e); he was the first person convicted under the Espionage Act for "leaking" information to the media. Morison was employed as an amphibious and mine warfare analyst at the Naval Intelligence Support Center at Suitland, Maryland. For some time prior to the incident in question, he had been doing off-duty work for *Jane's* with the approval of the Navy. In July 1984 he met a *Jane's* representative about possible employment and discussed a recent explosion at a Soviet naval base. Morison subsequently saw, on the desk of a fellow employee in the vaulted area where he worked, glossy photographs - marked Top Secret - of a Soviet aircraft carrier under construction. The photographs had been produced by a KH-11 reconnaissance satellite. Morison purloined the photographs, cut off the classification markings, and provided them to *Jane's*. After *Jane's* published them on its front cover, the Navy investigated the case.

During the initial investigation, Morison denied ever seeing the photographs and tried to implicate two fellow employees. The Navy seized and examined Morison's typewriter ribbon,

[76] *U.S. v. Morison*, 844 F.2d 1057 (4th Cir. 1988), *cert. denied*, 488 U.S. 908, 109 S. Ct. 259, 102 L. Ed. 2d 247 (1988). *See generally* Appendix B: Table of U.S. Leak and Representative Leak Cases.

which revealed numerous letters to *Jane's* describing the explosion. *Jane's* cooperated with the Navy's investigation, returning the original photographs. The Navy then found Morison's fingerprints on the returned photographs. After further interview, the Navy obtained a search warrant for Morison's home where additional classified documents were found. Morison was then convicted for violation of the Espionage Act as well as theft of government property. Morison argued that the espionage statutes did not apply to his conduct because he lacked the intent to commit espionage. The Court of Appeals for the Fourth Circuit rejected this argument, finding the intent to sell photographs that he knew to be classified sufficient to satisfy the scienter requirement under § 793.

The *Morison* case shows a need for stronger laws regarding the unauthorized disclosure of classified information. First, it should be noted that Morison's chain of command knew that he performed off-duty work for *Jane's*. While in itself this is not evidence of malfeasance, it provided an initial basis to question him about the recently published photographs since he also worked in the same general area that handled the photographs. Second, it should be noted that *Jane's* cooperated with the Navy's investigation by returning the purloined photographs. In this particular case, *Jane's* has had an on-going relationship with the defense community and could rightfully be concerned about protecting its reputation.

While the Navy had reason to suspect Morison's involvement even before the return of the photographs, the fingerprint evidence demonstrated that Morison had made a false statement when he denied ever previously seeing the photographs. This evidence, in turn, provided probable cause for a search of his home, which also led to further incriminating evidence. Other media organizations might not be as likely to cooperate with the government during future investigations.

Because the *Morison* case is one of the few convictions for "leaking" information, the opinion of the Court of Appeals warrants careful review. The court considered the fact that the case was not a classic espionage case even though it was brought under the Espionage Act, reviewed First Amendment case law, and examined the judge's instructions to the jury. The defense, like some scholars, argued that the Espionage Act is not an appropriate vehicle for leak prosecutions.[77] Yet, the case involved material that the defendant knew to be properly classified at the time he provided it to *Jane's*. Indeed, in the concurring opinions two of the three judges on the panel concluded that the limiting nature of the jury instructions had been important in upholding the defendant's conviction. The fact that the trial judge had to use limiting instructions to the jury likely suggested that the judge was uncomfortable with the broad brush wording of the statute itself. It is generally considered preferable for a court to interpret a statute with a narrowing construction so as to avoid a finding of facial invalidity. This use of limiting instructions to support Morison's conviction is therefore indicative that the Espionage Act may not be the most effective means of prosecuting leakers. In sum, while Morison's conviction was upheld on appeal, the case provides limited legal authority to support further prosecutions. The legitimacy of the prosecution was further questioned when President Clinton at the end of his second term pardoned Morison for his crimes.

Senator Daniel P. Moynihan (Democrat, New York), who is sometimes described as a "public interest intellectual," championed Morison's case to President William Clinton. On 29 September 1998, Senator Moynihan recommended approval of Morison's application for pardon. Senator Moynihan explained that the country had "virtually no law" concerning unauthorized disclosure and described Morison's prosecution as a selective action that was "capricious at

[77] *Morison,* 844 F.2d at 1063-1071.

best."[78] He briefly described the legislative history of the Espionage Act of 1917, explaining that President Wilson had wanted to include press censorship in the bill but the Senate had voted to strike that provision.[79] Senator Moynihan cited President Kennedy for the notion that "the ship of state leaks from the top."[80] He argued that Morison was probably convicted because of his rank - neither too high nor too low. He considered Morison's conviction to be an example of the erratic application of the law. President Clinton pardoned Morison on 20 January 2001.

Senator Moynihan makes a strong point on the issue whether Morison met the scienter requirement under 18 U.S.C. § 793 (d) and (e). Under either sub-section, the accused must have possession of information that "could be used to the injury of the United States or to the advantage of any foreign nation . . . ." Arguably, this language was crafted with the intent to criminalize acts of espionage rather than disclosures of information to the press.

Senator Moynihan's position is noteworthy because he did not recommend action against persons who leak classified information and because he considered the action against Morison to be a form of press censorship. Yet, Morison was not a member of the press and the government did not take action against *Jane's*. Clearly, Senator Moynihan construed the action against Morison to be an indirect and impermissible form of press censorship.

On a related note, Senator Moynihan chaired the *Commission on Protecting and Reducing Government Secrecy*, a bipartisan statutory commission created under the Foreign Relations Authorization Act for Fiscal Years 1994 and 1995. The commission unanimously

---

[78] Senator Daniel P. Moynihan, letter to the President, 29 September 1998, subject: Pardon of Samuel L. Morison, URL: <http://www.fas.org/sgp/news/2001/04/moynihan.html>, accessed 15 December 2006. Cited hereafter as Senator Moynihan, letter to the President.

[79] *See also* Harold Edgar, "The Espionage Statutes and Publication of Defense Information," 73 *Columbia Law R*. 5 (1973).

[80] Senator Moynihan, letter to the President.

found that secrecy is a form of government regulation, that excessive secrecy has significant consequences for the national interest when policy makers are not fully informed, that secrecy limits government accountability for its actions, and that secrecy prevents full public participation in informed debate.[81] In short, Senator Moynihan made the best case for those who advocate greater openness in government and minimal restrictions on the freedom of the press.

Randel

Another prominent leak case involves Jonathan Randel, a DEA agent, who leaked unclassified information to the press. In February 2002, the government indicted Randel for stealing sensitive unclassified information and providing it to a London newspaper. Randel was indicted on the 18 counts: he was indicted on the general theft statute, with information alleged to be the "thing of value" that was stolen; he was indicted under 18 U.S.C. § 1030, a 1994 statute designed to protect information in government computers, charging that he exceeded his authorized use of the DEA computers; and he was indicted on the mail/wire fraud statutes.[82] Randel admitted that he supplied information concerning Lord Michael Ashcroft from DEA data banks during the period February to September 1999 to a British television correspondent. The information did not jeopardize any government operations or put any person at risk; rather, the information concerned Lord Ashcroft's financial business in Belize. Randel had a fiduciary duty to protect the sensitive information and he had an obligation not to disclose it. The U.S.

[81] U.S. Senate, "Report of the Commission on Protecting and Reducing Government Secrecy," Senate Document 105-2 (Washington, D.C.: Government Printing Office, 1997), URL: <http://www.fas.org/sgp/library/moynihan/index.html>, accessed 14 December 2006. Cited hereafter as "Report of the Commission on Protecting and Reducing Government Secrecy."

[82] Randel was prosecuted under 18 U.S.C. § 641 (selling public property or records), §1031 (obtaining money through false pretenses), and §1343 (fraud by wire, radio or television).

Attorney defined the information, including electronic mail correspondence, as government property and assigned a value to it of at least $13,000.00, the amount that Randel received from the London *Times* for his expenses in connection with his trip to London. In fact, the prosecutor argued that the information had a value much greater than the $13,000.00. The prosecutor had a London literary agent testify that the information the *Times* had a market value of as much as 50,000 British pounds (about $80,000). The literary agent based his estimate on the news value of the story in the competitive London newspaper market. In the end, Randel cooperated with the government and pled guilty to a violation of the theft statute. He was sentenced to a one year prison term.

Plame

In a 14 July 2003 article syndicated columnist Robert Novak revealed the name of a CIA officer, Valerie Plame. At the time, Ms. Plame was the spouse of former ambassador James Wilson and her identity as a CIA operations officer was protected pursuant to the Intelligence Identities Protection Act (IIPA).[83] Mr. Novak's column appeared eight days after Ambassador Wilson had alleged in a *New York Times* opinion piece that the Administration had twisted pre-war intelligence on Iraq to justify going to war. I. Lewis "Scooter" Libby, then Chief of Staff to the Vice President, and Karl Rove, a former White House aide, were initially suspected of being the sources of the leak. Libby testified before the grand jury in August 2005 about a meeting with Judith Miller, a reporter for the *New York Times*, on 8 July 2005 in which they discussed Wilson, but Miller refused to testify about that meeting despite a waiver from Libby. Miller was then jailed for contempt. On 29 August 2006, Neil Lewis, a reporter with the *New York Times*,

[83] 50 U.S.C. § 421 et. seq.

revealed that Mr. Richard Armitage, a former Deputy Secretary of State, was the initial and primary source of the leak. Subsequently, on 12 June 2006, Special Counsel Patrick Fitzgerald decided against indicting Karl Rove on the charge of disclosing Ms. Plame's CIA status.

While the Plame case has involved a relatively straightforward issue regarding an application of the IIPA, the government experienced difficulty in identifying the source of the leak. Judith Miller and Matthew Cooper, both reporters, refused to identify the source of the leak, claiming First Amendment privilege. Libby had signed a blanket waiver allowing journalists to discuss their conversations, but Miller argued that the waiver to all journalists could have been coerced and that she would only testify if given an individual waiver. Libby later gave her that individual waiver. Unfortunately for them, there is no First Amendment privilege protecting source confidentiality. The judge held both Miller and Cooper in civil contempt of court for refusing to identify the source of the leak to the grand jury investigating the disclosure of Valerie Plame's identity. Both were sentenced to jail until the grand jury expired unless they testified sooner. The contempt citation was upheld by a three-judge panel of the U.S. Court of Appeals for the District of Columbia. Finally, the judge could have convened a trial on the issue of criminal contempt with a maximum possible sentence of life. . In short, it appears questionable that a reporter could refuse to identify the source of a leak in the face of a running criminal statute of limitations and the prior holding of the Supreme Court in *Branzburg*.

Franklin

Lawrence A. Franklin, a career analyst with the Defense Intelligence Agency (DIA), leaked classified information to two lobbyists from the American Israel Public Affairs

Committee (AIPAC) and an Israeli diplomat. Mr. Franklin disclosed information to Steven J. Rosen and Keith Weissman, both former AIPAC employees, concerning the Iranian threat to U.S. interests in Iraq. Allegedly, Mr. Franklin did not believe that U.S. policymakers were sufficiently alarmed over the threat and hoped to influence U.S. policy with Israeli assistance.

A search by the Federal Bureau of Investigation (FBI) of Franklin's home uncovered approximately 83 classified documents. Mr. Franklin was indicted on conspiracy to communicate national defense information to persons not entitled to receive it (18 U.S.C. § 793) and conspiracy to communicate classified information to a foreign government (18 U.S.C. § 793 and 18 U.S.C. § 371). Arguably, the government would have had difficulty with a prosecution under § 793 in that the statute also requires the possessor to have "reason to believe [that the information] could be used to the injury of the United States or to the advantage of any foreign nation. . . ." Franklin probably lacked a culpable intent; he believed that the information could re-shape U.S. policy to the advantage, rather than the detriment of the United States. Ultimately, Franklin pled guilty to the three conspiracy counts and was fined $10,000.00 and sentenced to 12 years in prison.

Both Rosen and Weissman were indicted under 18 U.S.C. § 794 for the crime of communicating information relating to the national defense to a foreign government.[84] The trial judge denied a motion to dismiss by Rosen and Weissman on the grounds that the government could prosecute and punish those who retransmitted classified information without regard to whether they had a security clearance. Both Rosen and Weissman are pending trial.[85]

---

[84] *U.S. v. Franklin,* criminal indictment, E.D.VA., Crim. No. 1:05CR225, 4 August 2005, URL: http://www.globalsecurity.org/intell/library/reports/2005/franklin_indictment_04aug2005.htm>, accessed 5 September 2006. This is a consolidated indictment against Franklin, Rosen and Weissman.

[85] David Johnston, "Pentagon Analyst Gets 12 Years for Disclosing Data," *New York Times*, online ed., 20 January 2006. URL: http://www.nytimes.com/2006/01/20/politics/20cnd-

The government's case against Rosen and Weissman is a case of first impression -- the government is applying the 1917 Espionage Act to the actions of private citizens. If Rosen and Weissman are convicted and the convictions withstand appellate review, the Espionage Act could be applied to journalists, lobbyists and academics who receive leaked classified information. Arguably, journalists, lobbyists and academics are more experienced in intelligence and foreign policy matters than the average citizen, making it easier for the government to establish that they "did unlawfully, knowingly and willfully conspire" to pass classified information to persons not entitled to receive it. In short, journalists, lobbyists and academics usually know what they want and who they can get it from, making them excellent candidates for a novel application of the Espionage Act -- it would be hard for a sophisticated consumer to argue that he didn't know what he was receiving.

Should motive matter?

The application of the Espionage Act to leak cases raises important questions about motives. The case of Samuel Morison is an anomaly under the Espionage Act: Morison provided photographs to a foreign periodical, rather than an agent of a foreign power, and that probably explains why his prison term was considerably shorter than that of any other persons convicted under these sections. Neither §§ 793 nor 794 have ever been used to prosecute someone who has received the classified information from the source, although two colorable arguments can be made under the wording of the statutes. First, § 793 applies to persons "having unauthorized possession" of national defense material, and who communicate it to others not

---

franklin.html?ex=1295413200&en=3e46a585271c0505&ei=5088&partner=rssnyt&emc=rss>, accessed 10 September 2006.

entitled to receive it. Second, a recipient could be charged with conspiracy under § 793 (g). Lawrence Franklin was indicted under § 793 (d) (e) and (g), but unlike other prosecutions under §§ 793-794, he did not disclose the classified information for private gain. Rather, he leaked the information to a lobbying group in an effort to influence U.S. government policy. The pending cases against Steven J. Rosen and Keith Weissman, both former AIPAC lobbyists, may result in a substantial extension of existing case law.

The case of Jonathan Pollard illustrates the reach of § 794(a). Mr. Pollard was a civilian analyst working for the Navy at Suitland, Maryland, when he was arrested in November 1985. Mr. Pollard had sold extensive materials to Israel and had provided information to several other countries. He ultimately pled guilty to violation of § 794 (a) for sale of information to Israel. Under § 794 (a) a person is in violation of the law if he discloses information to a foreign government and if he has "reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation . . . ." Mr. Pollard has maintained for over 20 years that he did not intend either to injure the United States or to advantage an adversary (i.e. a Communist nation). Rather, he contends that because he aided an important ally, his punishment has been excessive. He argues that he made the disclosures because senior U.S. officials were withholding critical information from Israel. Clearly, Mr. Pollard acted to advantage a foreign nation, ally or not, and was properly convicted under § 794 (a). The critical scienter problem is whether he acted with intent to advantage a foreign nation, not his intent in providing that information to Israel. Moreover, his actions did damage on-going U.S. relations with Arab countries and his motives were not as altruistic as he claims (he didn't simply disclose information to Israel; he sold it and sometimes complained to his Israeli handlers that he wasn't being paid enough).

Arguably, 18 U.S.C. § 793 (c) and (e) could be applied to journalists, lobbyists and academics who receive unauthorized information from inside sources but the motive requirement is different. The scienter requirement under § 793 (c), "knowing or having reason to believe," is appropriately higher than that in § 793 (d), the sub-section presumably applicable to inside sources such as Lawrence Franklin. The sanctions are, however, the same for both sources and recipients - a point that merits reconsideration based upon the insider's fiduciary status and likely understanding of the harm that could ensue from a disclosure of the information. Clearly, the statutory mandate that any person convicted under § 793 shall forfeit all foreign proceeds from the violation is applicable to espionage, but not leak cases.

Recently, there have been unauthorized disclosures concerning the CIA's secret overseas prisons and the NSA's warrantless surveillance program. Because these disclosures were probably made in an effort to expose illegal government activity, it is questionable whether it would be politically feasible to prosecute these leak cases under the Espionage Act. Those who leaked this information could make a colorable argument that they performed the act in the public interest. This creates problems for prosecutors planning to use the Espionage Act. If the government were to proceed with a prosecution, one of several outcomes is possible. First, media pressure could create greater scrutiny than the Administration wants, forcing the Administration to justify various programs before Congressional oversight committees. Second, Congress could take direct action either cutting funding or enacting laws to eliminate programs or practices. Third, a jury could nullify the law by acquitting culpable persons based upon a lack of agreement with the law and despite the existence of dispositive evidence of guilt. This problem is known as jury nullification. It occurs when a person is apparently guilty of violating the law, but the jury acquits the person because of a disagreement with the law itself. After the

accused has been acquitted, the Double Jeopardy Clause of the Fifth Amendment precludes re-trial.[86] Moreover, even if the government were able to prosecute successfully the leakers, one could easily envision how a future U.S. President might pardon them, just as President Clinton pardoned Samuel Morison even though his leak was clearly made for private gain and did not expose illegal government activity.

OTHER RELATED LAWS

Non-Criminal Sanctions

There are numerous non-criminal remedies that have been or could have been used to discipline persons who make unauthorized disclosures of classified information. In *Agee* the Supreme Court considered the decision of the Secretary of State to revoke the passport of Philip Agee, a U.S. citizen and former employee of the CIA who had undertaken a campaign to expose the names of and biographical information on U.S. covert agents operating abroad.[87] The Court noted that Agee had repeatedly and publicly identified persons and organizations located in foreign countries as CIA agents, employees or sources. Moreover, his actions violated his

[86] Wayne R. LaFave, and Jerold H. Israel. *Criminal Procedure* (St. Paul, MN: West Publishing Co., 1985) 830-31. One of the earliest and most famous incidents of jury nullification in the United States occurred in 1734 when John Peter Zenger, a New York printer, was tried for seditious libel. The jury acquitted Zenger despite the judge's instructions. Conceivably, if a person leaked classified information, exposing an illegal or politically embarrassing program, it is not difficult to see jury nullification as a possible trial outcome. The Historical Society of the Courts of the State of New York, "The Trial of John Peter Zenger," URL: http://www.courts.state.ny.us/history/Zenger.htm>, accessed 14 December 2006.

[87] *Haig v. Agee*, 453 U.S. 280, 101 S. Ct. 2766, 69 L. Ed. 2d 640 (1981). Cf. *Kent v. Dulles*, 357 U.S. 116, 78 S. Ct. 1113, 2 L. Ed. 2d, 1204 (1958) (the Court held that the Secretary of State could not withhold the issuance of passports from persons because of their political beliefs and associations, not involving any criminal activity); and *Zemel v. Rusk*, 381 U.S. 1, 85 S. Ct. 1271, 14 L. Ed. 2d 179 (1965) (the Court held that the Secretary of State could refuse to validate passports for Cuba based upon national security interests; the Court concluded that the refusal was an inhibition on action).

employment contract with the CIA not to make any public statements about the Agency without prior clearance by the Agency. His actions had, in turn, been followed by episodes of violence against the persons and organizations that had been identified. The Court noted that the Executive branch used the likelihood of damage to national security or foreign policy of the United States as the single most important criterion in passport decisions. The Court held that Mr. Agee's First Amendment claim lacked foundation: The revocation of his passport rested upon the content of his speech brigaded with his conduct; the revocation of his passport was an inhibition on his actions. In sum, the Court concluded that the "mere fact that Agee is also engaged in criticism of the Government does not render his conduct beyond the reach of the law."[88] The Court's decision provides three indicators for unprotected national security speech: purpose, inside information gained from fiduciary status and conduct.

In *Department of the Navy v. Egan* the Supreme Court considered the validity of an individual's entitlement to a security clearance.[89] Egan lost his job because the government denied his security clearance. The Court held that the grant of a clearance is an affirmative act of discretion on the part of the Executive branch and a person does not have a property right in a security clearance. The general standard is that a clearance is granted only when it is "clearly consistent with the interests of national security."[90] Moreover, the Merit Systems Protection Board does not have the authority to review the substance of the underlying security clearance

[88] Agee, 453 U.S. at 309.

