2004

Information Control in Times of Crisis: The Tools of Repression (symposium, Privacy and Surveillance)

Christina E. Wells
University of Missouri School of Law, wellsc@missouri.edu

Information Control in Times of Crisis: The Tools of Repression

CHRISTINA E. WELLS*

During the twentieth century the United States faced numerous threats to national security—*e.g.*, World War I, the Red Scare, World War II, the Cold War, and the Vietnam War.[1] When responding to these crises, the government took several steps to control information. Thus, the government tried to (1) muster public support for its national security agenda via public information campaigns, (2) safeguard critical information, or (3) gather information regarding potential spies or other enemies. Such steps were obviously legitimate in the abstract. One can hardly question the government's right to protect itself and its citizens. The actual application of information control, however, has been more questionable.

While there are examples of reasonable and legitimate government actions, many government attempts to control information during national security crises resulted in substantial and lasting abuses of civil liberties. For example, government attempts to control public information have resulted in unreasonable punishment of political speech or stigmatization of individuals. Government attempts to control access to information have been used to hide government wrongdoing rather than protect national security. Finally, government attempts to gather information have devolved into egregious invasions of privacy.

This article identifies several tools of information control that occur consistently throughout history. The government does not use all of these tools in every national security crisis. Nor does it always abuse them. However, the patterns that emerge suggest a certain predictability to (1) the government's actions during national security crises, and (2) the potentially negative consequences flowing from them that warrants our attention.

Understanding this historical pattern of government action allows one to identify and potentially prevent future problems. This is especially important in the post-9/11 world in which the government has asked for and received

---

* Enoch N. Crowder Professor of Law, University of Missouri-Columbia School of Law. I am indebted to Michael Held, who provided valuable and enthusiastic research support for this article and whose tireless and unflagging support made it better than it would have been. I also am grateful to Billie Wells whose interest in politics and current events provided much valuable material and inspiration.

1. Although the United States has experienced other crises, this article examines prominent twentieth century crises because commentators generally agree that World War I introduced the modern era with respect to national security issues and because these incidents involved the most substantial judicial, congressional, and public discussion regarding the appropriate role of government control of information. *See, e.g., Report of the Commission on Protecting and Reducing Government Secrecy*, S. DOC. NO. 105-2, 103rd Cong., A1, A7 (1997) [hereinafter *Secrecy Report*]; Jules Lobel, *Emergency Power and the Decline of Liberalism*, 98 YALE L.J. 1385, 1398-99 (1989).

controversial powers with respect to information control. The current administration's actions are eerily similar to past government actions, suggesting that we should pay close attention to the government's use of specific tools.

Section I of this article identifies an historical pattern of information control during times of crisis. Government efforts at such control generally fall into one of three categories—(1) attempts to control confidential information, (2) attempts to control public information, and (3) attempts to gather information. Although many government attempts to control information ostensibly have claims to legitimacy, government actions in these areas have resulted in some of the most egregious and lasting abuses in this country's history. Section II discusses the current administration's expanded powers with respect to information control and reveals a striking similarity between the government's current powers and those used in past crises. Finally, this article offers some thoughts regarding the parallels between past and present government action.

I. HISTORICAL PATTERNS OF INFORMATION CONTROL

A. Government Control of Confidential Information

In national security crises, governments often initially resort to enhanced secrecy with respect to national security information. This secrecy manifests itself in several ways—the increased classification of information (*i.e.*, the determination that information in certain categories should not be divulged for national security reasons), increased assertions of executive privilege, and increased secrecy with respect to government operations generally. This paper focuses on the classification of information as that issue pertains most specifically to national security and because the classification system's evolution parallels increased government secrecy generally. This section will also occasionally discuss other issues regarding government secrecy when relevant.

Most observers consider classification of information necessary to the survival of the nation:

> [A] government must sometimes stringently control certain information that (1) gives the nation a significant advantage over adversaries or (2) prevents adversaries from having an advantage that could significantly damage the nation. Governments protect that special information by classifying it; that is, by giving it a special designation, such as "Secret," and then restricting access to it . . . .
>
> . . . In wartime, when a nation's survival is at stake, the reasons for secrecy are most apparent, the secrecy restrictions imposed by the

> government are most widespread, and acceptance of those restrictions by the citizens is broadest.[2]

Typically, such classification involves information necessary to national defense, such as information pertaining to military operations, weapons technology, diplomatic negotiations, intelligence activities, etc.[3] Viewed in this light, classification of such information is relatively uncontroversial.[4] Nevertheless, the historical pattern of government actions suggests that, while a tilt toward secrecy is understandable, government expansion of the scope of classified information and attempts to restrict dissemination in peacetime have led to abuse.

During World War I, several laws restricted public dissemination of certain information.[5] The Espionage Act of 1917, the primary purpose of which was to punish spies, enhanced existing criminal punishments for the unlawful dissemination of information pertaining to national defense or military secrets.[6] Similarly, the Trading With the Enemy Act, the first statute to grant presidential authority to designate information as secret, allowed the President to control the dissemination of certain patents considered to be "detrimental to the public safety or defense, or [which] may assist the enemy or endanger the successful prosecution of the war . . . ."[7] In addition to legislative restrictions, the American Expeditionary Forces in France also established the first document classification system, requiring that military

---

2. Arvin S. Quist, Security Classifications of Information, Volume 1, Introduction to Classification 1 (2002), *available at* http://www.fas.org/sgp/library/quist/index.html (last visited Aug. 11, 2004) [hereinafter Quist, Chapter 1]. *See also* United States v. Reynolds, 345 U.S. 1, 10 (1953) ("In the instant case we cannot escape judicial notice that this is a time of vigorous preparation for national defense . . . these electronic devices must be kept secret if their full military advantage is to be exploited in the national interests."); United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 319-230 (1936) ("Secrecy in respect of information gathered . . . may be highly necessary, and the premature disclosure of it productive of harmful results.").

3. Quist, Chapter 1, *supra* note 2, at 2.

4. I use the term "relatively" to acknowledge that while many people assume that the government must maintain some secrets, some believe all such secrecy is an anathema to democratic government. *See, e.g.*, ARTHUR M. SCHLESINGER, JR., THE IMPERIAL PRESIDENCY 362-63 (1973) (discussing beliefs of Edward Teller, who was involved in developing the hydrogen bomb, that government secrecy regarding scientific and technical information should be abolished).

5. For historical accounts of government actions pertaining to secrecy prior to World War I, see Harold C. Relyea, *The Presidency and the People's Right to Know*, *in* THE PRESIDENCY AND INFORMATION POLICY 1, 9-12 (Harold Relyea et al., eds. 1981); Arvin S. Quist, Security Classifications of Information, Volume 1, Classification in the United States Prior to World War II 2-17 (2002), *available at* http://www.fas.org/sgp/library/quist/index.html (last visited Aug. 11, 2004) [hereinafter, Quist, Chapter 2].

6. Act of June 15, 1917, ch. 30, tit. I, § 3, 40 Stat. 219. Although there already existed penalties for espionage, the Espionage Act significantly increased them, including imposition of the death penalty in time of war. Quist, Chapter 2, *supra* note 5, at 22.

7. Act of October 6, 1917, ch. 106, § 10(i), 40 Stat. 422; *see also* Relyea, *supra* note 5, at 14.

information be classified as "Secret," "Confidential," or "For Official Circulation Only."[8]

Because it was narrowly confined, government secrecy during World War I was largely uncontroversial. Legislative enactments and administrative regulations concerned themselves with punishment of spies or military officials deliberately leaking military or defense information to the enemy.[9] Furthermore, Congress explicitly refused to give the President complete authority regarding the designation of information subject to prosecution, noting that to do so would raise a danger of presidential manipulation of public opinion.[10] The Wilson administration tried to regulate dissemination of confidential information in other ways—*e.g.*, regulations regarding publication by the press and public--but such regulations were voluntary and not subject to significant penalties.[11]

President Roosevelt also acted to protect confidential information during World War II. In 1940, pursuant to an existing statute protecting "vital military and naval installations and equipment,"[12] he issued Executive Order No. 8381, the first to authorize government officials to classify documents for national security reasons.[13] In 1942, pursuant to the First War Powers Act, Roosevelt also issued Executive Order 9182, which gave the Office of War Information the power to classify national security information.[14] Pursuant to that order, the Office of War Information issued government-wide regulations providing definitions of "Secret," "Confidential," and "Restricted" information, designated authority to classify and guidelines for classification, and warned against over-classification of information.[15] Although the govern

---

8. Relyea, *supra* note 5, at 12; Quist, Chapter 2, *supra* note 5, at 17-22.

9. SCHLESINGER, *supra* note 4, at 338; Harold Edgar & Benno C. Schmidt, Jr., *Curtiss-Wright Comes Home: Executive Power and National Security Secrecy*, 21 HARV. C.R.-C.L. L. REV. 349, 394-95 (1986).

10. Edgar & Schmidt, *supra* note 9, at 394-95. This refusal meant that the military classification system was merely evidence that information pertained to national defense but was not determinative of that issue.

11. JAMES RUSSELL WIGGINS, FREEDOM OR SECRECY 95-96 (1956). One regulation, for example, requested that the press refrain from publishing "'information, reports, or rumors, attributing a policy to the government in any international situation, not authorized by the President or a member of the cabinet'" without consultation with the Department of State. *Id.* at 95.

12. Act of Jan. 12, 1938, ch. 2, § 1, 52 Stat. 3. Although Congress never likely intended the term "equipment" to apply to documents, Roosevelt wanted to invoke statutory authorization for his order rather than ground it in inherent executive authority. SCHLESINGER, *supra* note 4, at 339; Relyea, *supra* note 5, at 18.

13. Exec. Order No. 8,381, 3 C.F.R. 634 (1938-1943).

14. Exec. Order No. 9,182, 7 Fed. Reg. 4468 (June 16, 1942).

15. Williams S. Moorhead, *Operation and Reform of the Classification System in the United States*, *in* SECRECY AND FOREIGN POLICY 87, 94 (Thomas M. Franck & Edward Weisband eds. 1974); Arvin S. Quist, Security Classifications of Information, Volume 1, Classification Under Executive Orders, 4-7

ment's classification authority during World War II was considerably broader and more organized than in World War I, it still exercised that authority only to "safeguard[] . . . military secrets, rarely extending [it] to either secrets affecting related non-military agencies or those involving foreign policy or diplomatic relations."[16]

As in World War I, officials during World War II also enlisted the press regarding the dissemination of classified information. Created in 1941, The Office of Censorship identified information potentially helpful to the enemy that the press was to refrain from publishing until it consulted with the Office.[17] This system was also voluntary although the press apparently complied with it.[18] In large part, such compliance was due to the government's limited application of censorship. As one commentator noted, "[t]he Office scrupulously sought to limit censorship to matters involving a definite military risk and to avoid suppressing information merely because it was embarrassing to the Government."[19]

With the end of World War II, executive attempts to maintain confidentiality of classified information expanded dramatically and became increasingly controversial. Much of this came about with the advent of nuclear weapons and the United States' changing position in world politics. As the United States entered the Cold War in its new role as a dominant super power, government officials expansively viewed threats to national security. Every threat to American interests at home or abroad, especially those posed by Communism and potential nuclear warfare, was perceived as a potential national security crisis, which required increasingly dramatic action by the executive branch.[20] Such action included increased classification of information.

(2002), *available at* http://www.fas.org/sgp/library/quist/index.html (last visited Aug. 11, 2004) [hereinafter, Quist, Chapter 3].

16. Moorhead, *supra* note 15, at 94; *see also* Quist, Chapter 3, *supra* note 15, at 2-3.

17. *Developments in the Law—The National Security Interest and Civil Liberties*, 85 HARV. L. REV. 1130, 1194 (1972) [hereinafter *Developments—National Security*].

18. WIGGINS, *supra* note 11, at 95-99.

19. *Developments—National Security*, *supra* note 17, at 1194.

20. Lobel, *supra* note 1, at 1400; Thomas S. Blanton, *National Security and Open Government in the United States*, *in* NATIONAL SECURITY AND OPEN GOVERNMENT: STRIKING THE RIGHT BALANCE 40-41 (2003), *available at* http://www.maxwell.syr.edu/campbell/opengov/NSOG.pdf (last visited June 8, 2004). As Arthur Schlesinger noted,

> [t]he new American approach to world affairs, nurtured in the sense of omnipresent crisis, set new political objectives, developed new military capabilities, devised new diplomatic techniques, invented new instruments of foreign operations and instituted a new hierarchy of values. Every one of these innovations encouraged the displacement of power, both practical and constitutional, from an increasingly acquiescent Congress into an increasingly imperial Presidency.