[89] *Department of the Navy v. Egan,* 484 U.S. 518, 108 S. Ct. 818, 98 L. Ed. 2d 918 (1988). *See also Stehny v. Perry,* 101 F.3d 925 (3d Cir. 1996). In *Stehny* the court of appeals considered the imposition of a requirement to take a polygraph examination. When Stehny began work for the govermnent in 1982 she was not required to take a polygraph examination. Subsequently, the govermnent added that requirement as a condition of work on a NSA project. She was terminated when the refused to take the exam. She challenged her termination on the ground that the NSA had deprived her of a constitutionally protected interest when she was terminated for failing to comply with a new condition, but the court dismissed her claim.

[90] *Egan,* 484 U.S. at 528 (citing Executive Order 10450 §§ 2 and 3.

determination (apparently, the board can only review whether the Executive branch followed established procedures for denial of the clearance). Both the DCI and the Secretary of Defense have the authority to deny access and to initiate proceedings to revoke a person's security clearance.[91]

Officers and employees of the United States Government are also subject to sanctions if "they knowingly, willfully, or negligently: 1) disclose to unauthorized persons information properly classified under this order or predecessor orders …."[92] This language, however, conflicts with existing case law that holds that the fact of classification is sufficient to support a conviction. The sanctions that can be imposed under this order include reprimand, suspension without pay, removal, termination of classification authority, and loss or denial of access to classified information. If a person believes that information has been improperly classified, Executive Order 12958 § 1.9 provides a procedure to challenge that classification.

Under 5 U.S.C. § 8312, certain violations of the Espionage Act and the Atomic Energy Act may be subject to a forfeiture of retirement pay. This class of statutes includes 18 U.S.C. § 793 (national defense information), 18 U.S.C. § 798 (Signals Intelligence), 42 U.S.C. § 2272-76 (Atomic Energy Act) and 50 U.S.C. § 421 (IIPA).

Mary McCarthy was dismissed on 20 April 2006 from her employment with the Central Intelligence Agency. Presumably, she was dismissed under the Director's discretionary authority under 50 U.S.C. §§ 403-404(h). The Secretary of Defense has the same authority under 10 U.S.C. § 1609.

---

[91] 5 U.S.C. § 7513; 10 U.S.C. § 986; and Executive Order 12968, §§ 1.2 and 2.1.

[92] Executive Order 12958, § 5.7. (b) (1995). The head of an agency also has statutory authority to suspend without pay and subsequently remove an employee when he considers it necessary or advisable in the interests of national security. 5 U.S.C. § 7532 (1966).

Disclosures of Classified Information and FOIA

One important issue concerns the tension between the government's obligation to release information to the public under the Freedom of Information Act (FOIA) and the obligation to maintain secrecy. The FOIA provides that government agencies shall make available a broad spectrum of official information for public inspection.[93] The statute creates a statutory presumption favoring disclosure. The statute contains nine exclusive exemptions and aggrieved citizens are provided a speedy remedy in federal district court with the burden on the agency to sustain the validity of its denial of disclosure. In essence, the U.S. Congress affected a sweeping expansion of federal regarding public access to government records. There are three exemptions most directly applicable to the protection of national security information. In effect, the FOIA the Congress reaffirmed the President's authority to withhold national security information from the public discourse.

In the 1973 *Mink* case 44 Members of Congress sought release of documents prepared by an inter-departmental committee concerning the advisability of an underground nuclear test scheduled for later that year.[94] The Court reviewed the applicability of FOIA subsection (b) (1) (hereafter Exemption 1), which exempts material required by Executive Order to be kept secret, and subsection (b) (5) (hereafter Exemption 5), which exempts inter-agency materials that were used in the decision-making processes of the Executive Branch. The Court held that the test under Exemption 1 was simply whether "the President has determined by Executive Order that

[93] 5 U.S.C. § 552 (2000).

[94] *EPA v. Mink*, 410 U.S. 73, 93 S. Ct. 827, 35 L. Ed. 2d 119 (1973).

particular documents are to be kept secret."[95] The Court explained that the district courts lacked the authority to review the propriety of the classification decision. The Court also held that under Exemption 5 confidential intra-agency advisory opinions are privileged from public inspection. The Court explained that the public was entitled to such material that a private party could discover in litigation with the agency. The public was, however, limited to purely factual material that could be severed from the exempt material; the district courts could hold an ***in camera*** inspection of the material to ensure agency compliance. In 1974 the U.S. Congress acted quickly to overrule certain aspects of the *Mink* decision by providing for ***in camera*** review and the release of segregable portions of otherwise non-disclosable information. Moreover, the U.S. Congress amended Exemption 1 to provide protection for documents that "are in fact properly classified pursuant to such Executive Order."[96] Executive Order 12958 is the current authority for classifying, declassifying, and safeguarding national security information; the Executive Order also requires that information be "properly classified."[97]

In *Sims* a citizens group sought release of proposals and contracts awarded by the CIA under a research and development program that included various medical and psychological experiments to counter Soviet and Chinese advances in brainwashing and interrogation techniques.[98] The Court noted subsection (b) (3) (hereafter Exemption 3) exempted from disclosure matters specifically exempted by statute and that the CIA had, in turn, relied upon 50 U.S.C. § 403(d) (3) which obligated the DCI to protect intelligence sources and methods from unauthorized disclosure. The Court explained that the CIA was obligated to protect all sources

[95] *Mink,* 410 U.S. at 84.

[96] 5 U.S.C. § 552 (b) (1).

[97] Executive Order 12958, § 5.7 (b).

[98] *CIA v. Sims,* 471 U.S. 159, 105 S. Ct. 1881, 85 L. Ed. 2d 173 (1985).

and methods that provide or are engaged to provide the information that the agency needs to perform its statutory duties. The Court held that the DCI was within his statutory authority to withhold the names and institutions of researchers under the program. Subsequently, the U.S. Congress amended Exemption 3 to exempt matters protected from disclosure by another statute where an agency has limited, if any, discretion in the matter.

There are currently two statutes that have been held to be qualifying statutes under Exemption 3: 50 U.S.C. § 403 (d) (3), which requires the DCI to protect "intelligence sources and methods from unauthorized disclosure," and 50 U.S.C. § 431 (the CIA Information Act of 1984) which protects the nature of the agency's functions.[99] The U.S. Congress crafted the CIA Information Act to give the agency relief from the requirement to search and review its sensitive operational files, as defined in the act, in response to a FOIA request. Moreover, the act provides for a sharply curtailed judicial review of agency decision-making regarding document release.

The Secretary of Homeland Defense, like other agency heads, controls the dissemination of official documents by administrative regulation. For example, under the Homeland Security Act of 2002 and Executive Order 13311, the Secretary of Homeland Security has the authority to promulgate regulations pertaining to "sensitive but unclassified" information. This category of information includes caveats such as For Official Use Only (FOUO) or Law Enforcement Sensitive (LES). This category is used to control access to sensitive information "the release of which could harm a person's privacy or welfare, adversely impact economic or industrial institutions, or compromise programs or operations essential to the safeguarding of our national

[99] Karen A. Winchester and James W. Zirkle, "Freedom of Information and the CIA Information Act," 21 *U. Rich. L. Rev.* 231 (1987): 250-51.

interests."[100] Information so designated is not automatically exempt from disclosure under the FOIA and must be reviewed on a case-by-case basis before it can be disclosed to the public.

The *Report of the Commission on Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (hereafter *Report of the President's Commission on WMD*) noted that the imperative to share information within and beyond the IC frequently conflicted with the need to protect intelligence sources and methods. The Commission concluded that "Officials are fiduciaries who hold the information in trust for the nation. They do not have the authority to withhold or distribute it except as such authority is delegated by the President or provided by law."[101] Clearly, government officials have an obligation to share information within government and, as provided by statutes, with the public through the Freedom of Information Act. However, there are approved procedures for the declassification and release of information. A government official has a legal obligation to protect information within his control and cannot release that information except through approved procedures.

While both the FOIA and Executive Order 12958 refer to information that is "properly classified," there is scant legal authority for inappropriate classification as a defense to a leak prosecution under the Espionage Act, such as 18 USC § 793d. Indeed, the *Boyce* court concluded that the propriety of the classification was irrelevant under § 798. The *Boyce* case (1979) pre-dates Executive Order 12958 (and its predecessor Executive Order 12356, April 1982), but not the FOIA, leaving a serious issue whether the case is good authority on that point.

---

[100] Department of Homeland Security, "Safeguarding Sensitive But Unclassified Information." MD 11042.1, January 5, 2005, URL: <http://www.fas.org/sgp/othergov/dhs-sbu-rev.pdf>, accessed 22 October 2006.

[101] Lawrence H. Silberman, *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, Report to the President of the United States (Washington, DC: GPO, 2005), 430.

In sum, certain forms of national security information receive no or limited First Amendment protection. The Executive branch has legal authority to control the dissemination of information through security clearances, document classification, public disclosure and administrative sanctions. The U.S. Congress has set important priorities in terms of protection of certain information, and the sharing of information in and outside the IC. Moreover, the U.S. Congress has passed various statutes over the decades that reflect shifting national security concerns, but the statutes were designed primarily in view of the espionage problem. Unfortunately, the overall body of accumulated law has not been harmonized to meet the leak problem.

GAPS IN EXISTING LAW

There is a strong argument for a separate statutory basis for the prosecution of espionage and leak cases. On the balance, there are at least six unresolved legal issues regarding the application of §§ 793 and 794 to the unauthorized disclosure of classified information. These issues should be considered in determining appropriate changes in federal law.

First, the term "national defense" is a broad term in an era in which almost every facet of civilian life may have an important bearing on the nation's military capabilities. The legislative history and a facial reading of the statute offer no limits to an expansive definition of the term; the *Gorin* solution may have been a good result, but it was not supported by an adequate legal analysis. One issue concerns whether the term "national defense" is "sufficiently precise to withstand constitutional challenge where the actor does not behave with intention to harm the

United States or to advantage a foreign nation."[102] For example, would it have been appropriate to prosecute Lawrence Franklin under § 793 given his intention to work through AIPAC to change U.S. policy to what he perceived to be the long-term advantage of the United States? A more satisfactory result would occur if the U.S. Congress limited the terminology to information classified pursuant to law.

Second, §§ 793 and 794 could be used against both leakers and recipients of leaked information, but both sections contain troublesome problems. Sections 793 (d) and (e) each contain two separate offenses, the transmission and retention of national defense information. A careful reading of §§ 793 (d) and (e) shows an interesting disjunctive between tangible items and information. In both sections, a less than negligence standard ("could be used") modifies the information but not the tangible item aspect of the offense. Moreover, there is also a question whether the tangible items or information must originate with the government. The terminology could be equally applicable to tangible items and information that originate independent of the government.

Unfortunately, neither §§ 793 (d) or (e) contain a scienter requirement, other than that the communication or retention be willful. The word "willful" must be construed to permit an assessment of the actor's motivation in making the communication or retention. Neither sub-section requires an ulterior motive to harm the United States. Hence, both sub-sections broadly criminalize the possession of documents relating to national defense that the possessor willfully attempts to or communicates to someone "not entitled to receive it." Again, the terminology "not entitled to receive it" could be better applied through reference to persons with appropriate security clearances and an authorized need to know. Arguably, there is a Fifth Amendment self-

[102] Harold Edgar, "The Espionage Statutes and Publication of Defense Information," 73 *Columbia Law R.* 5 (1973): 976-77.

incrimination problem in the retention offenses. If a person produces the documents in his possession, can this be otherwise used against him for unauthorized possession? In short, § 793 raises serious questions about whether the flow of information between the Executive branch and the press constitutes serious criminal offenses.

Third, § 794 (b) applies only to wartime acts, but casts a broader net by including "whoever" (read: anyone), by including "publication" in the list of proscribed activities, and by including any information related to national defense, with the maximum punishment as death. This sub-section criminalizes preparatory acts. The meaning of "in time of war" is unclear; a declared war only? Section 794 (b) criminalizes publication, but apparently only when there is an intent to communicate it to the enemy. This prohibition on publication contrasts with § 793 which proscribes communication but does not mention publication. Is there an inference here that peacetime publication is not prohibited or is the word "communicates" expansive enough in § 793 to include a prohibition on peacetime publication? Unfortunately, there is no evidence in the legislative history to suggest that "communicates" does not include "publishing" within the ambit of § 793.[103] Arguably, this could have been the criminal liability that Justice White was referring to in *New York Times*.

Fourth, one must ask whether inappropriate classification is an adequate legal defense to a leak prosecution. If the leak occurred because a government employee disseminated the information, believing the information to be unclassified despite markings to the contrary, should that person be prosecuted for failure to follow approved declassification procedures? Arguably, public policy should encourage persons to follow approved procedures for declassification rather than take matters into their own hands. In fact, § 1.9, Executive Order 12958 directs that agency

[103] Edgar, "The Espionage Statutes and Publication of Defense Information," 73 *Columbia Law R.* at 1034.

heads establish procedures for classification challenge. On the other hand, public policy could also encourage insiders who know of illegal activities to make those activities public, particularly if they can show exigent circumstances for not using the prescribed classification challenge. Naturally, the leaker would be placing himself at considerable risk if he were mistaken about classification.

Next, while statutes, case law and regulations proscribe various penalties for leakers and recipients, current law provides ineffective mechanisms for identifying the sources of leaked information and bringing them to prosecution. The criminal penalties applicable to leaks should be reconsidered. If § 793 (d) is applicable to insiders who leak information and if § 793 (e) is applicable to recipients of leaked information, is it appropriate for both sub-sections to be punishable by the same penalty? Should not a more stringent penalty attach to persons who violate a fiduciary obligation?

Sixth, criminal prosecutions under the Theft Statute are open to serious question when it comes to intangible "goods." Indeed, the government's use of this statute in this way is an implicit statement to the effect that existing law provides an ineffective remedy. In short, a new statute could provide a salutary benefit, clearing up gaps and ambiguities in the law, facilitating both deterrence and effective prosecutions.

In conclusion, current law regarding the unauthorized disclosure of classified information is an accumulation of statutes, regulations and case law, most of which was enacted with the espionage problem in mind. There is some authority regarding unauthorized disclosure, such as the prior restraint of publication and the protection of intelligence identities, but the Executive branch and federal judiciary has struggled with the application of law when it comes to distinctions between prior restraint versus subsequent punishment, documents versus

information, classified versus unclassified material, and government employees versus members of the press. Moreover, certain terms of art, such as "national defense," lack clarity.

One could make a plausible argument that improper classification could be a valid defense to prosecution. The Congress can, however, enact a statute to clear up many of the ambiguities, creating a more effective deterrent and a more equitable punishment regime for the overall leak problem. This legislation should be drafted to reconcile the competing demands of national security and public debate about matters of prime political importance. This legislation should be drafted with both sources and recipients in mind, with respective obligations set forth in an equitable manner.

CHAPTER 3

RECENT LEGISLATIVE EFFORTS

There has been considerable legislative activity to remedy concerns raised in the preceding chapter. The 106th Congress passed the Shelby Amendment, an anti-leak law, as section 304 of H.R. 4392, the Intelligence Authorization Act for Fiscal Year (FY) 2001.[104] President Clinton subsequently vetoed H.R. 4392, citing the Shelby Amendment as the reason for his decision. Congress then removed the Shelby Amendment from H.R. 4392 and continued to authorize spending for the year. The 108th Congress proposed the same anti-leak language in the Classified Information Protection Act of 2001, H.R. 2943, but asked the Attorney General and other agency heads to review the adequacy of existing law and to issue a report by 1 May 2002.[105] In that report the Attorney General came to the conclusion that existing law was adequate and no changes were needed. The DCI subsequently disagreed with the Attorney General on the need for changes.[106] More recently, on 2 August 2006, Senator Kit Bond re-introduced the same language in a new bill.[107] While there seems to some level of consensus, even with public interest groups such as the Federation of American Scientists, regarding the

---

[104] The text of the Shelby Amendment is included at Appendix C.

[105] § 310, "Intelligence Authorization Act for Fiscal Year 2002," Public Law 107-108, 28 December 2001.

[106] George J. Tenet, Director Central Intelligence, Letter to U.S. Attorney General, subject: "Draft Report of the Attorney General to the U.S. Congress." 11 May 2002.

[107] Senator Kit Bond, "Bond Legislation Targets Intelligence Leaks," Press Release, URL: http://bond.senate.gov/press_section/record.cfm?id=260599, accessed 9 November 2006. *See also* U.S. Senate, *Congressional Record: August 2, 2006 (Senate),* page S8612-S8614, URL: http://www.fas.org/irp/congress/2006_cr/s3774.html, accessed 9 November 2006.

need for change to our disclosure laws, considerable disagreement exists about what should exactly be done.[108] The legislative history of the anti-leak efforts over the past five years warrants careful consideration by proponents of change for lessons learned.

THE SHELBY AMENDMENT

The stated purpose of the Shelby Amendment was to stop "leaks" by public officials of sensitive national security information to the press. The Shelby Amendment would have created 18 U.S.C. § 798A and sub-section (a) would have read:

> (a) Prohibition.--Whoever, being an officer or employee of the United States, a former or retired officer or employee of the United States, any other person with authorized access to classified information, or any other person formerly with authorized access to classified information, knowingly and willfully discloses, or attempts to disclose, any classified information acquired as a result of such person's authorized access to classified information to a person (other than an officer or employee of the United States) who is not authorized access to such classified information, knowing that the person is not authorized access to such classified information, shall be fined under this title, imprisoned not more than 3 years, or both.[109]

The amendment contained numerous qualifications, to include prohibitions against prosecution for disclosure to Article III courts (i.e. the federal district courts, the U.S. Courts of Appeals and the U.S. Supreme Court), to members of Congress, or to authorized foreign recipients. Moreover, the bill defined "classified information" as information or material "properly classified or represented, or that the person knows or has reason to believe was

---

[108] Steven Aftergood, "On Leaks of National Security Secrets: A Response to Michael Hurt," *National Security Studies Quarterly*, No. VIII (Winter 2002): 97-102.

[109] Congressional Research Service, "Protection of National Security Information: The Classified Information Protection Act of 2001," CRS Report for Congress (Washington, D.C.: Library of Congress, 16 January 2002): 2-3.

properly classified . . . ." This anti-leak law would have penalized the disclosure of any classified material without regard to whether the accused intended for the information to be delivered to and used by a foreign government. In sum, the Shelby Amendment was narrowly tailored to a limited class of leakers vice recipients, applied only to legitimate security interests, contained a scienter requirement, and imposed a limited term of imprisonment.

The Shelby Amendment initially drew bi-partisan support. The amendment was endorsed by Attorney General Janet Reno, Director of Central Intelligence George Tenet, and Director of the FBI Louis Freeh. Attorney General Janet Reno endorsed the new criminal penalties, promising that federal prosecutors would not bring charges against news reporters or those who inadvertently disclosed classified material. All the major intelligence agencies supported the Shelby Amendment. Ultimately, the measure was approved in the Senate and the House of Representatives on voice votes and without a public hearing.[110] After the measure passed, however, opposition to it mounted.

The Shelby Amendment was opposed by the *Washington Post*, the *New York Times*, *CNN* and the *Newspaper Association of America* as well as other interest groups.[111] On 24 October 2000 the heads of *Washington Post*, the *New York Times*, *CNN* and the *Newspaper Association of America* wrote a joint letter to President Clinton comparing the Shelby Amendment to Britain's Official Secrets Act and urging him to veto the bill. The media organizations contended that the provision went too far, warning that it would silence whistle-blowers and stop the media

---

[110] Associated Press, "Congress passes bill expanding penalties for classified leaks." *Associated Press,* online ed., 13 October 2000, URL: <http://www.freedomforum.org/templates/document.asp?documentID=3292>, accessed 26 October 2005.

[111] CNN, "News organizations ask Clinton to veto classified leaks bill," *CNN*, online ed., 2 November 2000. URL: <http://transcripts.cnn.com/2000/ALLPOLITICS/stories/11/02/classifiedleaks.ap/index.html>, accessed 18 December 2006.

from getting important information to the public. They feared the new law would be used to investigate journalists and editors, forcing them to reveal confidential sources and abridging the First Amendment. The media organizations maintained that government leaks had resulted in numerous important stories reaching the American public, such the Pentagon Papers, the Iran-Contra affair, and cases of waste, fraud and abuse in the defense industry.

Some Members of Congress expressed concern that Members of Congress, as well as staff members, could face felony charges for revealing classified information.[112] Representative Henry Hyde (Republican, Illinois), then Chairman of the House Judiciary Committee, also complained that the restrictions had been approved without public hearing.

Kate Martin, General Counsel of the National Security Archive, opposed the bill as an unconstitutional abridgement of First Amendment rights.[113] She contended that a proposal to criminalize possession all "properly classified" information is constitutionally overbroad. She argued that sanctions already exist for leakers, to include the loss of a security clearance and government employment. She noted that Congress has only previously protected narrow categories of information, namely intelligence identities, where there was a likelihood of immediate and substantial harm and the information was only marginally relevant to public policy debate. On the other hand, she maintained that much classified information is germane to public policy debate. Finally, she argued that media exposure is an important aspect of keeping

[112] Members of Congress have a limited immunity from criminal liability under Article I, § 6 (the Speech and Debate Clause): "for any Speech or Debate in either House, [members of Congress] shall not be questioned in any other Place." *U.S. Constitution*. While there is scant legal authority clarifying the reach of the Speech and Debate Clause, the Shelby Amendment could have conceivably exposed members of Congress to criminal liability if they disclosed classified information outside Congress (i.e. during a press conference held at the Member's District Office).

[113] Kate Martin, "The Pending "Leak" Statute is Unconstitutional," Federation of American Scientists, URL: <http://www.fas.org/sgp/news/2000/09/leaks.html>, accessed 15 December 2006.

national security agencies accountable. In short, she saw the bill as an abridgement of the public's right to know and of the freedom of the press.

Steven Aftergood, director of the Federation of American Scientists' government secrecy project, lobbied strenuously against the anti-leak provision. Mr. Aftergood noted that reporters are often the best or only "witnesses" to the crime. He observed that reporters are not passive recipients of information, but rather actively elicit information from government officials. He pointed out that under Senator Shelby's proposal that reporters could be charged as an "accessory before the fact."[114]

Mr. Aftergood contended that the Shelby Amendment would have created a separation of powers problem in that it would have endowed the Executive branch with the authority to define the crime and then punish it as the Executive branch saw fit. He was concerned that the classification system was governed by Executive Order not by statute, giving the Executive branch the power to classify, declassify and reclassify national security information at its discretion. Aftergood was concerned that the Shelby Amendment would have provided the Executive branch the power to create or dissolve the conditions for a felony prosecution. He argued that this was an abdication of Congress' obligation to "make all laws."

In response to this wave of lobbying, President Clinton vetoed H.R. 4392 on 4 November 2000 "because of one badly flawed provision that would have made a felony of unauthorized disclosures of classified information. Although well-intentioned, that provision is overbroad and may unnecessarily chill legitimate activities that are at the heart of a democracy."[115] President

---

[114] Steven Aftergood, "On Leaks of National Security Secrets: A Response to Michael Hurt," *National Security Studies Quarterly*, No. VIII (Winter 2002): 99.

[115] William J. Clinton, "Statement by the President to the House of Representatives," 4 November 2000, URL: <http://64.233.161.104/search?q=cache:n_stZ_BT6U0J:www.fas.org/irp/news/2000/11/irp-001104-

Clinton observed that the provision had been passed without the benefit of public hearings and maintained that the provision had been thoroughly deliberated by his Administration, which in turn led to a failure to apprise the Congress of his concerns. Mr. Aftergood explained that the "idea that the president had to tell Congress that it had to hold hearings was a well-deserved insult to the intelligence committees."[116] Senator Shelby complained that the amendment had been approved by the Administration before final passage by Congress and noted that the President's veto was timed several days before a very tight election.

ACTION IN THE 107TH CONGRESS

The leak issue was briefly reconsidered in the next (107th) Congress. Just prior to a closed hearing of the Senate Select Committee on Intelligence (SSCI) planned for 5 September 2001, Attorney General John Ashcroft asked the SSCI to defer action until the Bush Administration could conduct its own interagency review of the problem. The SSCI agreed and included a provision in the FY02 Intelligence Bill directing the Attorney General to conduct a comprehensive review of current protections against the unauthorized disclosure of classified information. In response to this Congressional directive, the Attorney General formed an interagency task force to carry out a comprehensive review of current protections against the unauthorized disclosure of classified information. The task force was chaired by an Associate Deputy Attorney General and the members were an attorney from the Department of State, an

---

leak.htm+clinton,+%22statement+by+the+president+to+the+house%22&hl=en&gl=us&ct=clnk&cd=1>, accessed 22 August 2006.

[116] Vernon Loeb, "Anti-Leak Veto Catches Sponsors Off Guard," *Washington Post*, 13 November 2000, URL: <http://www.fas.org/irp/news/2000/11/irp-001113-leak.htm>, accessed 11 November 2006.

attorney from Department of Defense, the Director of Security for the Department of Energy, the Acting General Counsel of the CIA, and the Deputy White House Counsel.

The task force was to consider any legal mechanisms to detect the unauthorized disclosure of information and any legal sanctions to deter and punish the unauthorized disclosure of information. The panel also considered whether the administrative regulations and practice of the Intelligence Community were adequate and whether recent developments in technology could further protect against the unauthorized disclosure of information. The review was limited in scope to the unauthorized disclosure of information to the media. The task force formed five working groups: litigation, legislative, security, science and technology, and legal review. Task force members recruited persons from their own organizations to serve on the working groups.

The task force issued a draft report dated 29 April 2002.[117] The task force reported that 320 leak cases had been reported to the Department of Justice by the Intelligence Community in the preceding five years and that no area of classified information had been immune to the epidemic. The panel reviewed the 1982 Willard Report that had concluded that "statutes criminalizing unauthorized leaks are unclear and resulted in highly unsuccessful prosecution efforts." The group found that no less than six versions of a criminal statute had been considered between 1982 and 2002, with the Shelby Amendment as coming closest to being enacted into law. The task force pointed out that the Shelby Amendment had the support of the Department of Justice, the FBI, CIA and the Office of Management and Budget, but had received considerable opposition from interest groups and media affairs organizations.

The task force then reviewed numerous criminal statutes, Executive Orders and regulations. It correctly observed that no single statute criminalized the unauthorized disclosure

[117] John Ashcroft, U.S. Attorney General, "Report to Congress on Unauthorized Disclosures of Classified Information," Draft Report, 29 April 2002 (9:49 AM). Cited hereafter as Ashcroft, Draft Report.

of classified information, but rather a patchwork of laws covered most unauthorized disclosures. The task force recognized several gaps in the legal framework: a gap with respect to unauthorized recipients who are not foreign agents whenever a scienter requirement is involved; a gap with respect to classified information concerning international relations not relating to the national defense; and a gap with respect to non-military sources and methods. The task force found that the current prohibitions are "not as comprehensive and clear and they could be." Nonetheless, the task force argued that the patchwork of laws as not the causative factor of the leak problem.[118] The task force did, however, conclude: "What has been articulated many times, and corroborated by the work of the task force, is that the primary factor for the lack of prosecutions of leaks is the singular inability of the government, heretofore, to positively identify the perpetrator with proof sufficient to sustain a conviction."[119]

The task force made some important findings:

- The criminal law is a patchwork and there is no single statute that provides coverage for all types of leaks. There is a legal, but not a practical gap in this patchwork.
- No new criminal legislation with respect to leaks. Existing law provides adequate protection against the unauthorized disclosure of information.
- Agency heads have substantial administrative authority to address the leak problem, but the when a leaker has been identified the sanctions applied have typically been inconsequential or inconsistently applied.
- There is a lack of uniformity throughout the Intelligence Community with respect to administrative regulations, policies and procedures, particularly where it involves security programs and leak investigations.
- A comprehensive, coordinated government-wide information security program. This effort should include training and education with an emphasis on personal accountability and "need to know."
- Agencies should conduct immediate and aggressive investigations, reporting crimes to the Department of Justice.
- The Department of Justice should pursue civil enforcement actions against leakers.
- The non-disclosure agreements signed by government employees should be amended to include a provision for liquidated damages.

[118] Ashcroft, Draft Report, 29.

[119] Ashcroft, Draft Report, 29.

On 11 May 2002, the DCI responded to the Attorney General's draft report to Congress based upon the recent work of the inter-agency task force. Mr. Tenet agreed there was a need to enhance administrative actions to deter and investigate leaks. He contended, however, that the Intelligence Community needed a more aggressive approach than the draft report recommended to address meaningfully the hemorrhage of information to the media. He argued that effective action against leaks requires the full engagement of the Department of Justice and the FBI, noting that the draft report assigned no actions to the Department of Justice to address this problem. The DCI maintained that as a result of laws not designed for the leak problem, weak enforcement of existing law and insufficient investigative authority that the government had been effectively unable to deter, identify, and punish leakers of classified information.

On 15 July 2002, Attorney General Ashcroft responded to the DCI's letter of 11 May 2002. The Attorney General noted that the Department of Justice had a paramount mission to protect the United States from terrorism and that this mission had placed an enormous burden on the Department and the FBI. He explained that he had recommended to the Congress that the Department and FBI play a supporting and consulting role in what he hoped would be a much more aggressive and collective administrative approach to leak investigations. He contended that the current statutory framework provides the government with adequate authority to investigate and prosecute leaks. He noted:

> The very real problem in the criminal realm, however, is the difficulty, in most cases, of establishing beyond a reasonable doubt who the perpetrator actually is. Without forensic evidence linking a defendant conclusively to a particular piece of information, or the positive identification of the defendant by the recipient of the information, such proof is extraordinarily difficult to obtain.[120]

[120] John Ashcroft, U.S. Attorney General, letter to the Director Central Intelligence, subject: "Reply to Letter, 11 May 2002," 15 July 2002.

He pledged the support of the Department of Justice, but he concluded that the vital need involved rigorous investigation of unauthorized disclosures but not the enactment of new laws.

On 15 October 2002, the Attorney General submitted his final report to the Congress. He reported that he had formed an inter-agency task force and reviewed the findings and assessment of that task force. He opined that "current statutes provide a legal basis to prosecute those who engage in unauthorized disclosures, if they can be identified."[121] He questioned whether additional legislation would enhance investigative efforts. The Attorney General concluded that a "comprehensive, coordinated, government-wide, aggressive, properly resourced, and sustained effort to address administratively the problem of unauthorized disclosures is a necessity." He recommended that the Executive Branch activate a wide range of administrative measures to improve the capacity to stem the practice of leaks, that all departments and agencies that originate or handle classified information use all means at their disposal to identify and impose sanctions upon leakers, and that the government improve enforcement of existing laws. Unfortunately, there has been no change in either federal law or the government's anti-leak policy since the Attorney General submitted his report to Congress.

On 2 August 2006, Senator Kit Bond re-introduced the anti-leak language previously submitted by Senator Shelby. Senator Bond proposed the bill to unify existing law and to ease the government's burden in prosecuting and punishing leaks. Senator Bond believes that current law should be amended to eliminate the need to prove that damage to the national security has or will result from an unauthorized disclosure. The bill still sits on the calendar and is not likely to be called up on its own. If the bill is re-introduced, however, one option is for it to be handled as

[121] John Ashcroft, U.S. Attorney General, "Report to Congress on Unauthorized Disclosures of Classified Information," 15 October 2002, URL: <http://www.fas.org/sgp/othergov/dojleaks.html>, accessed 26 October 2005.

a separate stand-alone bill with open, public hearings. The House and Senate Judiciary Committees could assert shared jurisdiction. As a stand-alone bill, the anti-leak provision could be reviewed by the Intelligence and Judiciary Committees without forcing the Intelligence Committees to refer the entire Intelligence Authorization Act to the Judiciary Committees for review.

THE SEPARATION OF POWERS ISSUE

Mr. Aftergood's concern about an unconstitutional separation of powers is misplaced. The Constitution does not contain an explicit separation of powers doctrine, rather the theory is judicially derived from a reading of the first three Articles. The Congress does have broad authority to delegate matters to the Executive branch so long as it lays down an intelligible principle to guide rule-making authority.

In *Touby v. United States* the Supreme Court considered the application of the non-delegation doctrine to the Controlled Substances Act, a statute that permitted the Attorney General, after following prescribed procedures, to add new drugs to existing schedules of regulated or controlled drugs.[122] The Court explained that the judicially-derived non-delegation doctrine is based upon the premise that the Congress may not delegate its legislative power to another branch of government. The Court noted that the Congress had authorized the Executive branch to promulgate regulations that contemplated criminal sanctions, but concluded that the statute provided a meaningful constraint on the Attorney General's discretion to define the criminal act. The Court held that so long as Congress lays "down by legislative act an

[122] *Touby v. United States*, 500 U.S. 160, 111 S. Ct. 1752, 114 L. Ed. 219 (1990).

intelligible principle to which the person or body authorized to [act] is directed to conform, such legislative action is not a forbidden delegation of legislative power."[123]

Here, the courts would likely find the Shelby Amendment to be a permissible delegation of power by Congress to the Executive branch. First, unlike the *Touby* case, the Shelby Amendment involves the classification of documents relating to national security and foreign affairs, areas that are firmly within the President's expertise under Article II, § 2. The federal judiciary has long recognized a substantial deference to the President on these issues.[124] Second, the Executive branch classified documents relating to national security even before the Congress passed the National Security Act of 1947. Third, the Congress understood and accepted this practice when it directed the Director of Central Intelligence to protect intelligence sources and methods in that act. Moreover, Congress has repeatedly recognized the President's authority to classify and declassify document in various contexts (i.e. the exemptions from disclosure under Freedom of Information Act). Fourth, the President has issued detailed Executive orders, with the full force of law, that establish policy procedures for the classification and declassification of information and documents that originate through Executive departments and activities. In fact, the Executive orders provide detailed procedures that limit the discretion of Executive officials. For example, under current Executive orders information must be "properly classified," a point that clearly excludes the classification of information to hide wrong-doing or prevent political embarrassment.

[123] *Touby*, 500 U.S. at 165.

[124] *Youngstown Sheet & Tube Co. v. Sawyer,* 343 U.S. 579, 72 S. Ct. 863, 96 L. Ed. 1153 (1952).

PUBLIC POLICY CONCERNS

While a free press performs an essential role in democracy, there must be practical limits when it comes to the receipt and use of information properly classified by the government. The need for an informed citizenry cannot be overstated but the Supreme Court has yet to rule that the public has a "right to know" that places a duty upon the government to disclose classified information.[125] Citizens must have access to relevant and significant information about government activities in order to vote intelligently or to register opinions on the administration of government. In fact, a free press plays a key role in this process. Moreover, there are countless instances in which the press has exposed wrongdoing on the part of government officials. The question, however, is where to draw the line between a free press that supports the citizenry and the elicitation of a crime to scoop a story? The press cannot have *carte blanche* when it comes to withholding information related to criminal activity. Public policy should not condone either the solicitation or facilitation of crime by members of the press. Moreover, when a member of the press receives classified material it should be treated for what it is - the receipt of stolen property. Finally, members of the press should be forced to disclose criminal accomplices - the culpable parties who breached their fiduciary obligation by dint of unauthorized disclosure.

Lastly, while it is laudable that the media should seek information about the government performance, there is no legal basis for the media's claimed role as a watchdog over the Intelligence Community. The media does not have a right under constitutional, statutory, or decisional law to either possess or retain classified information or documents. The Director of National Intelligence is obligated by law to protect intelligence sources and methods; in

[125] "Plugging the Leak: The Case for a Legislative Resolution of the Conflict Between the Demands of Secrecy and the Need for an Open Government," Note, 71 *Virginia Law Review* 5 (June 1985): 829-34.

Branzburg, however, the Supreme Court made clear that media sources and methods are not privileged. Indeed, the weight of authority is that media sources are discoverable by the government. Under Article I, U.S. Constitution, the Congress has the power to provide for the common defense and general welfare of the United States, to appropriate moneys and require accountings, and, in the case of the Senate, advise and consent to the appointment of certain Executive branch officials. Finally, in event that an official is derelict in his duties, the Congress has the power to discipline its own members and impeach selected officials. In short, Congress has a constitutional obligation to serve as a watchdog on Intelligence Community performance. Moreover, the Congress performs oversight through an established committee structure, with processes and procedures for safeguarding classified information and documents. Finally, unlike the journalists who are accountable to employers and consumers, members of Congress are accountable to the American people through the ballot box.

CHAPTER 4

THE BRITISH EXPERIENCE

The British approach to espionage and disclosure law provides a useful analogy in analyzing the strengths and weaknesses of existing U.S. law. British and American law share the same common law background: The criminal laws in the United Kingdom and the United States use many of the same concepts of *actus reus* (i.e. the wrongful deed in a crime), *mens rea* (i.e. the guilty or wrongful purpose in a crime), trial by jury, legal defenses, right to the assistance of counsel, burdens of proof, presumption of innocence, and right against self-incrimination. Moreover, British citizens have many of the same concerns as do Americans about excessive secrecy in government and the use of secrecy laws to avoid public disclosure of embarrassing facts about elected officials. Both nations have educated publics, a similar culture and language, and a press which is not adverse to seeking information about or criticizing the government. Finally, both nations have worldwide intelligence organizations and a resulting need to protect information from either espionage or unauthorized disclosure. In the United Kingdom the Official Secrets Act of 1989 is the current law on espionage and the unauthorized disclosure of classified information.[126] Parliament originally enacted this law in 1889 and subsequently amended it on several occasions in response to notable problems. Although it has existed for over a century, the British Official Secrets Act is not well understood in the United States.

[126] The full text of the 1989 British Official Secrets Act is included at Appendix D with a sununary table at Appendix E.

Efforts to reform U.S. law are typically vilified by media interest groups as an attempt to create an official secrets act in the United States.

ORIGINS OF THE OFFICIAL SECRETS ACT

In the late nineteenth century, the United Kingdom experienced a series of espionage acts and unauthorized disclosures. Parliament responded in 1889 by passing the in first Official Secrets Act with little debate or opposition. The 1889 Act applied only to Crown servants and contained provisions for both espionage and leakage, but was soon found to be cumbersome and lacking adequate powers of enforcement. For example, the 1889 Act made it unlawful for any person holding office to make an unauthorized disclosure of any material or information "to any person to whom the same ought not, in the interest of the state, or otherwise in the public interest, to be communicated at that time . . . ."[127] This language created a controversial argument in British law that allowed a person to argue that his disclosure, while unauthorized, was actually in the public interest. In 1911 the British Parliament repealed the 1889 Act and passed a new act that made several important changes.

Parliament passed the 1911 Act in response to the growing threat of international espionage to the United Kingdom and the perceived weaknesses in the 1889 Act. The new § 2 provided that:

> If any person having in his possession or control any sketch, plan . . . information which relates to or is used in a prohibited place or anything in such a place or which has been made or obtained in contravention of this Act, or which has been entrusted in confidence to him by an person holding office under His Majesty or which he has

[127] Oonagh Gay, *Official Secrecy*, online monograph, (London: House of Commons Library, 2004), URL: <http://www.parliament.uk/commons/lib/research/notes/snpc-02023.pdf>, accessed 11 January 2006. Cited hereafter as Gay, *Official Secrecy* Monograph.

> obtained owing to his position as a person who holds or has held office under HM, or as a person who holds or has held a contract made on behalf of his Majesty, or as a person who is or has been employed under a person who holds or has held such an office or contract
> (a) communicates the sketch, plan, model, article, note, document or information to any person, other than a person to whom he is authorised to communicate it, or a person to whom it is in the interest of the State his duty to communicate it, or
> (b) retains the sketch, plan model, article, note or document in his possession or control when he has no right to retain it or when it is contrary to his duty to retain it; that person shall be guilty of a misdemeanor.[128]

The 1911 Act broadened coverage from Crown servants to include the press and others who receive the material or information from Crown servants, and to include information without reference to classification, and eliminated the public interest defense. In fact, § 2 of the 1911 Act became known as the "catch-all" provision. Most important, Parliament created a strict liability offense by eliminating any question of scienter. In other words, a defendant could be found guilty even if he did not intend to release the information.