SCHLESINGER, *supra* note 4, at 164.

In 1947, Congress passed the Atomic Energy Act allowing an executive commission to control the dissemination of "restricted data" relevant to atomic energy.[21] A year later it enacted the National Security Act, which unified the government's defense structure and explicitly imbued the director of the CIA with responsibility for safeguarding intelligence.[22] Even these congressional enactments, however, left a great deal of discretion regarding classification of information to executive officials.[23]

In 1951, Truman signed Executive Order 10,290, which vastly expanded the government's ability to classify information. Truman's order broadened the categories of classification and extended the classification system beyond military officials, allowing any civilian agency to classify information "necessary . . . to protect the security of the United States."[24] Truman's order was not limited to information pertaining to "national defense" during wartime but allowed classification of military and non-military information if necessary to protect "national security," a move essentially allowing the government to establish a peacetime classification system based upon an undefined and elastic concept.[25] Finally, unlike Roosevelt, Truman grounded authority for the executive order in inherent executive power rather than statutory authorization, thus cementing executive control over classified information.[26]

Executive Order 10,290 was highly criticized. With only vague guidelines regarding classification and the meaning of "national security," and no provision for review of classification decisions, critics argued that the order would inevitably lead to a massive increase in information classification.[27] When President Eisenhower took office in 1953, he responded to such concerns with a new executive order narrowing classification guidelines, including allowing classification of information relevant to "national defense" rather than "national security," withdrawing classification authority from various civilian agencies, and providing for executive branch review of classification decisions.[28]

Eisenhower's new order was not without problems. Eisenhower also relied on inherent executive authority for the order as opposed to statutory

---

21. Atomic Energy Act of 1946, ch. 724, §10, 60 Stat. 766. For a history of the Act and the events leading up to it, see Arvin S. Quist, Security Classifications of Information, Volume 1, Classification Under the Atomic Energy Act, 1-8 (2002), *available at* http://www.fas.org/sgp/library/quist/index.html (last visited Aug. 11, 2004) [hereinafter, Quist, Chapter 4].

22. Relyea, *supra* note 5, at 19 n.40.

23. *Id.* at 19.

24. Exec. Order No. 10,290, Part I, § 1(a), 3 C.F.R. 790 (1949-53).

25. Quist, Chapter 3, *supra* note 15, at 9.

26. SCHLESINGER, *supra* note 4, at 340; Relyea, *supra* note 5, at 20.

27. *Developments—National Security*, *supra* note 17, at 1196; Moorhead, *supra* note 15, at 94.

28. Exec. Order No. 10,501, 3 C.F.R. 979 (1949-53).

authorization.[29] The order also provided no guidance with respect to declassification of information.[30] Furthermore, the classification scheme remained problematic in practice. Several executive and congressional commissions during the 1950s found that over-classification of information was a significant problem. One commission found, for example, that the power to classify had expanded to "some 1.5 million employees" and that overuse of the label "confidential" had begun to interfere with the free flow of scientific and technical information.[31] Others concluded that Pentagon officials were overly cautious, tended to overclassify, and failed to declassify information that no longer required secrecy.[32] Despite their uniform conclusions regarding abuse, the committees' calls for reform of the classification system went largely ignored.

Classification of information continued to be a problem throughout the 1950s and 1960s. By 1971, several government officials acknowledged that over-classification was a substantial problem, with some estimating that 90 to 99.5 percent of information was inappropriately classified.[33] Furthermore, classification guidelines had broadened to include designations such as "above Top Secret," a designation that was itself classified and over which there was little, if any, control.[34] Despite President Kennedy's executive order providing a mechanism for declassification of information,[35] executive officials proved reluctant to do so, and interpreted Kennedy's order as inapplicable to them.[36]

In addition, the government's desire for secrecy spread to non-classified information. The Office of Strategic Information, established in 1953, "work[ed] with the business community 'in voluntary efforts to prevent unclassified strategic data from being made available to those foreign nations which might use such data in a manner harmful to the defense interests of the United States.'"[37] The Defense Department similarly encouraged private con-

29. Relyea, *supra* note 5, at 21.

30. *Id.*

31. Moorhead, *supra* note 15, at 96.

32. *Id.* at 95-97; SCHLESINGER, *supra* note 4, at 341-42.

33. One official estimated that fully 99.5 percent of classified information within the Defense Department (estimated to encompass twenty million documents) could be declassified without prejudicing national security. *Developments—National Security*, *supra* note 17, at 1201. Another testified that 75 percent of that information "should never have been classified in the first place; another 15 percent quickly outlived the need for secrecy; and only about 10 percent genuinely required restricted access over any significant period of time." Moorhead, *supra* note 15, at 100. According to such officials, classified items included newspaper clippings and other clippings in the public domain, as well as memos from government officials complaining about overclassification. SCHLESINGER, *supra* note 4, at 344.

34. SCHLESINGER, *supra* note 4, at 344.

35. Exec. Order No. 10,964, 26 Fed. Reg. 8932 (Sept. 22, 1961).

36. SCHLESINGER, *supra* note 4, at 343.

37. WIGGINS, *supra* note 11, at 102-03.

tractors to avoid disclosing unclassified information that was "of possible use" to enemies of the United States.[38] Even President Kennedy, one of the few presidents inclined to openness after World War II, requested newspapers to refrain from publishing any information that was not "in the interest of national security."[39] These attempts at "voluntary" censorship were far broader than any government actions in World Wars I and II and engendered much protest by the press and organizations subject to the regulations.

During the 1960s and early 1970s, controversy erupted regarding several previously-secret incidents—the Kennedy administration's Bay of Pigs debacle, the government's secrecy with respect to its operations in Vietnam (which ultimately led to an expansion of the United States' role therein), the government's non-neutral stance about the India-Pakistan War, and the publication of the Pentagon Papers—prompting more thorough investigation of government secrecy.[40] In response to these investigations, Nixon signed a new executive order regarding classified information.[41]

Although Nixon claimed to be restricting the government's ability to classify information,[42] critics assailed Executive Order 11,652, noting that it broadened classification authority to matters "in the interest of national defense or foreign policy," essentially returning to the elastic notion of "national security" used in Truman's order.[43] They further charged that the order permitted executive officials to delay release of information in their own self-interest and "totally miscontrue[d] the basic meaning of the Freedom of Information Act,"[44] which had been enacted in 1967 to enhance public access to government records.[45]

---

38. *Id.* at 110.

39. *Developments—National Security*, *supra* note 17, at 1197. In a public speech to newspaper publishers, Kennedy noted that

> "[o]ur way of life is under attack. . . . If the press is awaiting a declaration of war before it imposes the self-discipline of combat conditions, then I can only say that no war ever posed a greater threat to our security. . . .
>
> The facts of the matter are that this nation's foes have openly boasted of acquiring through our newspapers information they would otherwise hire agents to acquire through theft, bribery, or espionage . . . ."

Id. (quoting President John F. Kennedy, Address to American Newspaper Publishers Ass'n (Apr. 27, 1961)).

40. Moorhead, *supra* note 15, at 89; Relyea, *supra* note 5, at 22.

41. Exec. Order No. 11,652, 37 Fed Reg. 5,209 (Mar. 10,1972).

42. Moorhead, *supra* note 15, at 102.

43. Relyea, *supra* note 5, at 24.

44. *Executive Classification of Information—Security Classification Problems Involving Exemption (b)(1) of the Freedom of Information Act*, H.R. REP. NO. 93-221, 93rd Cong. 58-59 (1973).

45. 5 U.S.C. § 552(b)(1)-(9) (2001). For a history on FOIA, see generally HERBERT N. FOERSTEL, FREEDOM OF INFORMATION AND THE RIGHT TO KNOW: THE ORIGINS AND APPLICATIONS OF THE FREEDOM OF INFORMATION ACT (1999).

The Nixon administration also used criminal penalties to protect government secrecy. Most famously, the Nixon administration brought Espionage Act prosecutions against Daniel Ellsberg, the former government official who leaked the Pentagon Papers to the *New York Times* and *Washington Post*. Prior to the Ellsberg trial, the government had never pursued criminal prosecution against a government official for leaking classified information as a matter of public interest, instead leaving such discipline to the administrative process.[46] Critics of the administration's actions noted that officials regularly leaked information to the press as a way of keeping the public informed and for their own advocacy purposes.[47] Others argued that the espionage laws did not allow prosecution for leaking information absent a malicious intent toward the security interests of the United States,[48] which Ellsberg did not have.[49] In order to punish Ellsberg, however, the Nixon administration pursued criminal penalties, and might have done so successfully had the case against Ellsberg not been dismissed due to the government's misconduct.[50]

In response to the Nixon administration's actions, Congress attempted some reform regarding government secrecy in the 1970s. Believing that the Nixon order gave far too much unchecked classification power to the executive branch, Congress amended FOIA to give courts the power to review *in camera* the propriety of government classification designations.[51] Congressional panels also recommended that Congress enact legislation establishing classification guidelines in order to protect national security while ensuring that government did not abuse the secrecy process.[52] No such legislation materialized. It is further unclear whether judicial review of classification designations has had much effect.[53]

---

46. Leonard B. Boudin, *The Ellsberg Case: Citizen Disclosure*, *in* SECRECY AND FOREIGN POLICY, *supra* note 15, at 291.

47. *Id.* at 309-310.

48. The classic examination of the Espionage laws is Harold Edgar & Benno C. Schmidt, *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929 (1973); *see also* Boudin, *supra* note 46, at 296-98; *supra* note 10 and accompanying text.

49. Boudin, *supra* note 46, at 294-95 (describing Ellsberg's reasons for disclosing information).

50. Officials in the Nixon administration broke into the office of Ellsberg's psychiatrist in order to find embarrassing information about him. With regard to the Ellsberg prosecution, see generally PETER SCHRAG, TEST OF LOYALTY, DANIEL ELLSBERG AND THE RITUALS OF SECRET GOVERNMENT 224-77 (1974).

51. 5 U.S.C. § 552(b)(1)(B) (2001). For background on the Nixon order and FOIA's amendment, see Relyea, *supra* note 5, at 24. Congress also acted partly in response to a Supreme Court decision finding that FOIA originally had not provided for judicial review of classification decisions. EPA v. Mink, 410 U.S. 73, 94 (1973).

52. Relyea, *supra* note 5, at 26.

53. Commentators argued that this reform was only marginally helpful because courts determining whether information is properly classified do not review the appropriateness of classification procedures

Even after FOIA, then, public access to "national security" information has depended largely on the good will of the President. Such good will has been inconsistently present, at best, and effectively non-existent, at worst. President Ford vetoed the 1974 amendments to FOIA (which Congress overrode) on the basis that judicial review of classification procedures violated the President's inherent, constitutional powers.[54] In contrast, President Carter's order emphasized the importance of "the public's interest in access to Government information" and the need to balance it against national security concerns[55]—the first executive order ever to do so.[56] While acknowledged as an improvement over Nixon's order, observers noted that Carter's order was "nonetheless weighted toward secrecy" and lacked sufficient oversight and control mechanisms.[57]

If Carter's order had its problems, the Reagan administration's approach to classification was disastrous with respect to public access to information. Executive Order 12,356[58] eliminated consideration of the public's right to know, expanded the categories of classifiable information, mandated that information within such categories be classified, eliminated automatic declassification, authorized reclassification of information, and encouraged classifiers to err on the side of classification.[59] The Reagan administration also successfully pushed for amendments weakening FOIA's disclosure requirements by broadening the categories of information that could be exempted.[60] Reagan officials further withheld from the public non-classifiable information (*i.e.*, "sensitive but unclassified" information) because such information could be exploited by terrorists and others working against the United States.[61]

---

but only ask whether the executive branch is following its own classification procedures. Note, *Keeping Secrets: Congress, the Courts, and National Security Information*, 103 HARV. L. REV. 906, 909 (1990).

54. Morton H. Halperin, *The President and National Security Information*, *in* THE PRESIDENCY AND INFORMATION POLICY, *supra* note 5. Congress, however, overrode Ford's veto. *Id.*

55. Exec. Order No. 12,065, 43 Fed. Reg. 28949 (July 3, 1978).

56. Halperin, *supra* note 54, at 68-69.

57. Relyea, *supra* note 5, at 26.

58. Exec. Order No. 12,356, 47 Fed. Reg. 14874-14884 (Apr. 6, 1982).

59. Harold C. Relyea, *Historical Development of Federal Information Policy*, *in* UNITED STATES GOVERNMENT INFORMATION POLICIES 25, 40 (Charles R. McClure et al. eds. 1989); Blanton, *supra* note 20, at 44; Quist, Chapter 3, *supra* note 15, at 22.