THE MODERN OFFICIAL SECRETS ACT

Parliament passed the current Official Secrets Act in 1989 partially in response to a former government official's high-profile publication of his memoirs, *Spycatcher,* and partially in response to several other high-profile cases that highlighted weaknesses in British law. Peter Wright was a former Assistant Director of British Security Service (MI5). He authored a book about his memoirs that made unauthorized disclosures of official information, to include an accusation that Sir Roger Hollis, a former Director-General of MI5, had been a Soviet agent. Mr. Wright had, however, moved to Australia and was using an Australian publisher, leaving him beyond the reach of British criminal law. The British government, therefore, initiated civil

[128] Gay, *Official Secrecy* Monograph, pp. 3-4.

proceedings in Australian court against Mr. Wright and his publisher, seeking to restrain publication of the memoirs on the basis of a breach of confidence. In effect, the British government argued that Mr. Wright owed a life-long duty of confidentiality to the British government. Moreover, the British government argued that his Australian publisher had induced Mr. Wright to breach that contractual obligation. The Australian court ruled, however, that MI5 had not been established by statute and that absent a statutory basis his employment could not be regarded as contractual. The Australian court also ruled in favor of Mr. Wright, holding that it lacked jurisdiction to enforce an obligation of confidence owed to a foreign government.

In the meantime, the British government initiated civil proceedings in British courts against several national newspapers seeking injunctive relief against local publication of Mr. Wright's material. The government obtained an interim restraining order, but three newspapers proceeded to publish material while the interim restraining order was in effect. The U.K. Attorney General initiated contempt proceedings against the three newspapers and their editors. While the civil and criminal actions were still pending, Mr. Wright published his memoirs in the United States.[129] The British High Court then ruled that the world-wide dissemination of the information removed from third parties any duty of confidence. The Court denied the request for injunctive relief and ruled that contempt proceedings were no longer applicable.

Parliament corrected the situation by passing the Security Service Act of 1989, placing MI5 on a statutory basis, and the Official Secrets Act of 1989. The British Official Secrets Act of 1989 (hereinafter BOSA 1989) made no alterations to § 1 of the 1911 Act, relating to espionage, but instead revised § 2, relating to the unauthorized disclosure of government information. The BOSA 1989 identifies six specific areas of information protected by criminal

[129] Peter Wright, *Spycatcher* (New York: Viking Penguin, 1987).

law: security and intelligence, defence, international relations, crime and investigation powers, information resulting from unauthorized disclosures or entrusted in confidence (i.e. leaks), and information entrusted in confidence to other States or international organizations (see Appendices D and E). The BOSA 1989 embodies, *inter alia*, provisions to protect the life-long confidentiality of information acquired by British intelligence officers in the course of their work. The BOSA 1989 codifies the government position that government information is government property held on behalf of the Crown. It is also important to note that the United Kingdom lacks either a Freedom of Information Act or an Intelligence Identities Protection Act. In short, the BOSA 1989 is the center-piece of British law on point.

THE STRUCTURE OF THE OFFICIAL SECRETS ACT

Structurally, the BOSA 1989 has created a two-part law that separates espionage from unauthorized disclosures. This means that if the British government lacks sufficient evidence to convict a person of espionage that it can fall back on the lesser-included offense of unauthorized disclosure. Moreover, the range of punishment under the lesser-included offense is appropriately lessened as well. Next, the section on unauthorized disclosures has three strict liability sub-sections that applies only to present and former security and intelligence officers who reveal information, documents or material relating to security or intelligence; to Crown servants or contractors who disclose information, documents or material that facilitates a crime; and to Crown servants or contractors who disclose information obtained pursuant to warrant issued under either the Interception of Communications Act or the Security Service Act. The remaining sub-sections contain important elements that the government must prove as part of its prima facie

case, to include the fact that the disclosure was damaging. If the sub-section requires that the government show that the disclosure was damaging, the accused is entitled to defend himself by showing that he "did not know, and no reasonable cause to believe" that the disclosure would be damaging. In effect, scienter is not absent from the statute, it merely operates differently from most criminal laws in the United States.

Under sub-section 1, a present or past member of the security and intelligence services, to include any person notified that he is subject to this sub-section, is guilty of an offense if he discloses without authority "any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of those services or in the course of his work while the notification is or was in force." Sub-section 1 then goes on to criminalize unauthorized disclosures relating to security and intelligence made by other Crown servants or contractors, but requires the government to prove that the disclosure was damaging and allows the accused the defense that he "did not know, and no reasonable cause to believe" that the disclosure would be damaging within the stated meaning. This means that the defendant has the burden of proving a lack of scienter. In effect, sub-section 1 imposes a life-long silence on members of the security and intelligence services, effectively dealing with the *Spycatcher* problem, but without the procedural and substantive due process protections extended to U.S. officials by the *Marchetti* and *Snepp* cases.

Under sub-section 2, a present or past Crown servant or government contractor "is guilty of an offense if without lawful authority he makes a damaging disclosure of any information, document or other article relating to defense which is or has been in his possession by virtue of his position as such." Sub-section 2 then defines damaging disclosures and provides for a defense if the person "did not know, and no reasonable cause to believe" that the disclosure

would be damaging within the stated meaning. Again, the burden of proving a lack of scienter is shifted to the defendant.

Under sub-section 5, a person is guilty of an offense if he comes into possession of any information, document or article in violation of this Act and "he discloses it without lawful authority knowing, or having reasonable cause to believe, that it is protected against disclosure" by this Act. Moreover, the government must prove that the disclosure was damaging. This sub-section clearly applies to person outside of government who are in unauthorized receipt of government information. Unlike Crown servants and contractors, the recipient of leaked information (i.e. journalists, lobbyists or academics) might have an easier time proving a lack of scienter in that they might not be aware of the contextual nuances of the leaked information.

IMPORTANT PROVISIONS OF THE OFFICIAL SECRETS ACT

There are several critical ancillary provisions to the BOSA 1989. Sub-section 8 deals with the obligation on the part of the Crown servant or contractor to safeguard government information and the unlawful retention of government documents or articles. Sub-section 9 deals with the role of the Attorney General in initiating criminal proceedings. Sub-section 10 deals with the negligent failure to safeguard or failure to return material upon demand.

First, under sub-section 8, Crown servants and government contractors are obligated to safeguard government information that would be an offense to disclose without lawful authority. The Crown servant is guilty of an offense if he unlawfully retains a document or article. The government contractor is guilty of an offense if he "fails to comply with an official direction for the return or disposal of the document or article." Both provisions are analogous to 18 U.S.C. §§

793 (d) and (f), although U.S. law imposes a scienter requirement in that the accused must act willfully. In view of the scienter requirement in U.S. law, U.S. courts can impose a more substantial punishment than can the British courts in a similar situation (10 years vice three months). Next, sub-section 8 contains provisions that apply to persons who are unauthorized recipients of government documents or article. A recipient commits an offense if he fails to comply with an official direction for the return of the document or article, which is analogous to 18 U.S.C. § 793 (e).

Second, under sub-section 9, no prosecution can be instituted in the United Kingdom under the BOSA 1989 without the consent of the Attorney General. British courts have held that the Attorney General's consent is absolute and he is accountable only to Parliament for his decision. This provision allows the Attorney General to consider the weight of the evidence, the degree of culpability on the part of the accused, the damage to public interest from the disclosure and the effect of the prosecution on public interest. While British law permits closed trials provided that the sentence is read in open court, the Attorney General could determine that prosecution could result in additional damage to the public interest and would, therefore, be inappropriate in a given case. Finally, the Attorney General's discretion is important because, unlike U.S. law, Crown prosecutors lack statutory authority to grant immunity to less culpable co-conspirators.

Third, under sub-section 10, persons convicted under other than sub-section 8 (negligent failure to safeguard or failure to return material upon demand) are subject to imprisonment not exceeding two years or a fine or both. If a person is convicted for negligent failure to safeguard or failure to return material upon demand, the person is subject to imprisonment not exceeding

three months or a fine or both. Second, under sub-section 15, the BOSA 1989 extends to acts done by British citizens or Crown servants while abroad.

BRITISH AND U.S. LAW COMPARED

The BOSA Act operates differently from U.S. law. First, in British political culture, the authority of government officials proceeds from the Crown, not from the electorate. The BOSA Act is based upon an underlying presumption that criminalizes the release any information without authority. The BOSA 1989 extends the protection of criminal law to all government information without regard to a classification schedule. Unlike the United Kingdom, the United States has a written constitution with a First Amendment that embodies certain expressive freedoms as a basis for federal and state laws. Indeed, under the U.S. Freedom of Information Act, all government information is presumptively releasable unless it falls within one of nine exclusive exemptions. Moreover, the U.S. Congress and the federal courts have repeatedly clarified and reaffirmed the government's obligation to release information to the public. Second, the BOSA contains strict liability provisions, but only involves government officials dealing with three limited categories of information. Third, where proof of damage is required, a person charged under sub-section has a defense of a lack of scienter. In effect, the BOSA Act has shifted an important burden to the defendant. It places the accused in a difficult, but not untenable, position of proving a negative.

The BOSA 1989 is a workable, effective law. It defines six categories of protected information; it removed the disclosure of much official information from the scope of prior criminal law. In a circumscribed class of cases, there are strict liability offenses, but in other

cases the government must prove the unauthorized disclosure was damaging and the accused can defend himself by showing that "he did not know, and had no reasonable cause to know" that the disclosure would be damaging. The BOSA 1989 makes important distinctions between persons who leak information in violation of a fiduciary obligation and those who receive that information (i.e. the press, lobbyists and academics). While the BOSA 1989 did not create a statutory presumption of disclosure, as in the U.S. Freedom of Information Act, it is not a blunderbuss of a law as it is sometimes vilified in the American press. Moreover, the BOSA 1989 is a substantial improvement on the BOSA of 1911. In sum, if Samuel Morison had been a British subject working for the Ministry of Defence when he made his disclosure to *Jane's*, he probably would have been convicted and received the same punishment that he did under U.S. law. On the other hand, if Lawrence Franklin had been a British subject working for the Ministry of Defence when he made his disclosures to AIPAC, he probably would have been convicted but would have received a substantially shorter prison sentence (two years vice the 12 year sentence he did receive). In short, this could a better politically acceptable result in the United States, particularly if the government eliminates problems with prosecutions under current law, gaining a greater deterrent effect with more prosecutions.

CHAPTER 5

A PROPOSED STATUTE

While the BOSA 1989 contains many interesting and innovative provisions, the United States does not require a similar single official secrets statute. U.S. law already contains many useful statutes that address many of the nuanced problems that have developed over the last century. The United States could, however, benefit from the two-part structure in British law that distinguishes between espionage and leak offenses. There are several advantages that would accrue to U.S. prosecutors with a two-part system. First, prosecutors would be able to distinguish between espionage and leak cases in terms of the nature of the offense and appropriate punishment. Second, prosecutors would be able to distinguish between sources and recipients of classified material or information, again in terms of the nature of the offense and appropriate punishment. Third, prosecutors would be able to strike a head-on blow at the journalistic shield based on privilege. The U.S. Congress should enact a leak law.

PROPOSED STATUTORY LANGUAGE

Unauthorized Disclosure of Classified Information

a) Whoever, having lawful possession of, access to, control over, or being entrusted with classified information or documents, communicates, transmits or discloses such damaging information to any individual not having authorized possession of such information or documents, shall be fined under this title or imprisoned not more than three years, or both;

b) In sentencing proceedings pursuant to this section, the court shall consider whether such disclosure was inadvertent or intentional;

c) In proceedings pursuant to this section, the Defendant shall have the burden, as an affirmative defense, of proving that the information or documents marked as classified were unclassified, irrespective of whether the information documents were classified by proper authority;

d) Whoever, having knowingly received classified documents by unauthorized disclosure, shall be considered in receipt of stolen property and shall be fined under this title or imprisoned not more than three years, or both. The defense of privilege shall not apply in any proceedings brought under this subsection;

e) Classified information refers to oral, non-documentary information that is clearly marked or represented to be properly classified pursuant to either a statute or Executive Order. This definition extends to information known by the defendant to be classified, but inadvertently not so marked. This definition extends to information that has not yet been classified pursuant to law, but which a reasonably prudent person would expect would be classified in the due course of business;

f) Classified documents refers to written, photographic, imagery or signals intelligence products that are clearly marked or represented to be properly classified pursuant to either a statute or Executive Order;

g) For the purposes this section, a disclosure is damaging if:

i) it causes damage to the work of, or of any part of, the defense and intelligence services; or

ii) it is of information or a document or other article which is such that its unauthorized disclosure would be likely to cause such damage or which falls within a class or description of information, documents or articles the unauthorized disclosure of which would be likely to have that effect; and

h) It shall not be an offense to report the improper classification of information or documents to a Member of Congress, an Executive department Inspector General, or other designated official under the federal *Whistleblower Protection Act*.

ANALYSIS OF PROPOSAL

In *Morison* the Court of Appeals was concerned about the language in the statute that involved the disclosure of documents "relating to the national defense" and whether the language was overbroad under First Amendment case law. The Court of Appeals concluded that the judge's instructions to the jury that clarified the language as relating to information "potentially damaging to the United States or might be useful to the enemy" was appropriate and precluded a

finding that the statute was unconstitutional.[130] The above-proposed statute eliminates the potentially overbroad language, focusing solely on the unauthorized disclosure of classified information or documents. Moreover, the proposed statute eliminates the intent element (the *mens rea*) of the crime, applying a strict liability standard. While it could be argued that a strict liability standard is inappropriate for a felony offense, the point is that persons who have been entrusted with classified information must maintain a high standard of personal accountability. A breached trust can have serious consequences for national security. Finally, the proposed statute avoids the contention of many government lawyers and scholars that the existing statutes were intended to address classic espionage cases, not leaks.

STRICT LIABILITY IS APPROPRIATE

The U.S. Congress has the constitutional power to create a strict liability offense in federal criminal law provided that it manifests the legislative intent to do so. In *U.S. v. Balint* the Supreme Court reviewed the common law rule that scienter is a necessary element in every criminal law.[131] In *Balint* the defendants had been indicted for selling opium and cocaine; the defendants demurred to the indictment, contending that it failed to charge that they had sold the drugs knowing them to be such. In fact, the statute did not require such knowledge as an element of the offense. The Court held that it was an issue of legislative intent, that the Congress could enact a strict liability offense in order to stimulate the proper level of care by punishing negligent persons.

---

[130] *U.S. v. Morison*, 844 F.2d at 1086.

[131] *U.S. v. Balint*, 258 U.S. 250, 42 S. Ct. 301, 66 L. Ed. 604 (1922).

In fact, the U.S. Congress could use the *Balint* rationale to stimulate the proper level of care by government employees, as well as those who regularly receive information from such persons. Government employees hold a fiduciary obligation to the government with regard to documents, materials and information placed in their care. It is entirely appropriate to hold such persons to have a high standard of care. The legal policy should encourage government employees to be diligent when handling classified information. In the case of journalists, lobbyists and academics, these persons are generally sophisticated consumers of government information. The legal policy should encourage the recipients of classified information to ask questions about the nature of information, particularly if it is not readily available to the general public. The proposed statute does, however, make an important distinction between leakers and recipients: the proposed statute creates a strict liability offense for persons having lawful possession of classified information or documents, but criminalizes only the knowing receipt of classified information or documents. In short, the government would be required to prove scienter against media recipients of classified information or documents.

CONTENT-BASED REGULATION UNDER THE FIRST AMENDMENT

The Supreme Court recognizes that the government may regulate the specific content conveyed by speech if the regulation involves a compelling government interest and the regulation uses the least restrictive means. In effect, the government can restrain prior publication of national security information within certain limits. In *Sable Communications* the Supreme Court reviewed a federal statute that banned indecent as well as obscene commercial telephone messages. The Court held that the government may regulate the content of

constitutionally protected speech to promote a compelling interest if it chooses the least restrictive means to further the articulated interest.[132] Here, the protection of national security from external threat is a compelling government interest. The government must show that the law is designed to serve that end and not some unrelated purpose (the law must not be overbroad). It would, for example, be insufficient if the government sought to preclude publication of material already in the public domain, over-classified material otherwise releasable under the Freedom of Information Act, or material that was politically embarrassing to the Administration. Finally, the government must show that the law has been narrowly drawn to affect only that type of speech that the government has a compelling need to suppress.

PROMOTES THE GOVERNMENT'S COMPELLING INTERESTS

The proposed statute promotes the government's interest in protecting national security from external threat. The proposed statute recognizes the fiduciary obligation of those persons who have authorized access to and possession of classified information and/or documents. Like its British cousin, the proposed statute creates a two-tier structure in U.S. law, reserving the Espionage Act and its sanctions for the more serious crime of espionage committed by government employees. The proposed statute recognizes that recipients of classified information and/or materials provide the most effective means of identifying the culpable parties. In the *Morison* case, the Navy had the full cooperation of *Jane's Defence Weekly*. The statute recognizes the cooperation of *Jane's Defence Weekly* in the *Morison* case was an anomaly, not

[132] *Sable Communications of California v. Federal Communications Commission*, 492 U.S. 115 (1989).

likely to occur in future cases. In fact, the statute recognizes that recipients of classified information are actually parties to criminal activity. Indeed, the Ashcroft Report stated: "It has been noted, repeatedly, for at least the past twenty years, that a leak is extremely difficult, for a number of reasons, to trace back to the responsible party."[133]

The media should not be shielded from either identifying the source of the disclosed information or from return of purloined documents. Moreover, the media should not be immune from criminal liability where the media has knowingly taken possession of illegally released material, particularly where someone has committed a crime by providing the material to the media in the first place. Again, the government would be required to prove scienter in cases involving media recipient of classified information or documents. Indeed, the law should clearly provide that all persons having received classified information by unauthorized disclosure shall be compelled to disclose the source of that information. With respect to the First Amendment case law, it should be noted that there is neither an attempt to restrain publication of information obtained by the media nor an attempt to impose criminal liability for unknowing receipt of classified information. The sole scope of this subsection should be to compel disclosure of the source so that persons guilty of breaching public trust by leaking classified information or documents can be prosecuted. Source protection should not be an inviolate media right, particularly when it comes to information and documents classified by the government in the national interest.

[133]Ashcroft, Draft Report, 50.

LEAST RESTRICTIVE MEANS

The proposed statute is the least restrictive means of promoting the government's compelling interests in protecting national security. The application of the Espionage Act to leak cases is problematic because of the statutory references to "information respecting the national defense." This statute, by contrast, applies to classified information. In fact, the current laws regarding the classification of information are narrowly drawn to protect only specified categories of information and avoid over-breadth problems. Executive Order 12958 requires that to be classified information must concern at least one of the following: military plans or capabilities, foreign government information; intelligence activities; scientific, technical or economic matters related to national security; U.S. programs for safeguarding nuclear materials or facilities; or national security vulnerabilities. In short, the proposed statute avoids over-breadth problems.

Initially, it should not matter whether the information was or was not properly classified. Under Executive Order 12356, § 5.5 (b)(1), officers and employees of the United States Government can be sanctioned to include reprimand, suspension without pay, removal or termination of classification authority, or loss or denial of access to classified information, if they "knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under this Order or predecessor orders . . . ." This language should be amended to cover information "clearly marked or represented to be properly classified pursuant to either a statute or an Executive Order."

In *Scarbeck v. United States,* the Court of Appeals considered the conviction of a State Department employee under 50 U.S.C. § 783 (b) for communicating classified information to the

Polish Government.[134] He argued that the government had the burden of proving that the documents he passed to Polish officers had been properly classified. The Court noted that the statute did not require that the information must have been properly classified as affecting the national security of the United States. The court found that the important elements were the security classification of the material by an official authorized to do so and the transmission of the material by the accused with the knowledge that the material had been so classified.

The "properly classified" language, however, obscures three different issues. The first issue is whether the document was inappropriately classified; in other words, was an unclassified document labeled classified either to avoid public embarrassment or to cover-up wrongdoing. The second issue is whether the classification decision was made by someone with the proper authority. The third issue is whether a document is misclassified; in other words, was a document not properly classified with the appropriate caveats, but instead inadvertently marked SECRET//NOFORN (no foreign dissemination). The first case may be a relatively uncommon occurrence. The latter instances probably happen all too often. This leaves open the problem involving unmarked information that has been received and should be classified, but the classification authority has not yet been able to act upon it in the due course of business. In fact, it should not make a difference whether or not the document was properly classified, the important fact should be whether or not the officer or employee knew that the document was marked classified under a claim of law. As a matter of public policy, individual officers or employees should not arrogate to themselves the decision whether classified information is "properly classified." The media should be prosecuted only for the knowing receipt of classified information or documents.