60. Diana M.T.K. Autin, *The Reagan Administration and the Freedom of Information Act*, *in* FREEDOM AT RISK: SECRECY CENSORSHIP AND REPRESSION IN THE 1980S, 69, 79-80 (Richard O. Curry ed. 1988); FOERSTEL, *supra* note 45, at 51-57.

61. *See* Genevieve J. Knezo, "Sensitive But Unclassified" and Other Federal Security Controls on Scientific Information: History and Current Controversy 11-13 (2003), *available at* http://www.fas.org/irp/crs/RL31845.pdf (last visited Aug. 12, 2004). The Reagan administration instituted numerous other mechanisms for secrecy regarding scientific and technical data. *See generally* John Shattuck, *Federal Restrictions on the Free Flow of Academic Information and Ideas*, *in* FREEDOM AT RISK, *supra* note 60, at 45-59.

Finally, hearkening back to the Nixon era, the Reagan administration pursued an Espionage Act prosecution against a government official who leaked information to a magazine publisher although the evidence showed he had not done so to injure the United States.[62] Reagan officials further intimated that they would pursue not only government officials but any publisher of the information as well, including newspapers and journalists.[63]

The Clinton administration reversed many of these polices, maintaining an openness that was unmatched by any previous administration.[64] Even here, however, the administration regressed toward secrecy. Spurred by allegations of carelessness regarding nuclear secrets, high-profile espionage cases involving CIA employees, and other politics, Clinton officials began refusing to provide unclassified information that had been public for years and fighting public requests regarding the CIA budget on the basis that such information "would put the United States at risk."[65] Not surprisingly, a government commission examining the issue of government secrecy in 1997 concluded that it remained a significant problem—costing Americans billions of dollars and eroding democratic principles of government accountability.[66] Nevertheless, Congress has not followed the commission's recommendations for legislation regarding the classification system.[67]

B. Government Control of Public Information

In times of national security crises, government officials have also tried to control public information to galvanize support for its efforts by minimizing dissension and creating an impression regarding the necessity of its actions. Such control of information has occurred through direct censorship or indirect censorship.

1. Direct Censorship

World War I provides the best example of direct government censorship. At the behest of the Wilson administration, which argued that dissent was "threatening the formation and maintenance of the armed forces," Congress passed two pieces of legislation designed to punish speech interfering with the

---

62. Steven Burkholder, *The Morison Case: The Leaker as "Spy," in* FREEDOM AT RISK, *supra* note 60, at 117-39. *See also* United States v. Morison, 844 F.2d 1057 (4th Cir. 1988).

63. Burkholder, *supra* note 62, at 120-21 (citing government memoranda).

64. Blanton, *supra* note 20, at 52-53. For details on Clinton's executive order (Exec. Order No. 12,958, 60 Fed. Reg. 19825 (Apr. 20, 1995)), see Quist, Chapter 3, *supra* note 15, at 22-31.

65. Blanton, *supra* note 20, at 52-54.

66. *Secrecy Report*, *supra* note 1, at 9-10 (cost estimates); *id.* at 7-9 (listing the intangible costs of secrecy).

67. *Id.* at 13.

war effort.[68] In 1917, Congress enacted the Espionage Act, providing criminal penalties for intentionally making false reports interfering with the war effort, causing insubordination or disloyalty in the military forces, or obstructing the draft. The Act also authorized the Postmaster to refuse to mail materials violating the Act.[69] In 1918, Congress further adopted the Sedition Act, which punished publication of information intended to cause contempt for the United States government, the Constitution or the flag of the United States, or supporting a country at war with the United States.[70]

The Espionage and Sedition Acts proved to be powerful weapons of suppression. Federal officials brought over 2,100 indictments under the Acts,[71] most of which involved speech critical of the war or the government rather than overt acts of disloyalty.[72] Thus, individuals were indicted for such things as distributing a pamphlet teaching that "Christians should not kill in wars" or arguing that "we must make the world safe for democracy, even if we have to bean the goddess of liberty to do it."[73] Such indictments were problematic primarily because they reached far into the realm of seemingly innocent speech. Many prosecutions, however, were more than simply over-zealous. Rather, they were specifically designed to destroy radical, social groups, such as the International Workers of the World and the Socialist Party, whose political philosophies the Wilson administration feared.[74] Thus, such prosecutions were not used to punish disloyalty but to enforce a national conformity by frightening people into silence.

The government also attempted to censor certain speech during the Cold War by prosecuting members of the Communist Party USA (CPUSA) under the Smith Act,[75] a peacetime sedition law prohibiting advocacy of overthrow of the government. Ostensibly the purpose of such a law was to prevent overthrow of the government by punishing those trying to incite such action. The Smith Act, however, was never used to punish the CPUSA for actual attempts to overthrow the government or even advocacy of such overthrow. Rather, despite voluminous evidence-gathering by the FBI, the government was unable to prove that the CPUSA advocated forcible overthrow of the

---

68. DAVID M. RABBAN, FREE SPEECH IN ITS FORGOTTEN YEARS 249 (1997); *see also* Christina E. Wells, *Discussing the First Amendment*, 101 MICH. L. REV. 1566, 1581-82 (2003) (reviewing LEE C. BOLLINGER & GEOFFREY R. STONE, ETERNALLY VIGILANT: FREE SPEECH IN THE MODERN ERA (2002)).

69. Act of June 15, 1917, ch. 30, tit. I, § 3, 40 Stat. 219.

70. Act of May 16, 1918, ch. 75, § 1, 40 Stat. 553.

71. ROBERT JUSTIN GOLDSTEIN, POLITICAL REPRESSION IN MODERN AMERICA FROM 1870-1976, 113 (rev. ed. 2001).

72. *Id.*

73. Wells, *supra* note 68, at 1583. *See also* RABBAN, *supra* note 68, at 259-60; GOLDSTEIN, *supra* note 71, at 113-14.

74. GOLDSTEIN, *supra* note 71, at 115.

75. Act of June 28, 1940, ch. 72, 54 Stat. 79.

government.[76] As a result, it prosecuted CPUSA members for "conspiring" to advocate forcible overthrow of the government. These charges rested on the theory that CPUSA leaders, in organizing and administering the CPUSA, taught Marxist-Leninist doctrine, which allegedly involved forcible overthrow as a necessary aspect of a Communist revolution.[77] The evidence for such prosecutions consisted of little more than Marxist-Leninist literature distributed by CPUSA members and testimony "interpreting" that literature from former CPUSA members.[78]

In effect, the Smith Act trials of CPUSA leaders were essentially political trials based upon the CPUSA leaders' belief in the possibility of an alternative political and economic system. As one commentator noted, such trials lacked any basis in law or fact and were little more than prosecutions for "organizing a group to commit a speech crime."[79] Typically, overtly political speech would have been protected by the First Amendment.[80] Nevertheless, the government systematically prosecuted CPUSA leaders during the Cold War for violating the advocacy provisions of the Smith Act.[81]

2. Indirect Censorship

During times of crisis, the government also has relied on equally powerful, if more indirect, censorship tools. Such tools fall into three categories

---

76. PETER L. STEINBERG, THE GREAT "RED MENACE:" UNITED STATES PROSECUTION OF AMERICAN COMMUNISTS 1947-1952, 108 (1984); *see also* MICHAL R. BELKNAP, COLD WAR POLITICAL JUSTICE: THE SMITH ACT, THE COMMUNIST PARTY, AND AMERICAN CIVIL LIBERTIES 80-81 (1977).

77. *See, e.g.*, United States v. Foster, 9 F.R.D. 367, 374-75 (S.D.N.Y. 1949) (setting forth grand jury indictment of CPUSA leaders).

78. *See* United States v. Dennis, 183 F.2d 201, 206 (2d Cir. 1950) (discussing evidence introduced at one of the CPUSA trials), *aff'd*, 341 U.S. 494 (1951); BELKNAP, *supra* note 76, at 80-92.

79. HARRY KALVEN, JR., A WORTHY TRADITION 193 (1988); *see also* STEINBERG, *supra* note 76, at 157.

80. In several cases prior to *Dennis v. United States*, 341 U.S. 494 (1951), the decision in which the Supreme Court upheld the CPUSA leaders' convictions, the Court had applied a very speech protective standard to political statements. *See* cases cited in Wells *supra* note 68, at 1577; *see also* Marc Rohr, *Communists and the First Amendment: The Shaping of Freedom of Advocacy in the Cold War Era*, 28 SAN DIEGO L. REV. 1, 31-36 (1991); Note, *Clear and Present Danger Re-examined*, 51 COLUM. L. REV. 98, 103-05 (1951).

81. Although *Dennis* involved the most famous of the CPUSA prosecutions, the government pursued CPUSA leaders in at least 126 prosecutions throughout the country. BELKNAP, *supra* note 76, at 156-57; Robert Mollan, *Smith Act Prosecutions: The Effect of the Dennis and Yates Decisions*, 26 U. PITT. L. REV. 705, 710-16, 723 (1965).

During this period the government also pursued many CPUSA leaders under the membership clause of the Smith Act, which prohibited active membership in an organization advocating forcible overthrow of the government. In fact, many of the CPUSA leaders who were convicted of conspiring to advocate overthrow of the government were released from jail only to be rearrested for membership clause violations. Mollan, *supra*, at 716-20; BELKNAP, *supra* note 76, at 262-65, 271-72.

—government propaganda, government accusations of lack of patriotism, and public stigmatization of people with certain beliefs or who belong to particular groups. Unlike direct punishment of expression, indirect tools amount to censorship by setting a national agenda and using pressure to conform as means to discourage dissenting opinions. Though they carry no legal sanctions, indirect tools can be remarkably effective.

Government officials perceiving a potential national security threat have often engaged in widespread propaganda—*i.e.*, dissemination of wholly or partially untrue information—to spur public support for immediate action. Such campaigns focus on an exaggerated characterization of the threat posed by certain individuals or groups. Specifically, government officials characterize the threat as new (thus requiring expanded powers), devious (often hidden within or controlling seemingly innocuous organizations) and immensely powerful (primarily because they were puppets of a threatening foreign power).[82]

Prior to and during World War I, for example, President Wilson gave numerous speeches emphasizing the threatening nature of radical groups and immigrants although he knew them to pose no threat of actual espionage or sabotage.[83] Thus, in a 1915 address he claimed that

> [t]he gravest threats against our national peace and safety have been uttered within our own borders. There are citizens of the United States . . . born under other flags but welcomed by our generous naturalization laws . . . who have poured the poison of disloyalty into the very arteries of our national life.[84]

He similarly accused the "military masters of Germany" of filling "our unsuspecting communities with vicious spies and conspirators" and of using "liberals in their enterprise . . .—socialists, the leaders of labor" to sow disloyalty in America.[85]

---

82. For a discussion of the characteristics of propaganda, see Richard Delgado, *The Language of the Arms Race: Should the People Limit Government Speech?*, 64 B.U. L. REV. 961 (1984).

83. The Wilson administration kept close watch on all potential spies and saboteurs in the German-American population, identifying approximately 1,800 for potential action in the event of war. SENATE SELECT COMM. TO STUDY GOVERNMENT OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 755, 94th Cong., Bk III, 380 (1976) [hereinafter CHURCH COMM., FINAL REPORT, BOOK III]. Almost all those persons believed to pose a threat during World War I were interned shortly after the war began. CURT GENTRY, J. EDGAR HOOVER: THE MAN AND THE SECRETS 71 (1991). Wilson's rhetorical invocation of the "spy within" image was aimed less at this threat than at galvanizing support for repression of radical groups who were heavily dominated by German immigrants who were not spies.

84. President Woodrow Wilson, Address to Congress (Dec. 7, 1915), *in* 53 CONG. REC. 99 (1915).

85. President Woodrow Wilson, Flag Day Address (June 14, 1917), *in* 55 CONG. REC. app. at 332, 334 (1917).

During World War II and the Cold War, government officials similarly characterized Japanese-Americans and CPUSA members, respectively, as potentially monstrous threats. Despite affirmative evidence regarding the loyalty of most Japanese-Americans,[86] government officials argued for their externship based upon the notion that they were almost inherently incapable of such loyalty:

> "[t]he Japanese race is an enemy race and while many second and third generation Japanese born on United States soil, possessed of United States citizenship, have become 'Americanized,' the racial strains are undiluted. . . . It, therefore, follows that along the vital Pacific Coast over 112,000 potential enemies, of Japanese extraction, are at large today."[87]

To spur support for his Cold War pursuit of domestic communists, J. Edgar Hoover, Director of the FBI, also painted a fearsome—if inaccurate—picture of them as devious and clever puppets of the Soviet Union:

> The Communist, once he is fully trained and indoctrinated, realizes that he can create his order in the United States only by "bloody revolution." . . .
>
> . . . .
>
> . . . [Cleverly, however, the] American progress which all good citizens seek, such as age-old security, houses for veterans, child assistance, and a host of others is being adopted as window dressing by Communists to conceal their true aims and entrap gullible followers. . . .
>
> The numerical strength of the party's enrolled membership is insignificant. . . .
>
> . . . .
>
> . . . [R]ather than the size of the Communist party, the way to weigh its true importance is by testing its influence, its ability to infiltrate
>
> . . . .
>
> The size of the party is relatively unimportant because of the enthusiasm and iron-clad discipline under which they operate.[88]

---

86. PETER IRONS, JUSTICE DELAYED: THE RECORD OF THE JAPANESE AMERICAN INTERMENT CASES 274-79 (1989) (discussing government reports concluding that Japanese-Americans were largely loyal to the United States).

87. COMMISSION ON WARTIME RELOCATION AND INTERNMENT OF CIVILIANS, PERSONAL JUSTICE DENIED, 66 (1982) (quoting General DeWitt).

88. J. Edgar Hoover, Testimony before HUAC, Mar. 26, 1947, *in* ELLEN SCHRECKER, THE AGE OF MCCARTHYISM 114-20 (1994). Government officials were quite aware that most members of the CPUSA

The existence of official propaganda machines facilitated these inaccurate portrayals of allegedly threatening domestic groups. During World War I, for example, the government's Committee on Public Information promoted films and organized speakers that recounted German atrocities, an action that further inflamed nativist and anti-immigrant sentiment.[89] Similarly, during the Cold War, FBI Director Hoover began a massive, secret educational campaign, including feeding his exaggerated image to newspaper reporters and anti-communist groups, to inform Americans about the dangers of domestic communism.[90]

In addition to propaganda, government officials also tried to co-opt public debate by accusing those who disagreed with them of being unpatriotic. Thus, during World War I, one prominent American noted:

> "The men who oppose the war; who fail to support the gov't in every measure which really tends to the efficient prosecution of the war; and above all who in any shape or way champion the cause and the actions of Germany, show themselves to the Huns within our own gates and allies of the men whom our sons and brothers are crossing the ocean to fight."[91]

Being branded as unpatriotic was not mere innocuous labeling. Rather, it could have significant consequences. As one commentator noted, during World War I "people who objected to, or even questioned, America's role in the war faced vilification by the press and the threat of mob violence."[92]

Finally, government officials often tried to induce conformity of thought and action by publicly exposing persons whom they believed belonged to dangerous organizations. Typically, government characterized this stigmatization as necessary to protect against anti-democratic propaganda. During its preparation for World War I, for example, Congress required that ownership of certain (often radical) publications sent through the mails be revealed because

> "[t]he extremely low postage rate accorded to second-class matter gives these publications a circulation and a corresponding influence unequaled in history. It is a common belief that many periodicals are

---

did not pose a threat to national security. *See* Christina E. Wells, Fear and Loathing in Constitutional Decision-Making 26 (Sept. 13, 2004) (unpublished manuscript on file with the author).

89. Bradley C. Bobertz, *The Brandeis Gambit: The Making of America's "First Freedom," 1909-1931*, 40 WM. & MARY L. REV. 557, 576-77 (1999).

90. RICHARD M. FRIED, NIGHTMARE IN RED: THE MCCARTHY ERA IN PERSPECTIVE 85 (1990); CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 430.

91. *Secrecy Report*, *supra* note 1, at A-1 (quoting President Theodore Roosevelt).

92. Bobertz, *supra* note 89, at 577.

> secretly owned or controlled, and that in reading such papers the public is deceived through ignorance of the interests the publication represents."[93]

Prior to World War II, the rise in popularity of fascist groups similarly prompted calls for exposure of the "identity and activities of foreign agents" in order to "'destroy[] the poison of totalitarian propaganda.'"[94] Such beliefs ultimately resulted in the Voorhis Act, which required the registration of groups with foreign affiliations.[95]

Public exposure as a tool reached its zenith, however, during the Cold War when HUAC, relying on information provided by the FBI, "regularly issued indices of identified 'communist sympathizers,' which became the basis of formal and informal blacklists in the public and private sectors."[96] Beginning in 1947, the Attorney General also regularly published lists of "subversive" organizations that ostensibly posed a threat to the United States.[97] The Internal Security Act of 1950 further required the registration of all Communist and "communist front" organizations.[98]

As with claims that dissenters were unpatriotic, public exposure of "communist sympathizers," "communist front organizations" and "subversives" was far from harmless. The definition of such terms was never clear and often interpreted far more broadly than necessary.[99] Furthermore, these lists became the basis of thousands of public and private actions, including interrogation by loyalty boards, job dismissal, and other social or economic sanctions.[100] Such broad stigmatization took a substantial toll on Americans as a whole, who became less willing to engage in open discussion.[101] As one commentator noted:

> In its full flower, the evils of the "method of exposure" were at least three-fold: The arbitrary and uncontrolled imposition of disabilities on citizens subjected to compelled disclosure, the substantive impact of exposure on individual exercise of constitutionally protected rights

---

93. Lewis Publ'g Co. v. Morgan, 229 U.S. 288, 312 (1913) (quoting S. REP. NO. 955, 62nd Cong. 24 (1912)).

94. Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 22 (1991) (quoting Institute of Living Law, *Combating Totalitarian Propaganda, The Method of Exposure*, 10 U. CHI. L. REV. 107, 108-09 (1943)).

95. Act of Oct. 17, 1940, ch. 897, 54 Stat. 1201.

96. Kreimer, *supra* note 94, at 18. On the relationship between the FBI and HUAC, see *id.* at 19 n.45; ELLEN SCHRECKER, MANY ARE THE CRIMES: MCCARTHYISM IN AMERICA 214-15 (1998).

97. Steinberg, *supra* note 76, at 29-30.

98. Act of Sept. 23, 1950, ch. 1024, 64 Stat. 987.

99. *Secrecy Report*, *supra* note 1, at A-43.

100. Kreimer, *supra* note 94, at 18 n.44.

101. *Id.* at 20 (citing opinion polls regarding public willingness to speak out).

of speech, thought, and associations, and the constraint on public thought and discourse from the fear of public investigation of private or long-buried beliefs and associations.[102]

C. Government Information Gathering

The third form of governmental information control involves information gathering—*i.e.*, intelligence[103]—regarding potential national security threats. During national security crises, when threats to national security are at their apex, the government expands its intelligence efforts. As history shows, however, although such efforts begin with legitimate national security concerns, they often mutate into tools of harassment of disfavored political groups.

1. Historical Pattern of Intelligence-Gathering

Although state and federal governments have always collected intelligence in some form,[104] World War I saw an enormous expansion of intelligence-gathering at the federal level in response to perceived threats from enemy aliens. Military intelligence personnel, for example, expanded from "two officers in early1917 . . . to more than 300 uniformed officers and 1,000 civilian employees" by the end of the war.[105] Similarly, the Justice Department's newly created Bureau of Investigation ("BI"), precursor to the FBI, expanded from 100 to 300 agents.[106] The BI's responsibilities also expanded beyond a narrowly defined set of crimes to include investigations of neutrality law violations.[107] Soon thereafter Congress further extended the BI's authority to investigations involving "'official matters under the control of the Department of Justice or the Department of State, as may be directed by the

---

102. *Id.* at 22.

103. *See* FRANK J. DONNER, THE AGE OF SURVEILLANCE xiv-xv (1980). Donner describes intelligence gathering as "a sequential process, which embraces the selection of the subject (an organization or individual) for surveillance, the techniques, both overt and clandestine, used in monitoring the subject or target, the processing and retention of information collected (files and dossiers), and its evaluation in the light of a strategic purpose (the intelligence mission)." *Id.* at 3. He further notes an "aggressive" aspect to intelligence that involves damage to or harassment of the target. *Id.* Typically, government officials gather intelligence by physical or electronic surveillance, *i.e.*, wiretaps, physical searches, etc. There are, however, related forms of surveillance, such as infiltration of private groups or enlistment of private entities/individuals to gather intelligence on the government's behalf.

104. For a brief history of intelligence efforts prior to World War I, see *id.* at 31.

105. HAROLD M. HYMAN, TO TRY MEN'S SOULS 271 (1959).

106. CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 379. For a history of the BI's birth and evolution up to 1916, see GENTRY, *supra* note 83.

107. GENTRY, *supra* note 83, at 114; Natsu Taylor Saito, *Whose Liberty? Whose Security? The USA PATRIOT Act in the Context of COINTELPRO and the Unlawful Repression of Political Dissent*, 81 OR. L. REV. 1051, 1071 (2002).

Attorney General,'"[108] language the BI interpreted as allowing it to engage in surveillance and investigations of enemy aliens for possible espionage or sabotage at the request of the Secretary of State.[109]

As the war continued, the government's intelligence activities expanded well beyond identifying actual threats of espionage or sabotage. As one historian noted:

> [m]ilitary intelligence agents participated in a wide range of dubious activities, which involved a wholesale system of spying on civilians that would be unmatched in scope until the late 1960's. Military intelligence activities included surveillance of the IWW, the SPA, the pacifist Fellowship of Reconciliation and the National Civil Liberties Bureau, forerunner of the American Civil Liberties Union. In some cases, military intelligence infiltrated the ranks of groups under surveillance and participated in raids and arrests of radical organizations.[110]

In some instances, military intelligence officers provoked strikes that they later "broke" via illegal raids and jailing of IWW members.[111] Other government personnel recommended investigation of targeted politicians and judges because their political or judicial decisions seemed too "radical."[112] The BI's intelligence activities also expanded well beyond any real threat posed by enemy aliens. Thus, investigations targeted any "[c]riticism of the war, opposition to the draft, expression of pro-German or pacifist sympathies, and militant labor organizing efforts."[113] These intelligence activities served as the basis for the thousands of repressive Espionage and Sedition Act prosecutions mentioned in the previous section.[114] Many were designed to do little more than destroy the disfavored political groups that were their target.

The government also enlisted private organizations to work on its behalf during World War I. Thus, Attorney General Gregory publicly requested "every loyal American to act as 'a volunteer detective'" regarding disloyalty, assuring citizens that they "'should feel free to bring their suspicions and information to the . . . Department of Justice.'"[115] Similarly, the BI worked

---

108. CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 379 (quoting 28 U.S.C. § 533(3) (2001)). Congress gave the BI this authority as part of an appropriations request in 1917.

109. *Id.* at 379-80.

110. GOLDSTEIN, *supra* note 71, at 110.

111. *Id.*

112. *Id.*

113. CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 382.

114. *See supra* notes 68-81 and accompanying text.

115. HYMAN, *supra* note 105, at 271-72 (citation omitted). Gregory also intimated that it was citizens' "patriotic duty" to report disloyal acts. *Id.* at 272.

closely with the American Protective League ("APL"), a vigilante organization initially formed to prevent German sabotage and espionage by using citizens in business to report on disloyalty, industrial disturbances or other actions potentially harming the nation.[116] With the APL's help, the BI staged a series of raids on IWW offices in 1917, rounding up hundreds of radicals allegedly posing a threat to national security.[117] Since most German agents had been rounded up months earlier, such raids were largely designed to destroy union influence rather than protect national security.[118] The APL's overzealous investigations of "un-American activities" led to significant abuses, involving "illegal arrests, strikebreaking, wiretapping, bugging, frame-ups, extortion, blackmail, kidnappings, rapes, and even . . . [in one case] murder."[119]

Rather than bringing about a decline in intelligence-gathering, the end of World War I saw a greatly expanded role for intelligence investigators. A series of "anarchist" bombings in 1919 rekindled national fear (the "Red Scare"), causing public and congressional demands for federal government action.[120] In response, Attorney General Palmer begged Congress for more resources, noting that the "recent bombings were part of a vast conspiracy to overthrow the government of the United States . . . . [T]he danger is imminent."[121] With these new resources, Palmer reorganized the BI, which immediately expanded its investigations of "'anarchists and similar classes, Bolshevism, and kindred agitations.'"[122] In 1919-20, these investigations, which also involved private citizens as informants,[123] resulted in a series of raids in which tens of thousands of aliens were rounded up and deported without due process of law.[124]

---

116. JOAN M. JENSEN, THE PRICE OF VIGILANCE 25 (1968). For a more in-depth discussion of the APL, see HYMAN, *supra* note 105, at 272-97.