---

[134] *Scarbeck v. United States*, 317 F.2d 546 (D.C. Cir. 1963), *cert. denied*, 83 S.Ct. 1897 (1963). N.B.: 50 U.S.C. § 783 (b) was subsequently repealed by Congress on other grounds.

One oft-repeated argument is that the government over-classifies information, sometimes for inappropriate reasons. William G. Florence, a former Pentagon security officer, testified before Congress over thirty years ago that of twenty million classified documents, "less than one-half of 1 percent . . . actually contain information qualifying even for the lowest defense classification . . . ." [135] As one government commission pointed out in 1997: "Excessive secrecy has significant consequences when policymakers are not fully informed, government is not held accountable for its actions, and the public cannot engage in informed debate."[136] While some fear over-classification as a threat to representative democracy, an officer or employee should proceed through proper declassification channels to permit the public disclosure of the information. Indeed, the federal government has made significant changes over the past thirty years in terms of limiting the classification of new documents and in promoting the declassification of older documents. Executive Order 12356 is significant in that it places the burden on the prosecution, in terms of proving the elements of a crime, that the accused released documents that were "properly classified." Again, this language should be amended to cover information "clearly marked or represented to be properly classified pursuant to either a statute or an Executive Order."

While Mr. Florence's statement may have been once true, it is open to serious question whether it is true today. The presumption should be that the U.S. government properly classifies documents; the Defendant should have the burden, as an affirmative defense, of proving that he released documents that were not actually classified. From a public policy perspective, the law should be framed such that aggrieved persons are expected to bring problems with over-

---

[135] "Plugging the Leak: The Case for a Legislative Resolution of the Conflict Between the Demands of Secrecy and the Need for an Open Government," Note, 71 *Virginia Law Review* 5 (June 1985): 854.

[136] "Report of the Commission on Protecting and Reducing Government Secrecy."

classification through Inspector General channels and, if necessary, seek protection through the *Whistleblower Protection Act*.[137] A whistleblower is an employee, former employee or other member of an organization who reports misconduct to people who have the power to take corrective action. Under federal law, federal employees benefit from the *Whistleblower Protection Act* in that it makes federal agencies liable for the economic damages caused by unlawful retaliation.

REDUCES POSSIBLE DAMAGE TO COMPELLING INTERESTS

In *Sable Communications* the Supreme Court held that the government may regulate the content of constitutionally protected speech to promote a compelling interest if it chooses the least restrictive means to further the articulated interest.[138] One important aspect is that the government must show that the law has been narrowly drawn to affect only that type of speech that the government has a compelling need to suppress. The proposed statute is narrowly drawn to protect imagery intelligence (IMINT), signals intelligence (SIGINT), and human intelligence (HUMINT) through a least restrictive means of identifying culpable persons.

The proposed statute would help the government in the prosecution of leaks involving IMINT. The United States uses national technical means (NTM) to conduct overhead surveillance of foreign locations. Leaks of U.S. NTM imagery and targets have proven detrimental to the U.S. Intelligence Community. The *Morison* case is an excellent example of the damage that can be caused to national security by leaks of imagery. While the Soviet Union

[137] 5 U.S.C. § 1221 (e).

[138] *Sable Communications of California v. Federal Communications Commission*, 492 U.S. 115 (1989).

knew that the United States had the capability to take overhead photographs, the publication of the photographs confirmed the extent of U.S. technical capabilities. In another example, a 1996 leak of imagery enabled India to understand U.S. NTM capabilities and employ an effective denial and deception to cover preparations for its 1998 nuclear tests.[139] When an imagery product is leaked to the press, it should be possible to match that product to the original classified product. The original document can provide forensic evidence of its origins. In short, the government should have no difficulty making a prima facie showing that the media representative has or had in his possession a classified document.

When an adversary learns the nature and extent of U.S. capabilities, that adversary can take steps to either reduce the effectiveness of U.S. collection systems or determine the best deception practices, all resulting in needless time and expense to the U.S. government as well as the dangers caused by a lack of timely, relevant information about an adversary's capabilities. The importance of timely, effective collection systems cannot be overstated. For example, the U-2 over-flights of the Soviet Union during the late 1950's helped establish that a bomber and later a missile gap did not exist in favor of the Soviet Union, thereby saving the American taxpayer needless time and expense.

The proposed statute would also assist the government in the prosecution of leaks involving SIGINT. The compromise of a SIGINT source could result in an adversary's improvement in security practices or his use of that knowledge to deceive the United States with false information. In one example, after a 1971 press disclosure, the Soviet Union began enciphering limousine telephone calls between Politburo members, drying up a valuable source

---

[139] James B. Bruce, "How Leaks of Classified Intelligence Help U.S. Adversaries: Implications for Laws and Secrecy," in *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, ed. Roger Z. George (Washington, D.C.: National Defense University Press, 2004), 403.

of intelligence.[140] SIGINT represents a unique capability and product that is not commercially available. As in the case of the telephone calls between Politburo members, a member of the press could only have received this type of information, either directly or indirectly, from a source well-placed in government. Again, the government should have no difficulty making a prima facie showing that the media representative has or had in his possession a classified document.

The proposed statute would, however, provide only limited help to the government in the prosecution of leaks involving HUMINT. In terms of HUMINT, the United States uses clandestine agents and often works closely with foreign intelligence services. The compromise of a HUMINT source could, therefore, cause a foreign source to be less than forthcoming, the death of the source, or an unwillingness of a foreign service to work with the United States. In one example, Philip Agee, a former CIA officer, published a book that identified the Richard Welch as the station chief in Athens.[141] Welch was subsequently gunned down on 23 December 1975. Unlike the transmission of information that could have only come from either SIGINT or IMINT, oral information such as the identity of an intelligence source or operative could possibly come from multiple sources and is more difficult to trace to its origin. In short, it would still be difficult to establish a prima facie for disclosure of the source, unless the leaked information is very specific or documentary.

In sum, the proposed statute should remedy many of the gaps, inequities and issues in existing law with regard to the problem of unauthorized disclosure of classified information.

---

[140] Bruce, "How Leaks of Classified Intelligence Help U.S. Adversaries," 402.

[141] (b) (3), (b) (6), "Legislative and Judicial Safeguards for US Intelligence Personnel," *Studies in Intelligence*, vol. 42 no. 2 (1998): 35-44.

The proposed statute builds upon many of the positive aspects of existing law, without adopting the broad, catch-all provisions that existed in the British Official Secrets Act 1911. The proposed statute creates a clear, logical structure that addresses the leak problem. It will not, however, provide a "fool proof" means of stopping unauthorized disclosure or prosecuting leakers who get caught.

CHAPTER 6

CONCLUSION

Representative Pete Hoekstra, former Chairman of the House Permanent Select Committee on Intelligence, opined that the leak problem could only worsen as the Intelligence Community (IC) presses for increased, community-wide information sharing. In part, Jonathan Pollard was able to wreak incalculable damage on the IC because of a willingness to share information between agencies. He amassed thousands of publications and documents related to the Soviet Union and the Middle East, but clearly unrelated to his duties as a Caribbean analyst. A policy that promotes information-sharing also raises a second serious concern - as more people have access to more information than ever before, it will become that much more difficult to investigate the source of a leak. At root level, there are several critical aspects to the leak problem. The IC must have effective investigative tools to search for and identify the source of the leak. And the framework of laws should be tailored for both leakers and recipients, with appropriate penalties based upon culpability.

The IC must have effective investigate tools. Security education can help eliminate inadvertent leaks and can help identify some of the more blatant leaks. Jonathan Pollard presents an interesting "what if" case. By September 1980, when his initial one-year probationary period with the Navy was ending, the Navy had already identified Mr. Pollard as a security risk. In fact, the Naval Investigative Service had already opened a counter-intelligence file on him.

Unfortunately, Mr. Pollard's chain of command may have been unaware of their legal authority to terminate him at that point.[142] Over the course of his subsequent employment, there were more than sufficient clues that should have alerted his co-workers that something was amiss. For example, he had performance problems, routinely collected intelligence products unrelated to his current duties, made repeated and obviously fabricated assertions about his foreign contacts, and violated numerous security practices. It was, however, an alert co-worker who reported him leaving a secure facility on a Friday afternoon with a top secret document and a conscientious supervisor who acted upon the co-worker's information. Subsequently, acting upon sparse information, astute investigators were able to unravel the story and elicit a confession from him.[143] Less blatant leaks, however, will require more effective tools.

As noted by Mr. Aftergood, reporters are not passive recipients of classified information but are instead part of the problem. Reporters are sophisticated consumers of information, usually with well-placed contacts in government. If a government official wants to leak a story, he usually knows who will make good use of that information while vigorously protecting the identity of his source. If, on the other hand, a reporter wants a story, he too usually knows who will talk to him and what promises will have to be exchanged to get that story. In short, reporters are frequently accomplices to crime when it comes to leaks, often word-smithing the story in the right way to protect their sources and methods. Thus, a well-crafted leak law should provide the government with the tools to facilitate a prompt investigation to identify the source. If the law were to compel disclosure of sources, it would make it possible to prosecute what in many cases has been misprision of a felony by members of the press. Nonetheless, reporters are not the root

[142] Ronald J. Olive, *Capturing Jonathan Pollard* (Annapolis, MD: Naval Institute Press, 2006), 23.

[143] Olive, *Capturing Jonathan Pollard*, 101.

of the problem, but reporters are frequently the best sources of information concerning the identity of the leaker.

In addition, the government must craft a structure of laws that addresses the various espionage and leak problems that confront the Intelligence Community. The United States does have a patchwork of existing laws with many strengths and weaknesses. While the Attorney General may be satisfied that the gaps in existing law are only technical and not practical, other informed observers believe that changes would be appropriate to harmonize current law, resolving the gaps, inequities and issues. This thesis has reviewed three viable alternatives to existing U.S. law: the Shelby Amendment, the British Official Secrets Act and the author's proposal. Each approach has its merits. While British law is frequently criticized in the United States, it does have numerous meritorious points that should be considered in revising U.S. law. Arguably, the Shelby Amendment fails to account for the role of the media in a direct manner. The author's proposal does so, but it would likely be vehemently opposed by the press. Nonetheless, the author contends that because the press is part of the problem that it should be part of the solution.

If the U.S. government were to structure the espionage and leaks into a two-part structure like the British Official Secrets Act, it would help in several ways. Revised laws could enhance the government's ability and willingness to investigate and prosecute leak cases. John L. Martin, a former Justice Department official who supervised espionage prosecutions noted that "the Justice Department generally has chosen not to prosecute suspected leakers because it is difficult to prove that a particular person was the source of the leak and such cases often would require

subpoenaing reporters and editors, leading to messy First Amendment issues."[144] Second, as the government expands its efforts to investigate and prosecute leak cases, it whould have a deterrent effect on would-be leakers and their accomplices. For example, *Washington Times* reporter Bill Gertz has said: "When I get information, I don't care where it comes from or why it came to me, but [whether] it's news and important."[145] In fact, reporters should care because they do have a basic legal obligation not to solicit or facilitate criminal activity. The journalistic thirst for a story must know some bounds.

There are important policy interests that must be considered when crafting new laws proscribing unauthorized disclosures of classified information. First, there must be some level of judicial and legislative oversight of Executive branch classification decisions. The law should punish only those persons who leak "properly" classified information. Second, there must be some balance between the government's need for secrecy and the public's interest in maintaining government accountability. While the press has overstepped the bounds of propriety in some cases, the press also performs an important role in a democracy. In short, in cases where civic-minded government employees cannot otherwise stop illegal, wasteful or corrupt activity, the press leak can serve as a socially useful dissent channel. On the other hand, the government cannot condone such activity. Intelligence Community employees must be advised about the correct procedures for raising such doubts. If an IC employee still chooses to go forward with a leak to the media, then that person should do so with the full risk of criminal prosecution and punishment.

---

[144] Michael Hurt, "Leaking National Security Secrets: Effects on Security and Measures to Mitigate," *National Security Studies Quarterly* 7, no. 4 (Autumn 2001): 20. Cited hereafter as Hurt, "Leaking National Security Secrets."

[145] Hurt, "Leaking National Security Secrets," at 29-30.

The government's right to maintain secrecy has an uncertain paternity in the United States. The framers of the Constitution recognized the need for some secrecy in government, but may not have recognized the inchoate tension with the First Amendment freedoms of speech and press. The Constitution obligates each House to keep and publish a journal of its proceedings, excepting those parts it determines to keep secret.[146] The Constitution does not, however, acknowledge a power in the Executive branch to impose rules of secrecy. Nevertheless, President George Washington asserted such a right regarding defense and foreign affairs, to include refusing compliance in 1796 with a request by the House of Representatives for information about treaty negotiations with Great Britain. On other hand, the Constitution recognizes neither the oft-claimed press privilege of source confidentiality nor a prohibition against persons who express free speech by disclosing classified information. In short, the Constitution does not bar passage of official secrets legislation in the United States. The Congress can, therefore, balance the need for secrecy and civil liberties as it sees fit to protect classified information.

[146] *U.S. Constitution*, Article 1, sec. 5, clause 3.

APPENDIX A

TABLE OF U.S. STATUTES

STATUTE	ACTUS REUS	BY WHOM	TO WHOM	MENS REA	SENTENCE
18 USC § 371 Conspiracy	Conspiracy	Two or more persons		"to commit any offense against the United States, or to defraud the United States"	5 years or $10k fine
18 USC § 641 Theft Statute	Theft of public record, voucher, money or "thing of value"	Whoever	Applies persons who receive, conceal, or retain "the same with the intent to convert it to his use or gain"	BY WHOM: "whoever embezzles, steals, purloins or knowingly converts to use" TO WHOM: "knowing it to have been embezzled, stolen, purloined or conveyed."	10 years or $10k fine
18 USC § 793a Espionage Act (1917)	Gathering National Defense Information	Whoever	N/A	"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" N.B.: "while upon places connected with national defense"	10 years or fine, or both; and Forfeiture of Foreign Proceeds

STATUTE	ACTUS REUS	BY WHOM	TO WHOM	MENS REA	SENTENCE
18 USC § 793b Espionage Act (1917)	Copies, Takes, Makes or Obtains National Defense Information	Whoever	N/A	"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"	10 years or fine, or both; and Forfeiture of Foreign Proceeds
18 USC § 793c Espionage Act (1917)	Receipt or attempted receipt of documents, etc – national defense Materials N.B.: Catch-all sub-section	Whoever	N/A	"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" contrary to this chapter (Espionage & Censorship)	10 years or fine, or both; and Forfeiture of Foreign Proceeds
18 USC § 793d Espionage Act (1917)	Transmission of § 793a national defense materials, including information; or Retention of materials after demand N.B.: Applies to sources of leaked information	"Whoever, having lawful possession of, access to, control over, or being entrusted with"	To "any person not entitled to receive it, or willfully retains the same" N.B.: Self-incrimination issue on retention offense?	Possessor willfully communicates, delivers or transmits materials, or causes or attempts the same; or willfully retains the same and fails to deliver to government officer or employee. N.B.: Minimum culpability standard. Information has higher scienter requirement: "has reason to believe could be used to the injury of the US or to the advantage of any foreign nation"	10 years or fine, or both; and Forfeiture of Foreign Proceeds

STATUTE	ACTUS REUS	BY WHOM	TO WHOM	MENS REA	SENTENCE
18 USC § 793e Espionage Act (Added by Internal Security Act of 1950)	Transmission of § 793a national defense materials Retention of materials N.B.: Applies to recipients of leaked material	"Whoever having unauthorized possession of, access to, or control over"	"to any person not entitled to receive it, or willfully retains" N.B.: Self-incrimination issue on retention offense?	Possessor willfully communicates, delivers or transmits materials, or causes or attempts the same; or willfully retains the same and fails to deliver to government officer or employee N.B.: Minimum culpability standard. Information has higher scienter requirement: "has reason to believe could be used to the injury of the US or to the advantage of any foreign nation"	$10k or 10 years or both, & Forfeiture of Foreign Proceeds
18 USC § 793f Espionage Act (1917)	Removal or loss of national defense materials "from proper place of custody"	"Whoever, being entrusted with or having lawful possession or control"	N/A	1. Applies gross negligence standard to person who removed material or permitted it to be lost/stolen. 2. Applies knowledge standard to person who was aware but failed to report it.	Fine or 10 years or both, & Forfeiture of Foreign Proceeds
18 USC § 793g Espionage Act (1917)	Conspiracy to Violate § 793	Two or more persons			As provided for in applicable section

STATUTE	ACTUS REUS	BY WHOM	TO WHOM	MENS REA	SENTENCE
18 USC § 794a Espionage Act (1917)	Transmission - national defense materials	Whoever	To any foreign recipient, directly or indirectly	"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"	Term of Years or Life or Death
18 USC § 794b Espionage Act (1917)	Attempts to communicate or communicates any information N.B.: includes preparatory acts	"Whoever, in time of war" N.B.: declared war only?	N/A	"with intent that the same shall be communicated to the enemy" N.B.: direct or indirect communication? N.B.: state of mind over consequences is irrelevant	Term of Years or Life or Death
18 USC § 795 Espionage Act (1938)	Photography or sketching defense installations where the President has declared it illegal	Whoever	N/A	Strict Liability Standard	Fine or 1 year or both
18 USC § 796 Espionage Act (1938)	Use of aircraft to photo of defense installation prohibited under § 795	Whoever	N/A	Strict Liability Standard	Fine or 1 year or both
18 USC § 797 Espionage Act (1938)	Publication or sale of photos of defense install prohibited under § 795	Whoever	N/A	Strict Liability Standard	Fine or 1 year or both

STATUTE	ACTUS REUS	BY WHOM	TO WHOM	MENS REA	SENTENCE
18 USC § 798 SIGINT Statute (1950)	Disclosure of classified information re: codes, ciphers or cryptographic or COMINT systems	Whoever	To anyone unauthorized	"knowingly and willfully communicates, furnishes, transits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interests of the United States"	10 years
18 USC § 951	Acts as an agent of a foreign govt	Whoever	Foreign government	Person agrees to operate in the USA under foreign control	Fine or 10 years or both
18 USC § 952 (1933) Diplomatic Codes (Response to H.O. Yardley book)	Disclosure of "any official diplomatic code or any matter prepared in any such code" or purported to be in such code	Whoever, by virtue of government employment	Publishes or furnishes to another	"willfully publishes or furnishes to another any such code or matter, or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States"	Fine or 10 years or both
18 USC § 953 Logan Act	Conducts private correspondence with a foreign government	Any citizen of the United States	Foreign Government	"with the intent to influence the measures or conduct of any foreign government . . . in relation to disputes or controversies with the United States or to defeat the measures of the United States"	Fine or 3 years

STATUTE	ACTUS REUS	BY WHOM	TO WHOM	MENS REA	SENTENCE
18 USC § 1001 False Statements Accountability Act	False Statements by government officials	Whoever	N/A	"makes materially false, fictitious, or fraudulent statement or representation"	Fine of $10k or 5 years or both
18 USC § 1030 Computer Fraud and Abuse Act	Accessing protected information without authorization or exceeding authorization	Whoever	NA	"knowing accessed a computer" and "willfully transmits" information harmful to the US or "willfully retains"	Fine or 10 year or both
18 USC § 1924	Unauthorized Removal and Retention of Classified Documents or Material	Whoever . . . and having lawful possession of classified documents		"knowingly removes such documents or materials without authority and with intent to retain such documents or material at an unauthorized location"	Fine of $1000 or One Year
42 USC § 2274 Atomic Energy Act	Communicates, transmits or discloses Restricted Data	Whoever	"to any individual or person"	“with intent to injure the United States or with intent to secure an advantage to any foreign nation”	Fine of $100k or Life or both

STATUTE	ACTUS REUS	BY WHOM	TO WHOM	MENS REA	SENTENCE
42 USC § 2275 Atomic Energy Act	Receipt of Restricted Data	Whoever	NA	"with intent to injure the United States or with intent to secure an advantage to any foreign nation"	Fine of $100k or Life or both
42 USC § 2276	Tampering with Restricted Data	Whoeover	NA	"with the intent to injure the United States"	Life or term of years $20k fine or both
42 USC § 2277 Atomic Energy Act	Disclosure of Restricted Data	Whoever, having been an employee or member of the Commission, military or US government, to include contractors and licensees	NA	"knowingly communications, or whoever conspires to communicate or to receive any Restricted Data, to any person not authorized to receive Restricted Data"	Fine of $12,500
50 USC § 421a Intelligence Identities Protection Act of 1982	"discloses any information identifying such covert agent"	"Whoever, having or having had authorized access to classified information that identifies a covert agent"	"to any individual not authorized to receive classified information"	"knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States"	Fine of $50k or 10 years or both

STATUTE	ACTUS REUS	BY WHOM	TO WHOM	MENS REA	SENTENCE
50 USC § 421b Intelligence Identities Protection Act of 1982	"discloses any information identifying such covert agent"	"Whoever, as a result of having authorized access to classified information, learns the identity of a covert agent"	"to any individual not authorized to receive classified information"	"knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agents' intelligence relationship to the United States"	Fine of $25k or 5 years or both
50 USC § 421c Intelligence Identities Protection Act of 1982	"discloses any information that identifies an individual as a covert agent"	Whoever	"to any individual not authorized to receive classified information"	"in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impede or impair the foreign intelligence activities of the United States"	Fine of $15 or 3 years pr both
50 USC § 781 McCarran Act REPEALED	Photos, sketching, mapping military installation	"Whoever, except in performance of duty or employment in connection with national defense"		"shall knowingly and willfully make any sketch, photograph, photographic negative," etc of military installation, equipment	Fine or 1 year or both
50 USC § 782 McCarran Act REPEALED	Permission to Photo, sketch or map military installation	NA	Secretary of War or Navy	Permission may be granted when "the interests of national security will not be adversely affected"	NA

STATUTE	ACTUS REUS	BY WHOM	TO WHOM	MENS REA	SENTENCE
50 USC § 783 Internal Security Act McCarran Act REPEALED	Communication or attempted receipt of classified information	"any officer or employee"	"to any other person whom such officer or employee knows or has reason to believe to be an agent … of any foreign government"	"any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified"	Fine of $10 or 10 years or both, and disqualification from official office
UCMJ Art. 104 Aiding the Enemy	Aids or attempts to aid	military personnel	the enemy	"knowingly harbors or protects or gives intelligence to or communicates or corresponds with or holds any intercourse with the enemy"	Death
UCMJ Art. 106(a) Espionage	"collecting or attempting to collect certain information"	military personnel during time of war	the enemy	"with the intent to convey this information to the enemy"	Death
UCMJ Art. 134 General Order	"all disorders and neglects" - used to charge §§ 793/794 violations	military personnel		prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces	Varies

STATUTE	REMEDY	APPLIES TO	AUTHORITY	STANDARD	COMMENTS
10 USC § 1609	Termination of Defense Intel EE	EE in defense intelligence position	SECDEF	If the SECDEF determines the action to be in the interests of the US and "determines that the procedures prescribed in other provisions of the law … cannot be invoked in a manner consistent with national security."	Lawrence Franklin?
50 USC § 402	Three year Limitation on Post Employment Activities	Applies to CIA	DCI	"may not represent or advise the government, or any political party, of any foreign country"	Potential loss of retirement benefits
50 USC § 403-404(h)	Termination of CIA Employee	Applies to CIA	DCI	"whenever the Director shall deem such termination necessary or advisable in the interests of the United States"	
EO 10450 (1953)	Security Requirements; Investigations	Any officer or employee of government	Department & Agency Heads	Appointments to positions are subject to investigation shall include, *inter alia*, "Intentional, unauthorized disclosure to any person of security information, or of other information disclosure of which is prohibited by law, or willful violation or disregard of security regulations"	Referral to FBI for full field investigation
EO 12958, § 5.7(b) (1995)	Sanctions: denial of access, removal, reprimand, and suspension.	Officers and employees of the United States Government		"knowingly, willfully, or negligently disclose to unauthorized persons information properly classified"	"Properly classified" tracks with FOIA, 5 USC § 552(b)(1)

STATUTE	REQUIREMENT	APPLIES TO	AUTHORITY	REMEDY	COMMENTS
5 USC § 7513 10 USC § 986	Access to National Security Information	All Government Employees	EO 12968 (1995)	May reinvestigate at any time there is reason to believe that the person no longer meets the standards for access	*Dept of Navy v. Egan,* 484 U.S. 518 (1988)
5 USC. § 8312	Conviction Under Selected Statutes	All Government Employees	18 USC § 793 18 USC § 798 42 USC § 2272-2276 50 USC § 421	Forfeiture of Retirement Pay	
22 USC § 211	Likelihood of "serious damage" to national security	U.S. citizens		Revocation of US passport	*Haig v. Agee*, 453 U.S. 280 (1980)
50 USC 403(d)	Pre-Publication Review	Present or past Government Employee	Breach of Contract	Contractual Damages Constructive Trust	*Snepp v. US,* 444 U.S. 507 (1980)

APPENDIX B

TABLE OF U.S. LEAK AND REPRESENTATIVE ESPIONAGE CASES

CASE/YEAR DECIDED	TYPE DEFENDANT	INDICTMENT	PLEA	TRIAL RESULT	SENTENCE
Christopher Boyce (1977)	TRW	18 USC § 641 18 USC § 951 18 USC § 793-4 18 USC § 798		Convicted on all counts	2 x 40 year sentences 6 x 10 year sentences
Truong Dinh Hung (1978)	Vietnam (Foreign National)	18 USC § 371 18 USC § 641 18 USC § 794a/c 18 USC §§ 951-2		Convicted	Remanded by Court of Appeals, 4th Circuit (Jencks Act statements)
Ronald L. Humphrey (1978)	United States Information Agency	18 USC § 371 18 USC § 641 18 USC § 794a/c 18 USC § 951-2		Convicted	Remanded by Court of Appeals, 4th Circuit (Jencks Act statements)
Samuel Morison (1984)	Navy	18 USC § 641 18 USC § 793(d) 18 USC § 793(e)		Convicted of espionage and theft	2 year prison sentence; served 3 months & Received pardon

CASE/YEAR DECIDED	TYPE DEFENDANT	INDICTMENT	PLEA	TRIAL RESULT	SENTENCE
Jonathan Pollard (1985)	US Navy	18 USC § 794(a)	Pled Guilty		Life
Sharon Scranage (1985)	CIA Employee	50 USC § 421(a)			2 years; paroled after 18 months
Robert W. Pelton (1986)	NSA	18 USC § 793		Convicted on espionage and conspiracy counts	Three Concurrent Life Sentences
SGT Clayton Lonetree (1987)	USMC Embassy Security	50 USC § 421(b) UCMJ 106(a) & 134		Convicted of espionage	25 year sentence, reduced to 20 years; released after 9 years
Michael Tobias (1988)	Navy	18 USC § 371 18 USC § 641 18 USC § 793 18 USC § 798		Guilty	20 years
Aldrich Ames (1994)	CIA Officer	18 USC § 794(a)	Plea Bargain		Life

CASE/YEAR DECIDED	TYPE DEFENDANT	INDICTMENT	PLEA	TRIAL RESULT	SENTENCE
Harold J. Nicholson (1996)	CIA Officer	18 USC § 794(a)	Pled to espionage		23 years
Wen Ho Lee (1999)	Los Alamos nuclear scientist	18 USC § 793(c) 18 USC § 793(e) 42 USC § 2275 42 USC § 2276	Pled to 1 Count Felony Download of Restricted Data		Served 278 days and released
Ana B. Montes (2001)	DIA Cuba analyst	18 USC § 794(a)	Pled guilty		25 years
Robert Hanssen (2002)	FBI	18 USC § 794(a)	Pled to espionage & conspiracy		Life without parole; spouse keeps pension
Jonathan Randel (2002)	DEA Civilian	18 USC § 641 18 USC § 1030 18 USC § 1343	Pled to theft		One year
Katrina Leung (aka Parlor Maid) (2003)	Political Activist; Covert Chinese agent	18 USC § 793(b)		Dismissal; prosecutor blocked defense access to witness (James J. Smith)	

CASE/YEAR DECIDED	TYPE DEFENDANT	INDICTMENT	PLEA	TRIAL RESULT	SENTENCE
James J. Smith (2004)	FBI Supervisory Agent	18 USC § 793(f) 18 USC § 1343 18 USC § 1346	Pled to failure to disclose relationship w/ K. Leung (18 USC § 1001)		3 months home confinement and 100 hours of community service
Ryan Anderson (2004)	Washington Army National Guard & Muslim convert	UCMJ 106(a)		Convicted of attempting to aid and provide intelligence to the enemy	Life with possible parole; reduction to E-1; and dishonorable discharge
Donald W. Keyser (2004)	Principal Deputy Asst SecState	18 USC § 793(f) 18 USC § 1001(a)			Released on bond, pending sentence
Sandy Berger (2005)	National Security Adviser	18 USC § 1924	Pled to Misdemeanor		Community Service, Fine & Probation
Lawrence Franklin (2006)	DIA Civilian	18 USC § 371 18 USC § 793 (d) 18 USC § 793 (e) 18 USC § 793 (g)	Pled to Conspiracy Counts		12 years

CASE/YEAR DECIDED	TYPE DEFENDANT	INDICTMENT	PLEA	TRIAL RESULT	SENTENCE
Steven J. Rosen (2006)	Lobbyist	18 USC § 371 18 USC § 793 (d) 18 USC § 793 (e) 18 USC § 793 (g) 50 USC § 783	Pending		
Keith Weissman (2006)	Lobbyist	18 USC § 793 (d) 18 USC § 793 (e) 18 USC § 793 (g)	Pending		
I. Lewis Libby	VP Chief of Staff	Not filed			
Karl Rove	Presidential advisor	Initial target of investigation, but later dropped.			
Judith Miller (2005)	*New York Times* reporter			Civil Contempt Citation; S. Ct. Declined Cert.	Jailed 18 months or until Grand Jury expires

CASE/YEAR DECIDED	TYPE DEFENDANT	INDICTMENT	PLEA	TRIAL RESULT	SENTENCE
Matthew Cooper (2005)	*Times* magazine reporter			Civil Contempt Citation; S. Ct. Declined Cert.	Source voluntarily waived confidentiality
Richard Armitage (2006)	DepSecState	Admission on 9/7/06; charges not filed			
Mary McCarthy (2006)	CIA Officer	Not filed; Leak related to Detainee Policy			Terminated 20 April 2006 (10 days before retirement); will receive pension

APPENDIX C

SHELBY AMENDMENT TO THE FY01 INTELLIGENCE AUTHORIZATION ACT

SEC. 304. PROHIBITION ON UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION.

(a) In General.--Chapter 37 of title 18, United States Code, is amended--

(1) by redesignating section 798A as section 798B; and

(2) by inserting after section 798 the following new section 798A:

``Sec. 798A. Unauthorized disclosure of classified information

`` (a) Prohibition.--Whoever, being an officer or employee of the United States, a former or retired officer or employee of the United States, any other person with authorized access to classified information, or any other person formerly with authorized access to classified information, knowingly and willfully discloses, or attempts to disclose, any classified information acquired as a result of such person's authorized access to classified information to a person (other than an officer or employee of the United States) who is not authorized access to such classified information, knowing that the person is not authorized access to such classified information, shall be fined under this title, imprisoned not more than 3 years, or both.

`` (b) Construction of Prohibition.--Nothing in this section shall be construed to establish criminal liability for disclosure of classified information in accordance with applicable law to the following:

`` (1) Any justice or judge of a court of the United States established pursuant to article III of the Constitution of the United States.

`` (2) The Senate or House of Representatives, or any committee or subcommittee thereof, or joint committee thereof, or any Member of Congress.

`` (3) A person or persons acting on behalf of a foreign power (including an international organization) if the disclosure--

`` (A) is made by an officer or employee of the United States who has been authorized to make the disclosure; and

`` (B) is within the scope of such officer's or employee's duties.

`` (4) Any other person authorized to receive the classified information.

``(c) Definitions.--In this section:

`` (1) The term `authorized', in the case of access to classified information, means having authority or permission to have access to the classified information pursuant to the provisions of a statute, Executive order, regulation, or directive of the head of any department or agency who is empowered to classify information, an order of any United States court, or a provision of any Resolution of the Senate or Rule of the House of Representatives which governs release of classified information by such House of Congress.

`` (2) The term `classified information' means information or material properly classified and clearly marked or represented, or that the person knows or has reason to believe has been properly classified by appropriate authorities, pursuant to the provisions of a statute or Executive order, as requiring protection against unauthorized disclosure for reasons of national security.

`` (3) The term `officer or employee of the United States' means the following:

`` (A) An officer or employee (as those terms are defined in sections 2104 and 2105 of title 5).

`` (B) An officer or enlisted member of the Armed Forces (as those terms are defined in section 101(b) of title 10).".

(b) Clerical Amendment.--The table of sections at the beginning of that chapter is amended by striking the item relating to section 798A and inserting the following new items:

``798A. Unauthorized disclosure of classified information.
``798B. Temporary extension of section 794.".

APPENDIX D

BRITISH OFFICIAL SECRETS ACT 1989

An Act to replace section 2 of the Official Secrets Act 1911 by provisions protecting more limited classes of official information.
[11th May 1989]

Be it enacted by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

Security and intelligence.

1.—(1) A person who is or has been—

(a) a member of the security and intelligence services; or

(b) a person notified that he is subject to the provisions of this subsection,

is guilty of an offence if without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services or in the course of his work while the notification is or was in force.

(2) The reference in subsection (1) above to disclosing information relating to security or intelligence includes a reference to making any statement which purports to be a disclosure of such information or is intended to be taken by those to whom it is addressed as being such a disclosure.

(3) A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he makes a damaging disclosure of any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as such but otherwise than as mentioned in subsection (1) above.

(4) For the purposes of subsection (3) above a disclosure is damaging if—

(a) it causes damage to the work of, or of any part of, the security and intelligence services; or

(b) it is of information or a document or other article which is such that its unauthorised disclosure would be likely to cause such damage or which falls within a class or description of information, documents or articles the unauthorised disclosure of which would be likely to have that effect.

(5) It is a defence for a person charged with an offence under this section to prove that at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the information, document or article in question related to security or intelligence or, in the case of an offence under subsection (3), that the disclosure would be damaging within the meaning of that subsection.

(6) Notification that a person is subject to subsection (1) above shall be effected by a notice in writing served on him by a Minister of the Crown; and such a notice may be

served if, in the Minister's opinion, the work undertaken by the person in question is or includes work connected with the security and intelligence services and its nature is such that the interests of national security require that he should be subject to the provisions of that subsection.

(7) Subject to subsection (8) below, a notification for the purposes of subsection (1) above shall be in force for the period of five years beginning with the day on which it is served but may be renewed by further notices under subsection (6) above for periods of five years at a time.

(8) A notification for the purposes of subsection (1) above may at any time be revoked by a further notice in writing served by the Minister on the person concerned; and the Minister shall serve such a further notice as soon as, in his opinion, the work undertaken by that person ceases to be such as is mentioned in subsection (6) above.

(9) In this section "security or intelligence" means the work of, or in support of, the security and intelligence services or any part of them, and references to information relating to security or intelligence include references to information held or transmitted by those services or by persons in support of, or of any part of, them.

Defence.

2.—(1) A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he makes a damaging disclosure of any information, document or other article relating to defence which is or has been in his possession by virtue of his position as such.

(2) For the purposes of subsection (1) above a disclosure is damaging if—

(a) it damages the capability of, or of any part of, the armed forces of the Crown to carry out their tasks or leads to loss of life or injury to members of those forces or serious damage to the equipment or installations of those forces; or

(b) otherwise than as mentioned in paragraph (a) above, it endangers the interests of the United Kingdom abroad, seriously obstructs the promotion or protection by the United Kingdom of those interests or endangers the safety of British citizens abroad; or

(c) it is of information or of a document or article which is such that its unauthorised disclosure would be likely to have any of those effects.

(3) It is a defence for a person charged with an offence under this section to prove that at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the information, document or article in question related to defence or that its disclosure would be damaging within the meaning of subsection (1) above.

(4) In this section "defence" means—

(a) the size, shape, organisation, logistics, order of battle, deployment, operations, state of readiness and training of the armed forces of the Crown;

(b) the weapons, stores or other equipment of those forces and the invention, development, production and operation of such equipment and research relating to it;

(c) defence policy and strategy and military planning and intelligence;

(d) plans and measures for the maintenance of essential supplies and services that are or would be needed in time of war.

International relations.

3.—(1) A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he makes a damaging disclosure of—

(a) any information, document or other article relating to international relations; or

(b) any confidential information, document or other article which was obtained from a State other than the United Kingdom or an international organisation,

being information or a document or article which is or has been in his possession by virtue of his position as a Crown servant or government contractor.

(2) For the purposes of subsection (1) above a disclosure is damaging if—

(a) it endangers the interests of the United Kingdom abroad, seriously obstructs the promotion or protection by the United Kingdom of those interests or endangers the safety of British citizens abroad; or

(b) it is of information or of a document or article which is such that its unauthorised disclosure would be likely to have any of those effects.

(3) In the case of information or a document or article within subsection (1)(b) above—

(a) the fact that it is confidential, or

(b) its nature or contents,

may be sufficient to establish for the purposes of subsection (2)(b) above that the information, document or article is such that its unauthorised disclosure would be likely to have any of the effects there mentioned.

(4) It is a defence for a person charged with an offence under this section to prove that at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the information, document or article in question was such as is mentioned in

subsection (1) above or that its disclosure would be damaging within the meaning of that subsection.

(5) In this section "international relations" means the relations between States, between international organisations or between one or more States and one or more such organisations and includes any matter relating to a State other than the United Kingdom or to an international organisation which is capable of affecting the relations of the United Kingdom with another State or with an international organisation.

(6) For the purposes of this section any information, document or article obtained from a State or organisation is confidential at any time while the terms on which it was obtained require it to be held in confidence or while the circumstances in which it was obtained make it reasonable for the State or organisation to expect that it would be so held.

Crime and special investigation powers.

4.—(1) A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he discloses any information, document or other article to which this section applies and which is or has been in his possession by virtue of his position as such.

(2) This section applies to any information, document or other article—

(a) the disclosure of which—

(i) results in the commission of an offence; or

(ii) facilitates an escape from legal custody or the doing of any other act prejudicial to the safekeeping of persons in legal custody; or

(iii) impedes the prevention or detection of offences or the apprehension or prosecution of suspected offenders; or

(b) which is such that its unauthorised disclosure would be likely to have any of those effects.

(3) This section also applies to—

(a) any information obtained by reason of the interception of any communication in obedience to a warrant issued under section 2 of the [1985 c. 56.] Interception of Communications Act 1985, any information relating to the obtaining of information by reason of any such interception and any document or other article which is or has been used or held for use in, or has been obtained by reason of, any such interception; and

(b) any information obtained by reason of action authorised by a warrant issued under section 3 of the [1989 c. 5.] Security Service Act 1989, any information relating to the obtaining of information by reason of any such action and any document or other article which is or has been used or held for use in, or has been obtained by reason of, any such action.

(4) It is a defence for a person charged with an offence under this section in respect of a disclosure falling within subsection (2)(a) above to prove that at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the disclosure would have any of the effects there mentioned.

(5) It is a defence for a person charged with an offence under this section in respect of any other disclosure to prove that at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the information, document or article in question was information or a document or article to which this section applies.

(6) In this section "legal custody" includes detention in pursuance of any enactment or any instrument made under an enactment.

Information resulting from unauthorised disclosures or entrusted in confidence.

5.—(1) Subsection (2) below applies where—

(a) any information, document or other article protected against disclosure by the foregoing provisions of this Act has come into a person's possession as a result of having been—

(i) disclosed (whether to him or another) by a Crown servant or government contractor without lawful authority; or

(ii) entrusted to him by a Crown servant or government contractor on terms requiring it to be held in confidence or in circumstances in which the Crown servant or government contractor could reasonably expect that it would be so held; or

(iii) disclosed (whether to him or another) without lawful authority by a person to whom it was entrusted as mentioned in sub-paragraph (ii) above; and

(b) the disclosure without lawful authority of the information, document or article by the person into whose possession it has come is not an offence under any of those provisions.

(2) Subject to subsections (3) and (4) below, the person into whose possession the information, document or article has come is guilty of an offence if he discloses it without lawful authority knowing, or having reasonable cause to believe, that it is protected against disclosure by the foregoing provisions of this Act and that it has come into his possession as mentioned in subsection (1) above.

(3) In the case of information or a document or article protected against disclosure by sections 1 to 3 above, a person does not commit an offence under subsection (2) above unless—

(a) the disclosure by him is damaging; and

(b) he makes it knowing, or having reasonable cause to believe, that it would be damaging;

and the question whether a disclosure is damaging shall be determined for the purposes of this subsection as it would be in relation to a disclosure of that information, document or article by a Crown servant in contravention of section 1(3), 2(1) or 3(1) above.