117. GENTRY, *supra* note 83, at 71.

118. *Id.*; JENSEN, *supra* note 116, at 32.

119. GENTRY, *supra* note 83, at 72. *See also* Saito, *supra* note 107, at 1073. The APL's abuse of civil liberties culminated in the "slacker" raids of 1918, in which thousands of citizens allegedly violating the selective service laws were forcibly rounded-up and detained without adequate due process. CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 381.

120. CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 382-83; FRIED, *supra* note 90, at 42.

121. GENTRY, *supra* note 83, at 77; DONNER, *supra* note 103, at 33-34.

122. CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 383. Military intelligence of domestic activities also continued during this period. *Id.* at 387.

123. For more detail on surveillance techniques during the Red Scare, see RICHARD POLENBERG, FIGHTING FAITHS: THE ABRAMS CASE, THE SUPREME COURT, AND FREE SPEECH 161-96 (1987).

124. CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 383-85; DONNER, *supra* note 103, at 35-39.

While the raids were deplorable, of greater interest for this paper is the lasting surveillance machinery established during the Red Scare. Soon after being appointed director of the BI's "General Intelligence Division" in 1919, J. Edgar Hoover established an index of "radicals, their organizations, and publications."[125] Within months, the index contained 150,000 names, increasing to 450,000 by 1921.[126] The index further contained detailed biographies of 70,000 of the more important radicals (*i.e.*, those "showing 'any connection with an ultra radical body or movement.'"),[127] including transcriptions of speeches, writings, and newspaper articles by or regarding particular individuals.[128] Although the FBI could point to no tangible accomplishments as a result of the index, it proved to be a valuable tool for harassment of ostensibly subversive groups. As one commentator noted, during this period "[t]he bureau wiretapped at random, broke into offices and kept tabs on personal lives. The targets were often critics of the bureau or of the Justice Department and even included several senators who may have asked too many questions."[129]

In 1924, newly-appointed Attorney General Harlan Fiske Stone tried to reign in the BI's excesses. Recognizing the BI had "become a secret political police force . . . 'maintaining many activities which were without any authority in federal statute's [sic] and engaging in many practices which were brutal and tyrannical in the extreme,'"[130] Stone ordered the BI to limit its investigations to violations of the law and to rid itself of incompetent personnel. He also appointed Hoover, who had promised to help with reform, as director of the BI.[131] While the Attorney General's reforms halted the most egregious of the BI's practices, they were not safeguards against future abuse. The BI maintained its intelligence files and continued to collect information on Communists that it regularly shared with military intelligence.[132]

---

125. DONNER, *supra* note 103, at 34; CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 386.

126. CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 386; DONNER, *supra* note 103, at 34.

127. GENTRY, *supra* note 83, at 79 (citation omitted).

128. DONNER, *supra* note 103, at 34-35.

129. Geoffrey R. Stone, *The Reagan Administration, the First Amendment, and FBI Domestic Security Investigations*, *in* FREEDOM AT RISK, *supra* note 60, at 272, 274.

130. CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 388 (citation omitted).

131. GENTRY, *supra* note 83, at 127; DONNER, *supra* note 103, at 46.

132. CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 390-91; GENTRY, *supra* note 83, at 141. Furthermore, local governments, private organizations and other branches of government filled the intelligence void, gathering information regarding and harassing allegedly subversive groups, especially labor unions. CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 390; DONNER, *supra* note 103, at 48.

By 1936, the BI (now renamed the Federal Bureau of Investigation) renewed its intelligence activities with zeal after President Franklin Roosevelt directed Hoover to gather information about "subversive activities in the United States, particularly Fascism and Communism."[133] Although there was no specific statutory authority for such an investigation, both men relied on the ill-defined authority given the FBI in an earlier 1917 appropriations request.[134] Pursuant to this authority, the FBI began investigating "subversive" organizations (including industries, labor, educational and youth groups),[135] using "all possible sources" of intelligence, including informants, physical and technical surveillances, mail openings, and "black bag jobs" (*i.e.*, burglaries).[136]

In 1939, Roosevelt issued another confidential directive vesting authority for the "investigation 'of all espionage, counterespionage, and sabotage matters'" in the FBI and two other federal intelligence agencies.[137] While enhanced intelligence activities were a legitimate concern in light of global hostilities, this directive, coupled with the 1936 directive, caused lasting confusion regarding the FBI's legal authority to collect domestic intelligence. As one commentator noted:

> J. Edgar Hoover assumed he had broad authority from the President, going back to directives from Franklin D. Roosevelt in the 1930s, for conducting intelligence operations against "subversive activities" in the United States. The scope of that authority was never adequately defined, the practical meaning of "subversion" varied according to the political climate of the times, and the Attorney General's role in supervising the FBI was uncertain because the FBI director's mandate came directly from the President.[138]

Over the years, Hoover manipulated that confusion in order to maintain intelligence on "an ever-expanding class of political dissidents."[139]

After World War II, the FBI intensified its intelligence investigations, initially focusing on Communist and other revolutionary organizations who

---

133. CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 394 (citing Hoover memorandum of meeting dated 8/24/36).

134. GENTRY, *supra* note 83, at 207. *See supra* note 108 and accompanying text.

135. GENTRY, *supra* note 83, at 207; CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 396-99; Saito, *supra* note 107, at 1075-76.

136. GENTRY, *supra* note 83, at 207-08; Saito, *supra* note 107, at 1075-76.

137. DONNER, *supra* note 103, at 57 (citations omitted); CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 402-403.

138. JOHN T. ELLIFF, THE REFORM OF FBI INTELLIGENCE OPERATIONS 6-7 (1979). For further discussion on the confusion surrounding the FBI's legal authority to conduct domestic intelligence investigations, see DONNER, *supra* note 103, at 64-78.

139. Stone, *supra* note 129, at 274.

might pose a threat to the country.[140] FBI officials believed, however, that it was "'not possible to formulate any hard-and-fast standards by which the dangerousness of individuals members or affiliates of revolutionary organizations may be automatically measured.'"[141] The FBI thus began to investigate groups potentially subject to communist influence, a term defined broadly to include groups dedicated to political, racial, children's, gender, agricultural, cultural, veterans', educational and industrial issues.[142] Such investigations rarely provided information regarding real threats, and instead provided political intelligence for government officials. As in previous eras, the FBI relied on a variety of legal and illegal information-gathering techniques, including wiretaps, bugs, confidential informants, physical and photographic surveillance, review of public and private records, and burglaries.[143]

The FBI's abuse of domestic intelligence-gathering culminated in its now-infamous COINTELPRO operations, which it conducted from 1956 until 1971. Counterintelligence operations such as these ostensibly include "those actions by an intelligence agency intended to protect its own security and to undermine hostile intelligence operations."[144] The FBI's programs, however, went far beyond intelligence-gathering to counter national security threats, instead extending to "secret actions de[signed] to 'disrupt' and 'neutralize' target groups and individuals . . . on the theory that preventing the growth of dangerous groups and the propagation of dangerous ideas would protect the national security and deter violence."[145]

As with earlier FBI surveillance operations, the targets of its COINTELPRO operations expanded over time. Beginning with the CPUSA in 1956,[146] the COINTELPRO programs grew to include the Socialist Workers Party, the civil rights movement, White hate groups, Black nationalist groups,

---

140. CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 430. The FBI maintained a "Security Index" of persons who were potentially dangerous to the United States in the event of a crisis. The list included not only known domestic communists but also suspected communist sympathizers. *Id.* at 436-38. By 1951, the list contained over 13,000 names; by 1954, it contained over 26,000 names. *Id.* at 440, 446.

141. *Id.* at 448.

142. *Id.* at 449; GOLDSTEIN, *supra* note 71, at 272-73. By 1960, the FBI had opened at least 432,000 files on "subversive" individuals and groups. CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 451.

143. *Id.* at 448; GOLDSTEIN, *supra* note 71, at 272-73. *See also* Socialist Workers Party v. Attorney General, 642 F. Supp. 1357, 1379-80 (S.D.N.Y. 1986).

144. CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 4. COINTELPRO is an acronym for "counterintelligence program."

145. *Id.* at 3.

146. The COINTELPRO operation against the CPUSA was not a dramatic departure from past practices but merely a "formalization of previous harassment of the [CPUSA] which had been directed by the FBI on an *ad hoc* basis for a number of years." GOLDSTEIN, *supra* note 71, at 407.

and "new left" groups, a broadly defined category of organizations including the Southern Christian Leadership Conference, Students for a Democratic Society, and the National Organization for Women.[147] The breadth of the investigations was staggering—over COINTELPRO's life the FBI opened 2,000 separate investigations.[148] It was also indiscriminate. Anything remotely considered to be subversive justified an investigation, even something as trivial as writing a letter to a newspaper supporting protests against censorship.[149]

The FBI's COINTELPRO tactics went far beyond surveillance, reliance on informers and illegal searchers, although those familiar techniques were part of its arsenal. COINTELPRO also included actions designed to harass targets, such as:

> attempts to disrupt marriages, to stir factionalism within and between dissident groups, to have dissidents fired from jobs and ousted by landlords, to prevent protestors from speaking and protest groups from forming, to have derogatory material planted in the press or among acquaintances of targets, to interfere with peaceful demonstrations and deny facilities for meetings and conferences, to cause funding cut-offs to dissident groups, to prevent the distribution of literature and to get local police to arrest targets for alleged criminal law violations.[150]

The FBI's tactics had a corrosive effect, chilling First Amendment expression by groups[151] and destroying individual lives.[152] They rarely, however, pro-

---

147. CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 15-24, 50-58.

148. *Id.* at 3.

149. *Id.* at 27. Approximately 18 percent of the FBI's total COINTELPRO operations were directed at groups simply for their First Amendment expression. *Id.* at 28.

150. GOLDSTEIN, *supra* note 71, at 470. *See also* CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 34-61; Saito, *supra* note 107, at 1082-86.

151. SENATE SELECT COMM. TO STUDY GOVERNMENT OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 755, 94th Cong., Bk II, 17 (1976) [hereinafter CHURCH COMM., FINAL REPORT, BOOK II].

152. *See, e.g.*, GENTRY, *supra* note 83, at 444 (noting the number of suicides and stress-related deaths of FBI targets); GOLDSTEIN, *supra* note 71, at 471 (noting FBI actions resulted in break-up of marriage); *id.* at 525 (noting that tactics caused the individual to flee the town in fear of his life). Despite the harm caused, the FBI justified its tactics as necessary to win the "war" against subversion. As William Sullivan, assistant director of the FBI explained:

> "This is a rough, tough, dirty business, and dangerous. It was dangerous at times. No holds were barred. . . . We have used [these techniques] against Soviet agents. They have used [them] against us. . . . [These same methods were brought] home against any organization against which we were targeted. We did not differentiate. This is a rough, tough business."

CHURCH COMM., FINAL REPORT, BOOK III, *supra* note 83, at 7 (alteration in original) (quoting William C. Sullivan, testimony to Congress dated 11/1/75).

vided advance knowledge of illegal activity or information leading to prosecutions for violation of the law.[153]

The FBI's surveillance of domestic groups, while most extensive during the 1960s, was not the only government surveillance during this period. The CIA also engaged in a number of domestic intelligence activities, including mail openings and surveillance of domestic groups thought to be radical or subject to foreign influence.[154] Military intelligence also gathered intelligence on civilian political activity, ostensibly to protect against domestic disorder.[155] Federal authorities encouraged local law enforcement to gather intelligence about dissident organizations.[156] As with the FBI, the scope of such investigations was expansive, including organizations involved in "completely peaceful and lawful activity."[157] Such investigations also rarely garnered valuable information regarding threats.[158]

2. Attempted Reform

As the federal government's abuse of intelligence-gathering came to light in the 1970s, Congress began to investigate. The Church and Pike committees, in the Senate and House respectively, mounted lengthy investigations of the intelligence community.[159] Although the Church Committee produced a detailed report regarding government abuse of intelligence gathering,[160] politics prevented either committee from directly bringing about reform.[161] In 1976, however, the Senate established a permanent committee regarding intelligence operations.[162] The House created such a committee in 1977.[163] While the committees provide some oversight regarding intelligence

153. GOLDSTEIN, *supra* note 71, at 465 (citing GAO report).

154. CHURCH COMM., FINAL REPORT, BOOK II, *supra* note 151, at 96-104; GOLDSTEIN, *supra* note 71, at 454-57.

155. CHURCH COMM., FINAL REPORT, BOOK II, *supra* note 151, at 77, 84; GOLDSTEIN, *supra* note 71, at 457-59.

156. CHURCH COMM., BOOK II, *supra* note 151, at 77.

157. GOLDSTEIN, *supra* note 71, at 458; *see also* CHURCH COMM. BOOK II, *supra* note 151, at 213.

158. One congressional committee, for example, noted that military surveillance of domestic groups was "utterly useless." GOLDSTEIN, *supra* note 71, at 459.