(4) A person does not commit an offence under subsection (2) above in respect of information or a document or other article which has come into his possession as a result of having been disclosed—

(a) as mentioned in subsection (1)(a)(i) above by a government contractor; or

(b) as mentioned in subsection (1)(a)(iii) above,

unless that disclosure was by a British citizen or took place in the United Kingdom, in any of the Channel Islands or in the Isle of Man or a colony.

(5) For the purposes of this section information or a document or article is protected against disclosure by the foregoing provisions of this Act if—

(a) it relates to security or intelligence, defence or international relations within the meaning of section 1, 2 or 3 above or is such as is mentioned in section 3(1)(b) above; or

(b) it is information or a document or article to which section 4 above applies;

and information or a document or article is protected against disclosure by sections 1 to 3 above if it falls within paragraph (a) above.

(6) A person is guilty of an offence if without lawful authority he discloses any information, document or other article which he knows, or has reasonable cause to believe, to have come into his possession as a result of a contravention of section 1 of the [1911 c. 28.] Official Secrets Act 1911.

Information entrusted in confidence to other States or international organisations.

6.—(1) This section applies where—

(a) any information, document or other article which—

(i) relates to security or intelligence, defence or international relations; and

(ii) has been communicated in confidence by or on behalf of the United Kingdom to another State or to an international organisation,

has come into a person's possession as a result of having been disclosed (whether to him or another) without the authority of that State or organisation or, in the case of an organisation, of a member of it; and

(b) the disclosure without lawful authority of the information, document or article by the person into whose possession it has come is not an offence under any of the foregoing provisions of this Act.

(2) Subject to subsection (3) below, the person into whose possession the information, document or article has come is guilty of an offence if he makes a damaging disclosure of it knowing, or having reasonable cause to believe, that it is such as is mentioned in subsection (1) above, that it has come into his possession as there mentioned and that its disclosure would be damaging.

(3) A person does not commit an offence under subsection (2) above if the information, document or article is disclosed by him with lawful authority or has

previously been made available to the public with the authority of the State or organisation concerned or, in the case of an organisation, of a member of it.

(4) For the purposes of this section "security or intelligence", "defence" and "international relations" have the same meaning as in sections 1, 2 and 3 above and the question whether a disclosure is damaging shall be determined as it would be in relation to a disclosure of the information, document or article in question by a Crown servant in contravention of section 1(3), 2(1) and 3(1) above.

(5) For the purposes of this section information or a document or article is communicated in confidence if it is communicated on terms requiring it to be held in

confidence or in circumstances in which the person communicating it could reasonably expect that it would be so held.

Authorised disclosures.

7.—(1) For the purposes of this Act a disclosure by—

(a) a Crown servant; or

(b) a person, not being a Crown servant or government contractor, in whose case a notification for the purposes of section 1(1) above is in force,

is made with lawful authority if, and only if, it is made in accordance with his official duty.

(2) For the purposes of this Act a disclosure by a government contractor is made with lawful authority if, and only if, it is made—

(a) in accordance with an official authorisation; or

(b) for the purposes of the functions by virtue of which he is a government contractor and without contravening an official restriction.

(3) For the purposes of this Act a disclosure made by any other person is made with lawful authority if, and only if, it is made—

(a) to a Crown servant for the purposes of his functions as such; or

(b) in accordance with an official authorisation.

(4) It is a defence for a person charged with an offence under any of the foregoing provisions of this Act to prove that at the time of the alleged offence he believed that he had lawful authority to make the disclosure in question and had no reasonable cause to believe otherwise.

(5) In this section "official authorisation" and "official restriction" mean, subject to subsection (6) below, an authorisation or restriction duly given or imposed by a Crown servant or government contractor or by or on behalf of a prescribed body or a body of a prescribed class.

(6) In relation to section 6 above "official authorisation" includes an authorisation duly given by or on behalf of the State or organisation concerned or, in the case of an organisation, a member of it.

Safeguarding of information.

8.—(1) Where a Crown servant or government contractor, by virtue of his position as such, has in his possession or under his control any document or other article which it would be an offence under any of the foregoing provisions of this Act for him to disclose without lawful authority he is guilty of an offence if—

(a) being a Crown servant, he retains the document or article contrary to his official duty; or

(b) being a government contractor, he fails to comply with an official direction for the return or disposal of the document or article, or if he fails to take such care to prevent the unauthorised disclosure of the document or article as a person in his position may reasonably be expected to take.

(2) It is a defence for a Crown servant charged with an offence under subsection (1)(a) above to prove that at the time of the alleged offence he believed that he was acting in accordance with his official duty and had no reasonable cause to believe otherwise.

(3) In subsections (1) and (2) above references to a Crown servant include any person, not being a Crown servant or government contractor, in whose case a notification for the purposes of section 1(1) above is in force.

(4) Where a person has in his possession or under his control any document or other article which it would be an offence under section 5 above for him to disclose without lawful authority, he is guilty of an offence if—

(a) he fails to comply with an official direction for its return or disposal; or

(b) where he obtained it from a Crown servant or government contractor on terms requiring it to be held in confidence or in circumstances in which that servant or contractor could reasonably expect that it would be so held, he fails to take such care to prevent its unauthorised disclosure as a person in his position may reasonably be expected to take.

(5) Where a person has in his possession or under his control any document or other article which it would be an offence under section 6 above for him to disclose without lawful authority, he is guilty of an offence if he fails to comply with an official direction for its return or disposal.

(6) A person is guilty of an offence if he discloses any official information, document or other article which can be used for the purpose of obtaining access to any information, document or other article protected against disclosure by the foregoing provisions of this Act and the circumstances in which it is disclosed are such that it would be reasonable to expect that it might be used for that purpose without authority.

(7) For the purposes of subsection (6) above a person discloses information or a document or article which is official if—

(a) he has or has had it in his possession by virtue of his position as a Crown servant or government contractor; or

(b) he knows or has reasonable cause to believe that a Crown servant or government contractor has or has had it in his possession by virtue of his position as such.

(8) Subsection (5) of section 5 above applies for the purposes of subsection (6) above as it applies for the purposes of that section.

(9) In this section "official direction" means a direction duly given by a Crown servant or government contractor or by or on behalf of a prescribed body or a body of a prescribed class.

Prosecutions.

9.—(1) Subject to subsection (2) below, no prosecution for an offence under this Act shall be instituted in England and Wales or in Northern Ireland except by or with the consent of the Attorney General or, as the case may be, the Attorney General for Northern Ireland.

(2) Subsection (1) above does not apply to an offence in respect of any such information, document or article as is mentioned in section 4(2) above but no prosecution for such an offence shall be instituted in England and Wales or in Northern Ireland except by or with the consent of the Director of Public Prosecutions or, as the case may be, the Director of Public Prosecutions for Northern Ireland.

Penalties.

10.—(1) A person guilty of an offence under any provision of this Act other than section 8(1), (4) or (5) shall be liable—

(a) on conviction on indictment, to imprisonment for a term not exceeding two years or a fine or both;

(b) on summary conviction, to imprisonment for a term not exceeding six months or a fine not exceeding the statutory maximum or both.

(2) A person guilty of an offence under section 8(1), (4) or (5) above shall be liable on summary conviction to imprisonment for a term not exceeding three months or a fine not exceeding level 5 on the standard scale or both.

Arrest, search and trial.

11.—(1) In section 24(2) of the [1984 c. 60.] Police and Criminal Evidence Act 1984 (arrestable offences) in paragraph (b) for the words "the Official Secrets Acts 1911 and 1920" there shall be substituted the words "the Official Secrets Act 1920" and after

that paragraph there shall be inserted— " (bb) offences under any provision of the Official Secrets Act 1989 except section 8(1), (4) or (5);"..

(2) Offences under any provision of this Act other than section 8(1), (4) or (5) and attempts to commit them shall be arrestable offences within the meaning of section 2 of the [1967 c. 18 (N.I.).] Criminal Law Act (Northern Ireland) 1967.

(3) Section 9(1) of the [1911 c. 28.] Official Secrets Act 1911 (search warrants) shall have effect as if references to offences under that Act included references to offences under any provision of this Act other than section 8(1), (4) or (5); and the following provisions of the Police and Criminal Evidence Act 1984, that is to say—

(a) section 9(2) (which excludes items subject to legal privilege and certain other material from powers of search conferred by previous enactments); and

(b) paragraph 3(b) of Schedule 1 (which prescribes access conditions for the special procedure laid down in that Schedule),

shall apply to section 9(1) of the said Act of 1911 as extended by this subsection as they apply to that section as originally enacted.

(4) Section 8(4) of the [1920 c. 75.] Official Secrets Act 1920 (exclusion of public from hearing on grounds of national safety) shall have effect as if references to offences under that Act included references to offences under any provision of this Act other than section 8(1), (4) or (5).

(5) Proceedings for an offence under this Act may be taken in any place in the United Kingdom.

"Crown servant" and "government contractor".

12.—(1) In this Act "Crown servant" means—

(a) a Minister of the Crown;

(b) a person appointed under section 8 of the [1973 c. 36.] Northern Ireland Constitution Act 1973 (the Northern Ireland Executive etc.);

(c) any person employed in the civil service of the Crown, including Her Majesty's Diplomatic Service, Her Majesty's Overseas Civil Service, the civil service of Northern Ireland and the Northern Ireland Court Service;

(d) any member of the naval, military or air forces of the Crown, including any person employed by an association established for the purposes of the [1980 c. 9.] Reserve Forces Act 1980;

(e) any constable and any other person employed or appointed in or for the purposes of any police force (including a police force within the meaning of the [1970 c. 9 (N.I.).] Police Act (Northern Ireland) 1970);

(f) any person who is a member or employee of a prescribed body or a body of a prescribed class and either is prescribed for the purposes of this paragraph or belongs to a prescribed class of members or employees of any such body;

(g) any person who is the holder of a prescribed office or who is an employee of such a holder and either is prescribed for the purposes of this paragraph or belongs to a prescribed class of such employees.

(2) In this Act "government contractor" means, subject to subsection (3) below, any person who is not a Crown servant but who provides, or is employed in the provision of, goods or services—

(a) for the purposes of any Minister or person mentioned in paragraph (a) or (b) of subsection (1) above, of any of the services, forces or bodies mentioned in that subsection or of the holder of any office prescribed under that subsection; or

(b) under an agreement or arrangement certified by the Secretary of State as being one to which the government of a State other than the United Kingdom or an international organisation is a party or which is subordinate to, or made for the purposes of implementing, any such agreement or arrangement.

(3) Where an employee or class of employees of any body, or of any holder of an office, is prescribed by an order made for the purposes of subsection (1) above—

(a) any employee of that body, or of the holder of that office, who is not prescribed or is not within the prescribed class; and

(b) any person who does not provide, or is not employed in the provision of, goods or services for the purposes of the performance of those functions of the body or the holder of the office in connection with which the employee or prescribed class of employees is engaged, shall not be a government contractor for the purposes of this Act.

Other interpretation provisions.

13.—(1) In this Act—

"disclose" and "disclosure", in relation to a document or other article, include parting with possession of it;

"international organisation" means, subject to subsections (2) and (3) below, an organisation of which only States are members and includes a reference to any organ of such an organisation;

"prescribed" means prescribed by an order made by the Secretary of State;

"State" includes the government of a State and any organ of its government and references to a State other than the United Kingdom include references to any territory outside the United Kingdom.

(2) In section 12(2)(b) above the reference to an international organisation includes a reference to any such organisation whether or not one of which only States are members and includes a commercial organisation.

(3) In determining for the purposes of subsection (1) above whether only States are members of an organisation, any member which is itself an organisation of which only States are members, or which is an organ of such an organisation, shall be treated as a State.

Orders.

14.—(1) Any power of the Secretary of State under this Act to make orders shall be exercisable by statutory instrument.

(2) No order shall be made by him for the purposes of section 7(5), 8(9) or 12 above unless a draft of it has been laid before, and approved by a resolution of, each House of Parliament.

(3) If, apart from the provisions of this subsection, the draft of an order under any of the provisions mentioned in subsection (2) above would be treated for the purposes of the Standing Orders of either House of Parliament as a hybrid instrument it shall proceed in that House as if it were not such an instrument.

Acts done abroad and extent.

15.—(1) Any act—

(a) done by a British citizen or Crown servant; or

(b) done by any person in any of the Channel Islands or the Isle of Man or any colony, shall, if it would be an offence by that person under any provision of this Act other than section 8(1), (4) or (5) when done by him in the United Kingdom, be an offence under that provision.

(2) This Act extends to Northern Ireland.

(3) Her Majesty may by Order in Council provide that any provision of this Act shall extend, with such exceptions, adaptations and modifications as may be specified in the Order, to any of the Channel Islands or the Isle of Man or any colony.

Short title, citation, consequential amendments, repeals, revocation and commencement.

16.—(1) This Act may be cited as the Official Secrets Act 1989.

(2) This Act and the Official Secrets Acts 1911 to 1939 may be cited together as the Official Secrets Acts 1911 to 1989.

(3) Schedule 1 to this Act shall have effect for making amendments consequential on the provisions of this Act.

(4) The enactments and Order mentioned in Schedule 2 to this Act are hereby repealed or revoked to the extent specified in the third column of that Schedule.

(5) Subject to any Order under subsection (3) of section 15 above the repeals in the Official Secrets Act 1911 and the Official Secrets Act 1920 do not extend to any of the territories mentioned in that subsection.

(6) This Act shall come into force on such day as the Secretary of State may by order appoint.

APPENDIX E

TABLE OF THE BRITISH OFFICIAL SECRETS ACT

SUB	TITLE	KEY PROVISIONS	NOTES
§ 1	Security & Intelligence Disclosures	(1) Members of the security or intelligence services are guilty of an offense "if without lawful authority he discloses any information, document or other article relating to security or intelligence" (2) Other Crown servants or contractors are guilty of an offense "if without lawful authority he makes a damaging disclosure …."	1. Defines damaging 2. Shifts burden to defendant to prove that he did not know, and had no reasonable cause to believe, that the disclosure would be damaging. 3. Effectively eliminates mens rea, creating strict liability.
§ 2	Defence Disclosures	"if without lawful authority he makes a damaging disclosure of any information, document or other article relating to defense" N.B.: Applies only to Crown servants and government contractors.	1. Defines damaging 2. Shifts burden to defendant to prove that he did not know, and had no reasonable cause to believe, that the disclosure would be damaging. 3. Effectively eliminates mens rea, creating strict liability.

SUB	TITLE	KEY PROVISIONS	NOTES
§ 3	International Relations Disclosures	Makes unlawful disclosures relating international relations or confidential information received from foreign states N.B.: Applies only to Crown servants and government contractors.	1. Defines damaging 2. Shifts burden to defendant to prove that he did not know, and had no reasonable cause to believe, that the disclosure would be damaging.
§ 4	Crime & Special Investigation Powers	Applies to disclosures that result in the commission of an offense, facilitates the escape of persons in legal custody or impedes the apprehension of criminal offenders. Applies also to warrants issued under the Interception of Communications Act or the Security Service Act. N.B.: Applies only to Crown servants and government contractors.	Shifts burden to defendant to prove that he did not know, and had no reasonable cause to believe, that the disclosure would be damaging.
§ 5	Information Resulting from Unauthorized Disclosures or Entrusted in Confidence	Applies to persons into who come into possession of information, documents or articles if "he discloses it without lawful authority knowing, or having reasonable cause to believe, that it is protected against disclosure by the foregoing provisions of this Act and that it has come into his possession" either having been disclosed without lawful authority or having been entrusted to him. N.B.: Applies to all persons, to include journalists who receive leaked information.	The person does not commit an offense unless the disclosure was damaging and "he makes it knowing, or having reasonable cause to believe, that it would be damaging"

SUB	TITLE	KEY PROVISIONS	NOTES
§ 6	International Organizations	This section applies to information, documents or articles relating to security, intelligence, defence or international relations and has been communicated to either another state or an international organization.	No offense is committed where the information, document or article is disclosed by lawful authority or has previously been made public.
§ 7	Authorized Disclosures	Defines lawful disclosures by Crown servants or government contractors. N.B.: It is not a crime to disclose information that has been officially published pursuant to this section.	
§ 8	Safeguarding of Information	(1) A Crown servant commits an offense if he retains a document or article contrary to official duty. (2) A contractor commits an offense he fails to comply with an official direction for return or disposal of a document or an article.	
§ 9	Prosecutions	Prosecutions require the consent of the Attorney General	

SUB	TITLE	KEY PROVISIONS	NOTES
§ 10	Penalties	(1) The penalty under Sub-section 8 is imprisonment not exceeding three months or a fine or both. (2) The penalty under all other sub-sections is not exceeding two years or a fine or both.	
§ 11	Arrest, Search & Trial	Amends existing police legislation. Provides that violations of this act arrestable offenses, allows for search warrants and permits exclusion of public from trial.	
§ 12	Definitions	Defines Crown servant and government contractor	Technical Provision
§ 13	Other Provisions	Provides other interpretation provisions for key language	Technical Provision
§ 14	Orders	Provides for orders by Secretary of State and Standing Orders of either House of Parliament	Technical Provision

SUB	TITLE	KEY PROVISIONS	NOTES
§ 15	Acts Done Abroad	Applies to acts done abroad by either British citizens or Crown servants. Makes it a crime for British citizens and Crown servants to disclose information abroad which would be illegal for them to do so in the United Kingdom.	
§ 16	Short Title & Citation	This act may be cited as the Official Secrets Act 1989.	Technical Provision

BIBLIOGRAPHY

A source, senior-level national official, who wishes to remain anonymous, 11 December 2006.

ACLU. "Government Backs Down in its Attempt to Seize "Secret" Document From ACLU," 18 December 2006. URL: http://www.aclu.org/safefree/general/27727prs20061218.html>. Accessed 30 December 2006.

Aftergood, Steven. "On Leaks of National Security Secrets: A Response to Michael Hurt." *National Security Studies Quarterly*, No. VIII (Winter 2002): 97-102.

Arnett v. Kennedy. 416 U.S. 134, 162, 94 S. Ct. 1633, 40 L. Ed.2d 15 (1974).

_____. U.S. Attorney General. "Report to Congress on Unauthorized Disclosures of Classified Information." Draft Report, 29 April 2002 (9:49 AM).

_____. U.S. Attorney General. Letter to the Director Central Intelligence. Subject: "Reply to Letter, 11 May 2002." 15 July 2002.

_____. U.S. Attorney General. "Report to Congress on Unauthorized Disclosures of Classified Information." 15 October 2002. URL: <http://www.fas.org/sgp/othergov/dojleaks.html>. Accessed 26 October 2005.

Associated Press. "Bill to create federal shield law introduced in House." *Associated Press,* online ed., 2 February 2005. URL: <http://64.233.161.104/search?q=cache:lZ-VVPp2YQAJ:www.firstamendmentcenter.org/news.aspx%3Fid%3D14782+%22bill+to+create+federal+shield+law+introduced+in+house%22&hl=en>. Accessed 19 January 2006.

_____. "CIA turncoat Harold Nicholson sentenced to 23 years in prison." *Associated Press,* online ed., 5 June 1997. URL: <http://www.jonathanpollard.org/1997/060597a.htm>. Accessed 16 September 2006.

_____. "Congress passes bill expanding penalties for classified leaks." *Associated Press,* online ed., 13 October 2000. URL: <http://www.freedomforum.org/templates/document.asp?documentID=3292>. Accessed 26 October 2005.

_____. "Senator Revives Classified Leaks Bill." *Associated Press,* online ed., 23 August 2001. URL: <http://www.freedomforum.org/templates/document.asp?documentID=14677>. Accessed 26 October 2005.

(b) (3), (b) (6) . "Legislative and Judicial Safeguards for US Intelligence Personnel." *Studies in Intelligence,* vol. 42 no. 2 (1998): 35-44.

BBC. "1994: CIA double agent jailed for life." *British Broadcasting Corporation*, online ed., 28 April 1994. URL: <http://news.bbc.co.uk/onthisday/hi/dates/stories/april/28/newsid_2501000/2501007.stm>. Accessed 16 September 2006.

Berry, David. "Theft and Misuse of Government Information." Journal of Public Inquiry (Fall/Winter 2003): 43-47. URL: <http://www.fas.org/sgp/eprint/jpi-theft.pdf>. Accessed 29 September 2006.

Branzburg v. Hayes. 408 U.S. 665, 92 S. Ct. 2646, 33 L. Ed. 2d 626 (1972).

Bruce, James B. "Laws and Leaks of Classified Intelligence: Costs and Consequences of Permissive Neglect." Meeting of the National Security Committee, American Bar Association Conference, 22 November 2002. Arlington, Virginia.

Intelligence and the National Security Strategist: Enduring Issues and Challenges. Ed. Roger Z. George. Washington, D.C.: National Defense University Press, 2004.

CBS News "Reporters Lose Appeal on CIA Leaks." *CBS News*, online ed., 15 February 2005. URL: <http://www.cbsnews.com/stories/2004/10/15/national/main649698.shtml>. Accessed 10 September 2006.

Chapman, Steve. "Have Leaks Crippled War on Terrorism?" *Chicago Tribune*, on line ed., 9 July 2006. URL: <http://www.chicagotribune.com/news/columnists/chi-0607090393jul09,1,1759071.column?coll=chi-navrailnews-nav>. Accessed 8 September 2006.

Charkes, Susan D. "The Constitutionality of the Intelligence Identities Protection Act." 83 *Columbia Law Review* 727 (1983).

CIA v. Sims. 471 U.S. 159, 105 S. Ct. 1881, 85 L. Ed. 2d 173 (1985).

Clinton, William J. "Statement by the President to the House of Representatives." 4 November 2000. URL: <http://64.233.161.104/search?q=cache:n_stZ_BT6U0J:www.fas.org/irp/news/2000/11/irp-001104-leak.htm+clinton,+%22statement+by+the+president+to+the+house%22&hl=en&gl=us&ct=clnk&cd=1>. Accessed 22 August 2006.

CNN. "Ex-FBI spy Hanssen sentenced to life, apologizes." *CNN*, online ed., 14 May 2002. URL: <http://archives.cnn.com/2002/LAW/05/10/hanssen.sentenced/index.html>. Accessed 16 September 2006.

_____. "News organizations ask Clinton to veto classified leaks bill." *CNN*, online ed., 2 November 2000. URL: <http://transcripts.cnn.com/2000/ALLPOLITICS/stories/11/02/classifiedleaks.ap/index.html>. Accessed 18 December 2006.

_____. "Sandy Berger fined $50,000 for taking documents." *CNN*, online ed., 8 September 2005. URL: <http://www.cnn.com/2005/POLITICS/09/08/berger.sentenced>. Accessed 16 September 2006.

Coalition of Journalists for Open Government. "Backgrounders." URL: <www.cjog.net/background.html>. Accessed 19 January 2006.

_____. "Protection of National Security Information: The Classified Information Protection Act of 2001." CRS Report for Congress. Washington, D.C.: Library of Congress, 16 January 2002.

Congressional Research Service. "Protection of National Security Information." CRS Report for Congress. Washington, D.C.: Library of Congress, 30 June 2006.

Connally v. General Construction Co. 269 U.S. 385, 46 S. Ct. 126, 70 L. Ed. 393 (1926).

"The Constitutionality of the Section 793 of the Espionage Act and its Application to Press Leaks." Note. 33 *Wayne L.Rev*. 205 (1986).

Dean, John W. "Bush's Unofficial Official Secrets Act." FindLaw. 26 September 2003. URL: <http://writ.corporate.findlaw.com/dean/20030926.html>. Accessed 29 August 2006.

Department of the Navy v. Egan. 484 U.S. 518, 108 S. Ct. 818, 98 L. Ed. 2d 918 (1988).

Department of Homeland Security. "Safeguarding Sensitive But Unclassified Information." MD 11042.1, January 5, 2005. URL: <http://www.fas.org/sgp/othergov/dhs-sbu-rev.pdf>. Accessed 22 October 2006.

Edgar, Harold. "The Espionage Statutes and Publication of Defense Information." 73 *Columbia Law R.* 5 (1973).

EPA v. Mink. 410 U.S. 73, 93 S. Ct. 827, 35 L. Ed. 2d 119 (1973).

Federation of American Scientists. "CIA Sued over Prepublication Review." URL: <http://www.fas.org/sgp/news/secrecy/2006/03/030706.html#1>. Accessed 22 October 2006.

Fisher, Louis. *In the Name of National Security: Unchecked Presidential Power and the Reynolds Case*. Lawrence, KS: University Press, 2006.

Gay, Oonagh. *Official Secrecy*. Online monograph. London: House of Commons Library, 2004. URL: <http://www.parliament.uk/commons/lib/research/notes/snpc-02023.pdf>. Accessed 11 January 2006.

Griffith, John. "The Official Secrets Act 1989." 16 *Journal of Law and Society* 2 (Autumn 1989).

Haig v. Agee. 453 U.S. 280, 101 S. Ct. 2766, 69 L. Ed. 2d 640 (1981).

Hedley, John Hollister. "Secrets, Free Speech, and Fig Leaves." *Studies in Intelligence,* unclassified edition (Spring 1998): 75-83.

Her Majesty's Stationary Office. Official Secrets Act 1989. URL: <http://www.opsi.gov.uk/acts/acts1989/Ukpga_19890006_en_2.htm>. Accessed 22 August 2006.

Herbert v. Lando. 441 U.S. 153, 99 S. Ct. 1635, 60 L. Ed. 2d 115 (1979).

Hersch, Seymour. "Why Pollard Should Never Be Released (The Traitor)." *The New Yorker,* online ed., 18 January 1999. URL: <http://www.freerepublic.com/focus/fr/576453/posts>. Accessed 16 September 2006.

Historical Society of the Courts of the State of New York. "The Trial of John Peter Zenger." URL: <http://www.courts.state.ny.us/history/Zenger.htm>. Accessed 14 December 2006.

Hoekstra, Pete. "Secrets and Leaks: The Costs and Consequences for National Security." The Heritage Foundation. 29 July 2005. URL: <http://www.heritage.org/Research/HomelandDefense/wm809.cfm>. Accessed 26 October 2005.

House Permanent Select Committee on Intelligence. "Report from the Permanent Select Committee on Intelligence." 109th Congress. Report to accompany H.R. 2475, Intelligence Authorization Act for Fiscal Year 2006, 2 June 2005.

Hurt, Michael. "Leaking National Security Secrets: Effects on Security and Measures to Mitigate." *National Security Studies Quarterly* 7, no. 4 (Autumn 2001): 1+.

Jameson, W. George. "Safeguarding National Security Information: Dealing with Unauthorized Disclosures of Classified Information." Meeting of the National Security Committee, American Bar Association Conference, 22 November 2002. Arlington, Virginia.

Jefferies, John Calvin. "Rethinking Prior Restraint." 92 *Yale L.J.* 409 (1983).

Johnston, David. "Pentagon Analyst Gets 12 Years for Disclosing Data." *New York Times*, online ed., 20 January 2006. URL: <http://www.nytimes.com/2006/01/20/politics/20cnd-franklin.html?ex=1295413200&en=3e46a585271c0505&ei=5088&partner=rssnyt&emc=rss>. Accessed 10 September 2006.

Kaplan, David E. "Pieces of the 9/11 Puzzle." *U.S. News & World Report*, online ed., 15 March 2004. URL: <http://www.keepmedia.com/pubs/USNewsWorldReport/2004/03/15/392037?from=search&criteria=yemen%2C+telephone&resultsPage=2&refinePubTypeID=0>. Accessed 17 November 2005.

Kent v. Dulles. 357 U.S. 116, 78 S. Ct. 1113, 2 L. Ed. 2d, 1204 (1958).

Landmark Communications v. Virginia. 435 U.S. 829, 98 S. Ct. 1535, 56 L. Ed.2d 1 (1978).

LaFave, Wayne R. and Jerold H. Israel. *Criminal Procedure*. St. Paul, MN: West Publishing Co., 1985.

Lewis, Neil A. "Lonetree, US Marine Convicted of Spying Appeals." *New York Times,* online ed., 13 May 1991. URL: http://www.jonathanpollard.org/1991/051391.htm. Accessed 16 September 2006.

Liberty Lobby, Inc. v. Pearson. 129 U.S. App. DC 74, 390 F.2d 489 (1968).

Library of Congress. "Laws and Regulations Governing the Protection of Sensitive But Unclassified Information." Washington, D.C.: Library of Congress, 2004. URL: <http://www.loc.gov/rr/frd/pdf-files/sbu.pdf>. Accessed 22 October 2006.

Liptak, Adam. "U.S. Subpoena Is Seen as Bid to Stop Leaks." *New York Times*, online ed., 14 December 2006. URL: <http://www.nytimes.com/2006/12/14/washington/14leak.html?_r=1&oref=slogin>. Accessed 15 December 2006.

Loeb, Vernon "Anti-Leak Veto Catches Sponsors Off Guard." *Washington Post*. 13 November 2000. URL: <http://www.fas.org/irp/news/2000/11/irp-001113-leak.htm>. Accessed 11 November 2006.

Martin, Kate. "The Pending "Leak" Statute is Unconstitutional." Federation of American Scientists, URL: <http://www.fas.org/sgp/news/2000/09/leaks.html>. Accessed 15 December 2006.

McDonald, R. Robin. "DEA Employee Gets Prison Term for Leaking to Reporter." Law.Com. 15 January 2003. URL: <http://www.law.com/jsp/article.jsp?id=1042568651135>. Accessed 29 August 2006.

Murphy, Kirsten and others. "The War on Terrorism: Balancing National Security and Civil Liberties." *Silha Bulletin* 8, No. 2 (Winter 2003). *Silha Center, University of Minnesota.* URL: <http://www.silha.umn.edu/winter2003.htm>. Accessed 7 September 2006.

National Security Law. Ed. John Norton Moore. Durham: Carolina Academic Press, 2005.

Near v. Minnesota. 283 U.S. 697 51 S. Ct. 625, 75 L. Ed. 1357 (1931).

Nelson, Jack. "U.S. Government Secrecy and the Current Crackdown on Leaks." Working Paper Series. *The Joan Shorenstein Center on the Press, Politics and Public Policy.* Boston, MA: Harvard College, 2002.

New York Times Co. v. United States. 403 U.S. 713, 91 S. Ct. 2140, 29 L. Ed. 2d 822 (1971).

Nimmer, Melville E. "National Security Secrets v. Free Speech: The Issues Left Undecided in the Ellsberg Case." 26 *Stanford Law Review* 311 (1974).

_____. *Nimmer on Freedom of Speech: A Treatise on the Theory of the First Amendment.* New York: Matthew Bender, 1984.

Olive, Ronald J. *Capturing Jonathan Pollard.* Annapolis, MD: Naval Institute Press, 2006.

"Plugging the Leak: The Case for a Legislative Resolution of the Conflict Between the Demands of Secrecy and the Need for an Open Government." Note. 71 *Virginia Law Review* 5 (June 1985): 801-868.

"Prior Restraint and the Press Following the *Pentagon Papers* Cases - Is the Immunity Dissolving?" Note. 47 *Notre Dame Law* 927 (1972).

Reporters Committee for Freedom of the Press. "Miller jailed for refusing to reveal source, Cooper to testify." *News Media Update,* online ed., 6 July 2005. URL: <http://www.rcfp.org/news/2005/0706-con-miller.html>. Accessed 16 September 2006.

Richelson, Jeffery T. *The U.S. Intelligence Community*. Boulder, CO: Westview Press, 1999.

Sable Communications of California v. Federal Communications Commission, 492 U.S. 115, 109 S. Ct. 2829, 106 L. Ed. 2d 93 (1989).

Scarbeck v. United States. 317 F.2d 546 (D.C. Cir. 1963), *cert. denied*, 83 S.Ct. 1897 (1963).

Shane, Scott and Mark Mazzetti. "Moves Signal Tighter Secrecy within C.I.A." *New York Times,* online ed., 24 April 2006. URL: <http://64.233.161.104/search?q=cache:iMX3NAcvnRoJ:www.thepowerhour.com/news2/secrecy_cia.htm+%22moves+signal+tighter+secrecy+within+C.I.A.%22&hl=en&gl=us&ct=clnk&cd=4>. Accessed 1 November 2006.

Shelby, Richard C. "September 11 and the Imperative of Reform in the U.S. Intelligence Community: Additional Views of Senator Richard C. Shelby." 10 December 2002. URL: <http://intelligence.senate.gov/shelby.pdf>. Accessed 26 October 2005.

Silberman, Lawrence H. *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*. Report to the President of the United States. Washington, DC: U.S. Government Printing Office, 31 March 2005.

Smith, R. Jeffery. "Fired Officer Believed CIA Lied to Congress." *Washington Post,* online ed., 14 May 2006. URL: <http://www.washingtonpost.com/wp-dyn/content/article/2006/05/13/AR2006051301311.html>. Accessed 16 September 2006.

Snepp v. United States. 444 U.S. 507, 100 S. Ct. 763, 62 L. Ed 2d 704 (1980).

Stehny v. Perry. 101 F.3d 925 (3d Cir. 1996).

Stephens, Hampton. "Supreme Court Filing Claims Air Force, Government Fraud in 1953 Case." URL: <http://www.fas.org/sgp/news/2003/03/iaf031403.html>. Accessed 16 November 2006.

Tenet, George J. Director Central Intelligence. Letter to U.S. Attorney General. Subject: "Draft Report of the Attorney General to the U.S. Congress." 11 May 2002.

"The Void-for-Vagueness Doctrine in the Supreme Court." Note. 109 *U.Pa.L.Rev*. 67 (1960).

Thomas, Rosamund M. *Espionage and Secrecy: The Official Secrets Acts 1911-1989 of the United Kingdom.* London: Routledge, 1991.

Topol, David. "*United States v. Morison*: A Threat to the First Amendment Right to Publish National Security Information." 43 S.C. L. Rev. 581.

Touby v. United States. 500 U.S. 160, 111 S. Ct. 1752, 114 L. Ed. 219 (1990).

Tribe, Laurence H. *American Constitutional Law*. 2d ed. Mineola, NY: The Foundation Press, 1988.

Turner, Robert F. "Congress Can't Keep a Secret." *Washington Post*, 12 October 2001.

Uniform Code of Military Justice. URL: <http://www.au.af.mil/au/awc/awcgate/ucmj2.htm>. Accessed 8 November 2006.

U.S. Constitution.

U.S. Senate. *Congressional Record: August 2, 2006 (Senate).* Page S8612-S8614. URL: <http://www.fas.org/irp/congress/2006_cr/s3774.html>. Accessed 9 November 2006.

_____. "Report of the Commission on Protecting and Reducing Government Secrecy," Senate Document 105-2. Washington, D.C.: Government Printing Office, 1997. URL: <http://www.fas.org/sgp/library/moynihan/index.html>. Accessed 14 December 2006.

U.S. v. Balint. 258 U.S. 250, 42 S. Ct. 301, 66 L. Ed. 604 (1922).

U.S. v. Boyce. 594 F.2d 1246 (9th Cir.), *cert. denied*, 444 U.S. 855 (1979).

U.S. v. Franklin. Criminal Indictment, E.D.V.A., Crim. No. 1:05CR225, 4 August 2005. URL: <http://www.globalsecurity.org/intell/library/reports/2005/franklin_indictment_04aug2005.htm>. Accessed 5 September 2006.

U.S. v. Gorin. 312 U.S. 19, 61 S. Ct. 429, 85 L. Ed. 2d 488 (1941).

U.S. v. Heine. 151 F.2d 813, *cert. denied*, 328 U.S. 833 (1946).

U.S. v. Hung. 629 F.2d 908 (4th Cir. 1980), *cert. denied*, 454 U.S. 1144 (1982).

U.S. v. Marchetti. 466 F.2d 1309 (4th Cir. 1972), *cert. denied,* 409 U.S. 1063, 93 S. Ct. 553, 34 L. Ed. 2d 516 (1972).

U.S. v. Morison. 844 F.2d 1057 (4th Cir. 1988), *cert. denied,* 488 U.S. 908, 109 S. Ct. 259, 102 L. Ed. 2d 247 (1988).

U.S. v. Reynolds. 345 U.S. 1, 7 S. Ct. 582, 97 L. Ed. 727 (1953).

U.S. v. Russo. No. 9373 – (WMB) – (1) filed Dec. 29, 1971, *dismissed* (C.D. Cal. May 11, 1973).

U.S. v. Smith. Criminal Indictment. C.D.CA. June 2002 Grand Jury. URL: <http://news.lp.findlaw.com/hdocs/docs/fbi/ussmith50703ind.pdf#search=%22james%20j.%20smith%22>. Accessed 16 September 2006.

U.S. v. Smith. Plea Bargain. C.D.CA. Criminal No. CR 03-429(A)-FMC. URL: <http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/fbi/ussmith51204plea.pdf> . Accessed 16 September 2006.

U. S. v. The Progressive, Inc. 467 F. Supp. 990 (W.D. Wis. 1979).

U.S. v. Tobias. 836 F.2d 449 (9th Cir. 1988).

U.S. v. Wen Ho Lee. Criminal Indictment, D.N.M., Crim. No. 99-1417, 10 December 1999. URL: <http://www.fas.org/irp/ops/ci/docs/lee_indict.html>. Accessed 16 September 2006.

U.S. Congress. "Intelligence Authorization Act for Fiscal Year 2002," Public Law 107-108, 28 December 2001.

U.S. President. Executive Order 10450. "Security Requirements for Government Employment." 27 April 1953. URL: <http://www.archives.gov/federal-register/codification/executive-order/10450.html>. Accessed 24 October 2006.

_____. Executive Order 12333. "United States Intelligence Activities." 4 December 1981. URL: <http://www.cia.gov/cia/information/eo12333.html>. Accessed 29 October 2005.

_____. Executive Order 12958. "Classified National Security Information." 17 April 1995. URL: <http://www.dss.mil/seclib/eo12958.htm>. Accessed 29 October 2005.

_____. President, Executive Order 12968. "Access to Classified Information." 4 August 1995. URL: <http://www.fas.org/sgp/clinton/eo12968.html>. Accessed 29 October 2005.

_____. President, Executive Order 13356. "Strengthening the Sharing of Terrorist Information to Protect Americans." 27 August 2004. URL: <http://www.fas.org/irp/offdocs/eo/eo-13356.htm>. Accessed 29 October 2005.

5 U.S.C. § 1221 (1989).

5 U.S.C. § 7513 (2000).

5 U.S.C. § 7532 (1966).

5 U.S.C. § 8312 (2001).

10 U.S.C. § 986 (2000).

18 U.S.C. App. 3, §§ 1-18 (2006).

18 U.S.C. § 641 (2000).

18 U.S.C. §§ 793-794, 797, 798, 952 (1982).

18 U.S.C. § 1924 (2002).

18 U.S.C. § 2071 (1990).

35 U.S.C. § 181 (1999).

42 U.S.C. §§ 2274-2277 (2000).

50 U.S.C. § 403 (2000).

50 U.S.C. § 421 (1982).

50 U.S.C. § 435 (2000).

50 U.S.C. § 783 (2000).

Waters v. CIA. Civil Action No. 06-383 (D.D.C.) (RBW). URL: <http://www.fas.org/sgp/jud/waters030306.pdf>. Accessed 22 October 2006.

Waters, Thomas J. *Class 11: Inside the CIA's First Post-9/11 Spy Class.* New York: Penguin Group, 2006.

Weaver, William G. and Robert M. Pallito. "State Secrets and Executive Power." *Political Science Quarterly* 120, no. 1 (2005): 85-112.

Winchester, Karen A. and James W. Zirkle. "Freedom of Information and the CIA Information Act." 21 *Univ. Rich. Law Review* 231 (1987).

Wright, Peter. *Spycatcher*. New York: Viking Penguin, 1987.

Xanders, Edward L. "A Handyman's Guide to Fixing National Security Leaks: An Analytical Framework for Evaluating Proposals to Curb Unauthorized Publication of Classified Information." *Journal of Law and Politics* (Summer 1989). URL: <http://www.law.ufl.edu/faculty/publications/pdf/fenster_transparency.pdf>. Accessed 12 January 2006.

Youngstown Sheet & Tube Co. v. Sawyer. 343 U.S. 579, 72 S. Ct. 863, 96 L. Ed. 1153 (1952).

Zemel v. Rusk. 381 U.S. 1, 85 S. Ct. 1271, 14 L. Ed. 2d 179 (1965).

Zurcher v. Stanford Daily. 436 U.S. 547, 98 S. Ct. 1970, 56 L. Ed. 2d 525 (1978).