159. KATHRYN S. OLMSTED, CHALLENGING THE SECRET GOVERNMENT 2 (1996). For in-depth discussions on the activities of the committees, *see id.* at 81-143.

160. *See supra* notes 83 & 151.

161. For a discussion of the politics surrounding both committees and executive branch attempts to discredit them, see generally OLMSTED, *supra* note 159.

162. *Id.* at 175-76; *see also* LOCH K. JOHNSON, A SEASON OF INQUIRY: CONGRESS AND INTELLIGENCE (1988).

163. FRANK J. SMIST, JR., CONGRESS OVERSEES THE UNITED STATES INTELLIGENCE COMMUNITY 1947-89, 214-15 (1990).

activities.[164] reformers fell short of establishing comprehensive statutory authority regarding intelligence activities.[165]

Congress did enact the Foreign Intelligence Surveillance Act ("FISA") in 1978 in order to constrain federal wiretapping authority in certain foreign intelligence investigations.[166] FISA authorized wiretaps in those situations under lesser standards than required in criminal investigations or intelligence investigations of purely domestic threats.[167] The statute allowed intelligence officials to wiretap persons in the United States only if officials certified to a special court that they had "probable cause" to believe the person was a foreign power or agent of a foreign power, that the target was conducting activities that may violate U.S. criminal law, and that the wiretap would be conducted for the purpose of gathering foreign intelligence information.[168] Thus, FISA, while allowing electronic surveillance in foreign intelligence investigations on U.S. soil, nevertheless provided oversight for the decision to wiretap, which had previously been grounded solely in the executive branch.

During the 1970s the executive branch also took steps to reform its domestic intelligence gathering activities, primarily to undercut legislative efforts at reform.[169] In 1976, Attorney General Edward Levi issued a set of guidelines governing the FBI's domestic security investigations.[170] A response to the abuses of the past, the guidelines "were designed to focus such investigations solely on possible criminal activity and to prevent the bureau from engaging in open-ended investigations of 'subversives' and 'dissidents' generally."[171] Accordingly, the guidelines allowed the FBI to open domestic

---

164. Some observers have noted that by centralizing oversight authority and reducing the number of people involved, the creation of a permanent committee was a "victory for secrecy." OLMSTED, *supra* note 159, at 176 (citation omitted).

165. Some scholars argue that the entire point of the Church committee was to develop legislation for the intelligence community that would restrict certain activities. JOHNSON, *supra* note 162, at 227; SMIST, *supra* note 163, at 84. Congress "abandoned the effort to enact a comprehensive intelligence charter" in the 1980s. SMIST, *supra* note 163, at 84.

166. 50 U.S.C. §§ 1801-11 (2001). The Senate Report regarding FISA indicates that it is a direct response to abuse revealed during congressional investigations of the intelligence community. S. REP. NO. 95-1267, 95th Cong., 8-9 (1978).

167. Katz v. United States, 389 U.S. 347 (1967); United States v. United States District Court, 407 U.S. 297 (1972).

168. 50 U.S.C. §§ 1805(a)(3); 1801(b)(2)(A); 1804(a)(7)(B). For a thorough discussion of FISA prior to the USA Patriot Act amendments in 2001, see William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 74-91 (2000).

169. *See* OLMSTED, *supra* note 159, at 173.

170. Domestic Security Investigation Guidelines (1976), *reprinted in FBI Statutory Charter: Hearings on S. 1612 Before the Senate Committee on the Judiciary*, 95th Cong., 18-26 (1978) [hereinafter Levi Guidelines].

171. Stone, *supra* note 129, at 276.

security investigations only to ascertain information on groups or individuals whose activities might involve violence and the violation of federal law.[172]

The Levi guidelines contemplated three levels of investigations: preliminary, limited and full. Preliminary investigations could be instigated only upon the basis of "allegations or other information" that the target might be engaged in unlawful activities involving the use of force or violence.[173] Such investigations were confined to ascertaining "whether there [was] a factual basis for opening a full investigation" and were limited to 90 days unless longer periods were approved by FBI headquarters.[174] The guidelines further limited surveillance techniques in preliminary investigations to review of existing FBI files, existing law enforcement records, public records, and other established sources of information.[175] Physical surveillance and interviews were allowed only to identify the subject of an investigation and more intrusive forms of surveillance, such as mail covers, mail openings, electronic surveillance, and recruitment of new informants were expressly prohibited.[176]

The Levi guidelines allowed "limited" investigations only when a preliminary investigation was "inadequate to determine if there is a factual basis for a full investigation." As with preliminary investigations, limited investigations were confined to 90 days. Surveillance tools available to investigators were also confined to those listed above with two additions: Investigators could use physical surveillance and interviews for purposes other than identifying the subject of the investigation.[177]

The Levi guidelines allowed the FBI to conduct full investigations when there existed "specific and articulable facts giving reason to believe that an individual or a group is or may be engaged" in unlawful activities involving the use of force or violence.[178] The guidelines further directed investigators to consider the magnitude of the threatened harm, its likelihood, the immediacy of the threat, and the danger to privacy and free expression posed by opening an investigation.[179] Full investigations could be conducted for up to one year without approval of the Department of Justice.[180] Investigators were allowed to use more intrusive techniques such as electronic surveillance and mail covers but only in limited circumstances.[181]

---

172. Levi Guidelines, *supra* note 170, § I(A).
173. *Id.* § II(C).
174. *Id.*; *id.* § II(H).
175. *Id.* § II(E).
176. *Id.* § II(G).
177. *Id.* § II(F)-(H).
178. *Id.* § II(I)
179. *Id.*
180. *Id.* § III(C).
181. *Id.* § II(J).

Although the Levi guidelines served merely as an internal document and were not judicially enforceable, they had an immediate effect.[182] The number of security investigations instituted by the FBI fell from 4,868 before the guidelines to 26 in 1981 and the latter all involved organizations involved in violent activities.[183]

In 1983, however, at the behest of critics who believed that the guidelines hampered the FBI's law enforcement capabilities,[184] William French Smith, Attorney General under Ronald Reagan, issued new guidelines. The Smith guidelines eliminated preliminary and limited investigations solely for domestic security purposes, a move that some saw as more potentially restrictive than the Levi guidelines.[185] The Smith guidelines, however, allowed full investigations to be instituted when "facts or circumstances reasonably indicated that two or more persons are engaged in an enterprise for the purpose of furthering political or social goals wholly or in part through activities that involve force or violence."[186] Such a standard was admittedly lower than the requirement of "specific and articulable facts" found in the Levi guidelines.[187] The Smith guidelines further allowed the FBI to open investigations based upon a group's advocacy of criminal activity "unless it is apparent, from the circumstances or the context in which the statements [were] made, that there

182. For a discussion of the legal effect of the guidelines, see John T. Elliff, *The Attorney General's Guidelines for FBI Investigations*, 69 CORNELL L. REV. 785, 786-92 (1984).

183. Stone, *supra* note 129, at 277; *see also* GENERAL ACCOUNTING OFFICE, REPORT OF THE COMPTROLLER GENERAL OF THE UNITED STATES, FBI DOMESTIC INTELLIGENCE OPERATIONS: AN UNCERTAIN FUTURE 22 (1977).

184. Stone, *supra* note 129, at 277-78; Athan Theoharis, *Conservative Politics and Surveillance: The Cold War, the Reagan Administration, and the FBI*, *in* FREEDOM AT RISK, *supra* note 60, at 259, 265-66.

185. Elliff, *supra* note 182, at 804-5. The Smith guidelines placed preliminary investigations under the auspices of "general crimes" authority, which allowed such investigations where "responsible handling require[d] some further scrutiny . . . in response to . . . allegation[s] or information indicating the possibility of criminal activity." The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations § II(B)(1) (1983), *reprinted in* 32 CRIM L. REP. (BNA) 3087-93 (1983) [hereinafter Smith Guidelines]. The consolidation of preliminary inquiries did not eliminate them for intelligence purposes. The guidelines make clear that preliminary inquiries can be used as the basis for full criminal or intelligence investigations. *Id.* § I. Such inquiries were still limited to 90 days without additional approval and mail covers, mail openings, and electronic surveillance were still prohibited. *Id.* § II(B)(3)-(5).

186. Smith Guidelines, *supra* note 185, § III(B)(1).

187. Elliff, *supra* note 182, at 799; Stone, *supra* note 129, at 278-79. The Smith Guidelines, however, allowed investigations to continue only for 180 days without authorization from high-level FBI officials. Smith Guidelines, *supra* note 185, § III(B)(4)(b). As with the Levi guidelines, a wide variety of investigative techniques were allowed in full investigations although officials were admonished to consider "whether the information could be obtained in a timely and effective way by less intrusive means." *Id.* § IV(A).

[was] no prospect of harm."[188] Some critics charged that the Smith guidelines represented a "reexpansion of the FBI's authority to investigate domestic 'subversion.'"[189] The Smith guidelines remained in force in somewhat amended form until 2002.[190]

The Reagan administration expanded the FBI's ability to instigate domestic security investigations in other ways. In 1981, President Reagan issued Executive Order 12,333 regarding intelligence activities within the United States.[191] That order allowed intelligence agencies to use intrusive surveillance techniques against domestic groups, including electronic surveillance, warrantless searches, and group infiltration. Although the order ostensibly allowed such techniques only when used to collect information related to a foreign intelligence investigation, critics have noted that its breadth could include surveillance of purely domestic groups.[192] The order, in somewhat amended form, remains in force.

II. CURRENT POWERS PERTAINING TO INFORMATION CONTROL

The September 11th terrorist attacks and the on-going war against terrorism, as arguably the most significant national security crisis in decades, have again spurred the government to take control of information. While this effort is still in its nascency, the discussion below reveals that many of the government's recent efforts are strikingly similar to its historical pattern of information control.

A. Government Control of Confidential Information

On March 25, 2003, President Bush signed Executive Order 13,292,[193] which amended the pre-existing order signed by President Clinton[194] and expanded the government's ability to keep information secret. The Bush order gives the government greater leeway to designate material as classified for

188. Smith Guidelines, *supra* note 185, at § I.

189. Stone, *supra* note 129, at 279.

190. Attorney General Richard Thornburg issued new guidelines in 1989 but they were substantially similar to the Smith Guidelines. The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations (1989), *available at* http://www.usdoj.gov/ag/readingroom/generalcrimea.htm (last visited Aug. 11, 2004) [hereinafter Thornburg Guidelines].

191. Exec. Order No. 12,333, 46 Fed. Reg. 59941 (Dec. 8, 1981).

192. Autin, *supra* note 60, at 74-75; Theoharis, *supra* note 184, at 269.

193. Exec. Order No. 13,292, 68 Fed. Reg. 15315 (Mar. 28, 2003).

194. Exec. Order No. 12,958, 60 Fed. Reg. 19825 (Apr. 20, 1995).

longer periods of time[195] and to reclassify previously released information.[196] It also broadens the government's ability to exempt from automatic disclosure certain categories of information by requiring only that the government show that the information "could" hurt national security if released.[197] Finally, the Bush order removed several provisions of Clinton's previous order designed to protect against excessive secrecy by requiring that information be disclosed or classified at the lowest level if there existed doubt about the propriety of classification.[198] As one commentator noted, these "seemingly minor deletion[s]" will likely promote greater secrecy by "changing the 'default' setting from 'do not classify' to 'classify.'"[199] The Bush administration's 14 percent increase in classification actions in 2001 to 2002, the year prior to Bush's order, supports they argument.[200]

The Bush administration also tended toward secrecy in its interpretation of FOIA requests. Almost immediately after the September 11th attacks, Attorney General John Ashcroft encouraged agency heads to withhold discretionary information in response to FOIA requests.[201] Within a few months, White House Chief of Staff Andrew Card further directed agencies to expansively interpret FOIA exemptions to withhold "sensitive but unclassified" data[202]—material which is not automatically exempted from disclosure in response to FOIA requests.[203] These memos generated criticism.

---

195. *Compare* Exec. Order No. 13292 § 1.5 *with* Exec. Order No. 12,958 § 1.6.

196. *Compare* Exec. Order No. 13292 § 1.7(c) *with* Exec. Order No. 12,958 § 1.6(c).

197. Exec. Order No. 13,292 § 3.3(b). The Clinton order allowed exemption only if release of such information "should" be expected to harm national security. Exec. Order No. 12,958 § 3.3(b).

198. *See* Exec. Order No. 12,958 §§ 1.2(b), 1.3(c).

199. Lawyers Committee for Human Rights, *Assessing the New Normal: Liberty and Security for the Post-September 11 United States* 6 (2003), *available at* http://www.humanrightsfirst.org/us_law/loss/assessing/assessingnewnormal.htm (last visited Aug. 11, 2004) [hereinafter *Assessing the New Normal*].

200. *Id.* at 2.

201. Memorandum from Attorney General John Ashcroft to all heads of federal departments and agencies (October 12, 2001), *available at* http://www.doi.gov/foia/foia.pdf (last visited Aug. 11, 2004). Ashcroft's directive specifically noted that the Department of Justice would defend agency decisions unless they "lack[ed] a sound legal basis or present[ed] an unwarranted risk of adverse impact on the ability of other agencies to protect other important records." *Id.* His directive thus reversed a previous "presumption of disclosure" with respect to agency information. *Assessing the New Normal*, *supra* note 199, at 89 n.14.

202. Memorandum from White House Chief of Staff, Andrew H. Card, Jr. to the heads of executive departments and agencies (Mar. 19, 2002), *available at* http://www.fas.org/sgp/bush/wh031902.html (last visited Aug. 11, 2004). Congress also acted regarding "sensitive but unclassified" information, directing the President to "identify and safeguard homeland security information that is sensitive but unclassified." Homeland Security Act of 2002 § 892(a)(1)(B), 6 U.S.C.A. § 482(a)(1)(B) (West Supp. 2004).

203. For more in-depth discussion of the Bush administration's directives see, Kristen Elizabeth Uhl, Comment, *The Freedom of Information Act Post -9/11: Balancing the Public's Right to Know, Critical Infrastructure Protection and Homeland Security*, 53 AM. U. L. REV. 261, 272-74 (2003); Keith Anderson, Note, *Is there Still a "Sound Legal Basis?": The Freedom of Information Act in the Post 9-11 World*, 64 OHIO ST. L.J. 1605, 1621-28 (2003).

Some argued that Ashcroft's memo would exacerbate agencies' already abysmal responses to FOIA requests, making discoverable information even harder to obtain than before the terrorist attacks.[204] The scientific community, whose research is potentially subject to the "sensitive but unclassified" restriction, also argued about the dangers of using that term, noting that it has never been adequately defined and that there exist no administrative mechanisms to challenge government secrecy determinations.[205]

In 2002, at the White House's behest, Congress broadened the government's powers to withhold information under FOIA by adding a "critical infrastructure exemption" that specifically allows agencies to withhold information voluntarily submitted to it by private entities "regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose."[206] The new exemption has also been widely criticized, with commentators arguing that its breadth allows business and industry to hide wrongdoing by submitting information regarding public hazards to the government under the guise of "critical infrastructure" information.[207] Commentators are also concerned that the new legislation allows criminal punishment of government officials who reveal such information even if they do so as "whistleblowers" trying to protect the public interest.[208]

There have been other, related signs of increased government secrecy following the terrorist attacks. Within weeks of September 11, 2001, government agencies removed non-classified information from their websites

204. Reporters Committee for Freedom of the Press, *Homefront Confidential: Freedom of Information* 1-3 (4th ed. 2003), *available at* http://www.rcfp.org/homefrontconfidential/foi.html (last visited Aug. 14, 2004) [hereinafter *Homefront Confidential, Freedom of Information*]. For a history of agency resistance to FOIA requests, see FOERSTEL, *supra* note 45, at 1-72, 99-114.

205. *See* Knezo, *supra* note 61, at 30-35; Patrice McDermott, *Withhold and Control: Information in the Bush Administration*, 12 KAN. J.L. & PUB. POL'Y 671, 675-76 (2003). *But see* Anderson, *supra* note 203, at 1622-28. For a discussion of the practical impact of the Ashcroft and Card memos on agency FOIA practice, see *The National Security Archive, The Ashcroft Memo: "Drastic" Change or "More Thunder than Lightning*?," (2003), *available at* http://www.gwu.edu/%7Ensarchiv/NSAEBB/NSAEBB84/index.html (last visited Aug. 12, 2004) [hereinafter *National Security Archive, The Ashcroft Memo*].

206. Homeland Security Act of 2002 § 214, 6 U.S.C.A. § 133(a)(1). Federal law defines "critical infrastructure" as "systems, assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." 42 U.S.C. § 5195c(e) (Supp. I 2003).

207. Uhl, *supra* note 203, at 280-81; *Assessing the New Normal*, *supra* note 199, at 5-6; Press Release, American Civil Liberties Union, ACLU Says Freedom of Information Act Exemptions For Private Industry Would Endanger Public Safety (July 24, 2002), *available at* http://archive.aclu.org/news/2002/n072402a.html (last visited Aug. 12, 2004).

208. Uhl, *supra* note 203, at 277. *See* Homeland Security Act of 2002 § 214(f), 6 U.S.C. § 133(f).

"because of its possible usefulness to terrorists."[209] During the summer of 2002, the Bush administration also refused to reveal information regarding its implementation of the USA Patriot Act in response to congressional questions, only doing so after Congress threatened to subpoena the information. Even then, the administration asserted that much of the material was classified.[210] Secrecy with respect to quasi-judicial proceedings has also increased. In October, 2001, Chief Immigration Judge Michael Creppy issued a memo providing for blanket closures of all immigration proceedings deemed to be of "special interest."[211] The government also refused to reveal the names and identities of persons detained in the immediate aftermath of the terrorist attacks, claiming that dissemination of such information would interfere with an on-going law enforcement investigation.[212] Finally, in November 2001, President Bush signed Executive Order 13,233, which expands the ability of sitting and incumbent presidents to delay release of presidential records from the national archives.[213]

Furthermore, the Bush administration has aggressively tried to preempt disclosure of information by threatening criminal punishment or refusing to share information with Congress. In October 2001, President Bush reduced the number of congressional officials allowed to attend intelligence briefings, allegedly because of leaks regarding potential future terrorist attacks.[214] In the Summer of 2002, the White House further requested that congressional officials produce documents and take lie detector tests to determine if they had

---

209. *Homefront Confidential, Freedom of Information*, *supra* note 204, at 20.

210. *Assessing the New Normal*, *supra* note 199, at 8-9.

211. *Id.* at 12. This move was upheld by the Third Circuit in *North Jersey Media Group, Inc. v. Ashcroft*, 308 F.3d 198 (3d Cir. 2003) but struck down by the Sixth Circuit in *Detroit Free Press v. Ashcroft*, 303 F.3d 681 (6th Cir. 2002). For discussion of other secrecy issues surrounding quasi-judicial proceedings, see Reporters Committee for Freedom of the Press, *Homefront Confidential: Access to Terrorism and Immigration Proceedings* 9-17 (4th ed. 2003), *available at* http://www.rcfp.org/homefront confidential/immigration.html (last visited Aug. 14, 2004).

212. Ctr. for Nat'l Sec. Studies v. United States DOJ, 331 F.3d 918, 923 (D.C. Cir. 2003). The majority ruled in the government's favor over a vociferous dissent by Judge David Tatel, who argued that the government's argument was "vague" and "poorly reasoned." *Id.* at 937 (Tatel, J., dissenting).

213. Exec. Order No. 13,233, 66 Fed. Reg. 56025 (Nov. 15, 2001). For commentary on the order, see Jonathan Turley, *Presidential Papers and Popular Government: The Convergence of Constitutional and Property Theory in Claims of Ownership and Control of Presidential Records*, 88 CORNELL L. REV. 651 (2003); Marcy Lynn Karin, *Out of Sight, But Not Out of Mind: How Executive Order 13,233 Expands Executive Privilege While Simultaneously Preventing Access to Presidential Records*, 55 STAN. L. REV. 529 (2002).

214. Dana Milbank & Peter Slevin, Bush Edict on Briefings Irks Hill; White House Stems Information Flow, WASH. POST, Oct. 20, 2001, at A1, *available at* 2001 WL 29160567 (last visited Aug. 14, 2004).

leaked information regarding the September 11th attacks.[215] Many congresspersons objected, claiming that the measures were coercive and a violation of separation of powers.[216] In October, 2002, the Department of Justice announced a policy of aggressively enforcing existing laws to prevent disclosures of classified information and suggested that a new law criminalizing disclosures generally, not simply in the espionage context, might be helpful.[217]

B. Government Control of Public Information

The Bush administration has attempted to control public information as well. As discussed below, although some of the Bush administration's actions involve direct repression, the bulk of them involve more informal, indirect censorship.

1. Direct Censorship

The primary potential weapons of direct censorship involve expanded federal laws criminalizing (1) "material support" of terrorism and (2) "domestic terrorism." The material support laws allow prosecution and deportation of individuals providing "material support" to terrorist groups (as designated by the State Department).[218] Such support includes provision of weapons, physical assets, transportation, expert advice, monetary assistance, training and personnel.[219] The laws do not require that the defendant intend to further terrorism; it is enough that one's actions support terrorism regardless of one's intent. Civil libertarians are greatly concerned about the sweeping nature of such laws. As one commentator pointed out,

> [u]nder this law, it would be a crime for a Quaker to send a book on Ghandi's theory of non-violence—a "physical asset"—to the leader

---

215. Laura A. White, Note, *The Need for Governmental Secrecy: Why the U.S. Government Must Be Able to Withhold Information in the Interest of National Security*, 43 VA. J. INT'L L. 1071, 1095-96 (2003).

216. *Id.*; Editorial, *The Danger of Leak Probes*, WASH. POST, Sept. 3, 2002, at A16.

217. Letter from John Ashcroft, Attorney General of the United States, to Congress and the President (Oct. 2002), *available at* http://www.fas.org/sgp/othergov/dojleaks.html (last visited Aug. 14, 2004).

218. 8 U.S.C.A. § 1182(A)(3)(B)(iv)(VI) (West Supp. 2002); 18 U.S.C.A. § 2339B (West 2000 & Supp. 2002). Commentators note that the "targeting of material support to terrorist organizations is the linchpin of the government's current war on terror." David Cole, *The New McCarthyism: Repeating History in the War on Terrorism*, 38 HARV. C.R.-C.L. L. REV. 1, 8 (2003); *see also* Nancy Chang & Alan Kabat, *Summary of Recent Court Rulings on Terrorism-Related Matters Having Civil Liberties Implications* 16-27 (Feb. 4, 2004) (listing prosecutions under the material support laws), *available at* http://www.ccr-ny.org/v2/reports/report.asp?ObjID=n7yKoAObvc&Content=324 (last visited Aug. 12, 2004).

219. 18 U.S.C.A. § 2339A(b) (West Supp. 2002).

> of a terrorist organization in hopes of persuading him to forgo violence. . . . Similarly, if this law had been on the books in the 1980s, the thousands of Americans who donated money to the African National Congress (ANC) for its lawful political struggle against apartheid would face lengthy prison terms, because during those years the ANC was designated as a terrorist organization by our State Department.[220]

The laws essentially punish individuals merely because of their association with certain groups regardless of the individual's lawful motives. Thus, critics liken the material support laws to Cold War era tactics, when government officials used lists of subversive organizations and prosecutions of their members to wipe out undesirable elements.[221]

Federal laws allowing prosecution of "domestic terrorism" have also been much criticized. The USA Patriot Act amended the existing definition of domestic terrorism to include, in addition to acts of violence normally associated with terrorism, any criminal activity within the United States that "involve[s] acts dangerous to human life, . . . ; appear[s] to be intended to intimidate or coerce a civilian population; [or] to influence the policy of a government by intimidation or coercion."[222] Critics have argued that such an expansive definition of domestic terrorism may result in suppression of legitimate dissent. As one commentator noted:

> Vigorous protest activities, by their very nature, could be construed as acts that "appear to be intended . . . to influence the policy of a government by intimidation or coercion." Further, clashes between demonstrators and police officers and acts of civil disobedience–even those that do not result in injuries and are entirely non-violent–could be construed as "dangerous to human life" and in "violation of criminal laws."[223]

Commentators are particularly concerned that organizations known for their aggressive protests—*e.g.*, anti-abortion, environmental, animal rights activists —might be subject to labeling as terrorist organizations.[224]

---

220. Cole, *supra* note 218, at 10.

221. *Id.* at 6-15.

222. Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act of 2001 § 802, 18 U.S.C. § 2331(5) (Supp. I 2003).

223. Nancy Chang, *The USA Patriot Act: What's So Patriotic About Trampling on the Bill of Rights?* 3 (2001), *available at* http://www.ccr-ny.org/v2/reports/docs/USA_PATRIOT_ACT.pdf (last visited Aug. 14, 2004).

224. John W. Whitehead & Steven H. Aden, *Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA Patriot Act and the Justice Department's Anti-terrorism Initiatives*, 51 AM. U. L. REV. 1081, 1093 (2002) ("Conceivably, these extensions of the definition of

In addition to the potential for censorship under new USA Patriot Act provisions, some reports indicate increased harassment of protestors and attempts to suppress criticism of the government's policies on terrorism and the war in Iraq. According to these reports, cities have denied or delayed permits for rallies, restricted protestors to areas far from public view, or harassed protestors with arrests and interrogations regarding political affiliations and prior protest activities.[225] Other officials have used their subpoena power to harass protestors, requiring them to testify before grand juries and requiring that organizations turn over membership lists of groups participating in peaceful protests.[226]

2. Indirect Censorship

The Bush administration has also engaged in acts of indirect censorship. In an effort to quash dissent, government officials have accused its critics of lack of patriotism. Thus, Attorney General John Ashcroft, in testimony before the Senate Judiciary Committee proclaimed that:

> We need honest, reasoned debate; not fearmongering. To those who pit Americans against immigrants, and citizens against non-citizens; to those who scare peace-loving people with phantoms of lost liberty; my

---

'terrorist' could bring within their sweep diverse domestic political groups which have been accused of acts of intimidation or property damage such as Act Up, People for the Ethical Treatment of Animals (PETA), Operation Rescue, and the Vieques demonstrators."); Sharon H. Rackow, Comment, *How the USA Patriot Act Will Permit Governmental Infringement Upon the Privacy of Americans in the Name of "Intelligence" Investigations*, 150 U. PA. L. REV. 1651, 1689 (2002) (noting that the definition of domestic terrorism "encompasses activities ranging from those of anti-abortion activists who use violence against women entering Planned Parenthood clinics, to World Trade Organization protesters who throw rocks through the windows of merchants and politicians who publicly support the WTO.").

225. *See generally* American Civil Liberties Union, *Freedom Under Fire: Dissent in Post-9/11 America* (2003), *available at* http://www.aclu.org/Files/OpenFile.cfm?id=12580 (last visited Aug. 14, 2004); Press Release, American Civil Liberties Union, ACLU of New Mexico Sues Albuquerque Police Over Mistreatment of Peaceful Protestors (Mar. 22, 2004), *available at* http://www.aclu.org/FreeSpeech/FreeSpeech.cfm?ID=15288&c=86 (last visited Aug. 14, 2004).

226. In a February 2004 incident in Iowa, for example, the U.S. attorney issued grand jury subpoenas to individual protestors who organized and attended an anti-war forum and related peaceful protest and to Drake University, in whose facilities the forum was held. The subpoenas were served by an official associated with the local anti-terrorism task force and ordered the protestors to testify before a grand jury regarding an unidentified law enforcement investigation. The subpoena to Drake University also requested that the university turn over all records concerning the National Lawyer's Guild, who had sponsored the forum, and any identities of persons attending the event. The local U.S. Attorney eventually withdrew the subpoenas after massive public outcry. *See* Leonard Post, *A Furor Over Iowa Subpoenas; Amid Howls of Protest, a U.S. Attorney Backs Down; Suits to Follow?*, NAT'L L.J., Feb. 16, 2004, at 4; Jeff Eckhoff & Mark Siebert, *U.S. Officials Drop Activist Subpoenas; Judge Lifts Drake Gag Order in Probe of Anti-war Protest*, DES MOINES REGISTER, Feb. 11, 2004, at 1, *available at* 2004 WL 60231472 (last visited Aug. 14, 2004).

> message is this: Your tactics only aid terrorists—for they erode our national unity and diminish our resolve. They give ammunition to America's enemies, and pause to America's friends. They encourage people of good will to remain silent in the face of evil.[227]

Private, right-wing organizations closely tied to the government also implied that critics of the Bush administration's war on terror were unpatriotic. The American Council of Trustees and Alumni, for example, published a report in November 2001, claiming that college faculty who criticized the Bush administration were the "weak link in America's response to the [September 11th] attack."[228] The report implied that liberal college faculty as a whole were out-of-step with American's otherwise patriotic response:

> While America's elected officials from both parties and media commentators from across the spectrum condemned the attacks and followed the President in calling evil by its rightful name, many faculty demurred. Some refused to make judgments. Many invoked tolerance and diversity as antidotes to evil. Some even pointed accusatory fingers, not at terrorists, but at America itself.[229]

The report further published an appendix with quotations attributed to identified faculty members, thus reaching into the realm of stigmatization so heavily relied upon during the Cold War years.[230]

The Bush administration has also apparently relied on propaganda as a tool of information control. Less than a month after the September 11th attacks, Attorney General John Ashcroft urged the Senate to adopt the Bush administration's proposals expanding its law enforcement powers, noting that

> [t]he American people do not have the luxury of unlimited time in erecting the necessary defenses to future or further terrorist acts. The danger that darkened the United States of America and the civilized

---

227. *DOJ Oversight: Preserving Our Freedoms while Defending Against Terrorism: Hearing Before the Senate Committee on the Judiciary*, 107th Cong. (2001) (statement of Attorney General John Ashcroft), *available at* 2001 WL 26188084 (last visited Aug. 14, 2004).

228. American Association of Trustees and Alumni, *Defending Civilization: How Our Universities are Failing America and What Can Be Done About It* 1 (2001), *available at* http://www.eecs.harvard.edu/~aaron/defciv.pdf (last visited Aug. 14, 2004). The organization is the brainchild of Vice President Cheney's wife, Lynne Cheney.

229. *Id.*; *see also id.* at 5 ("The fact remains that academe is the only sector of American society that is distinctly divided in its response").

230. *Id.* at 8-38.

> world on September 11 did not pass with the atrocities committed that day. Terrorism is a clear and present danger to Americans today.[231]

Reference to "clear and present danger"—language that strikes a cord with many Americans[232]—was a powerful rhetorical tool designed to spark fear and galvanize support for passage of the administration's proposed USA Patriot Act, which was then pending before Congress.

Assistant Attorney General Viet Dinh, the primary author of the USA Patriot Act, similarly relied on fear-inducing images of terrorists as monsters to galvanize support for expansion of government powers:

> [The] enemy we face [is] a criminal whose objective is not crime but fear; a mass murderer who kills only as a means to a greater end; a predator whose victims are all innocent civilians; a warrior who exploits the rule of war; a war criminal who recognizes no boundaries and who reaches all corners of the world. To confront this threat, the Department of Justice needed a fundamentally new paradigm, different from the way we approached the traditional task of law enforcement. Unlike traditional soldiers, terrorists wage war dressed not in camouflage, but in the colors of street clothing. Unlike traditional criminals, terrorists are willing to sacrifice their own lives in order to take the lives of innocents.[233]

In another setting, he argued:

> The enemy we confront is a multinational network of evil that is fanatically committed to the slaughter of innocents. Unlike enemies that we have faced in past wars, this one operates cravenly, in disguise. It may operate through so-called "sleeper" cells, sending terrorist agents into potential target areas, where they may assume outwardly normal identities, waiting months, sometimes years, before springing into action to carry out or assist terrorist attacks. And unlike garden-variety criminals the Department has investigated and prosecuted in the past, terrorists are willing to give up their own lives to take the lives of thousands of innocent citizens. We cannot afford to wait for them to execute their plans; the death toll is too high; the

---

231. *Hearing on "Homeland Defense" Before the United States Senate Comm. on the Judiciary*, 107th Cong. (2001) (testimony of Attorney General John Ashcroft), *available at* 2001 WL 1132689 (last visited Aug. 15, 2004).

232. Douglas Laycock, *The Clear and Present Danger Test*, 25 J. SUP. CT. HIST. 161 (2000).

233. Conference Proceedings, *Life After 9/11: Issues Affecting the Courts and the Nation*, 51 U. KAN. L. REV. 219, 222 (2003) (comments of Viet Dinh).

> consequences too great. We must neutralize terrorists before they strike.[234]

Such rhetoric harkens back to past crises in which executive officials described the victims of their actions as sly, devious and secretive puppets of foreign powers.[235] To be sure, terrorists do have many of the characteristics Dinh describes but that does not justify the government's actions. The government has been concerned about and asking for expanded law enforcement powers regarding terrorism since the 1970s, making it hardly the new and pressing threat that Dinh conjures. Thus, Dinh's characterization, while partly true, serves more to create an unthinking fearful response rather than to add neutral information to the public debate. Such is the purpose of propaganda and one rightly views these statements with a measure of skepticism.

Critics of the Bush administration have pointed out other incidents of potential propaganda. Some argue, for example, that the government's "Terror Alert" system—a color coded system designed to warn Americans regarding the terrorist threat level—is a propaganda tool.[236] Others have pointed to the Bush administration's attempts to galvanize support for the war on Iraq by claiming that Sadam Hussein had ties to Al-Quaeda and was developing weapons of mass destruction. As the war unfolded and information became available, many observers began to question the veracity of those statements, ultimately concluding that the Bush administration deliberately lied to win support for the war.[237] Finally, some observers have labeled Justice Department officials' tour of the United States to galvanize support for the USA Patriot Act as a disinformation campaign designed to quell criticism of government's expanded law enforcement powers.[238]

---

234. Viet D. Dinh, *Freedom and Security after September 11*, 25 HARV. J.L. & PUB. POL'Y 399, 400-401 (2002) (emphasis omitted).

235. *See supra* notes 82-88 and accompanying text.

236. After a flurry of terrorist warnings in December 2003 resulted in heightened anxiety, and delayed or rerouted international flights, but no arrests or detentions of terrorists, some people noted that the system was more effective as a tool for diverting public opinion from other administration actions than for warning citizens of possible danger. *See* Michael Chossudovsky, *Bush's Christmas Terror Alert*, Dec. 24, 2003, *available at* http://www.globalresearch.ca/articles/CHO312D.html (last visited Aug. 14, 2004). Aside from the propaganda argument, many critics of the terror alert system argue for its overhaul simply because it appears not to be working. Michael Isikoff & Mark Hosenball, No More Orange, Yellow and Red?, NEWSWEEK, Jan. 14, 2004, *available at* http://www.msnbc.msn.com/id/3959828/ (last visited Aug. 14, 2004).

237. Christopher Scheer et al., *Bush's Lies About Iraq*, THE NATION, Mar. 29, 2004, *available at* http://www.thenation.com/doc.mhtml?i=20040329&s=scheer (last visited Aug. 14, 2004); Richard Morin & Dana Millbank, *Poll Finds Distrust of Bush on Iraq*, BOSTON GLOBE, Feb. 13, 2004, at A26, *available at* 2004 WL 59771706 (last visited Aug. 14, 2004).

238. *See generally* American Civil Liberties Union, *Seeking Truth from Justice: Patriot Propaganda - The Justice Department's Campaign to Mislead the Public About the USA PATRIOT Act* (July 2003), *available at* http://www.aclu.org/Files/OpenFile.cfm?id=13098 (last visited Aug. 14, 2004).

C. Government Information Gathering

In the last few years the Bush administration has also expanded its surveillance and intelligence-gathering capabilities through amendments to FISA and executive initiatives.

In October 2001, at the behest of the Bush administration, Congress passed the USA Patriot Act which expanded the government's existing surveillance capabilities under FISA. Section 218 of the USA Patriot Act, for example, has eroded the wall between foreign-intelligence gathering and law enforcement erected under the earlier Act.[239] Under the USA Patriot Act amendments, the FBI can now obtain wiretaps under FISA standards (lower than probable cause) if they certify that the collection of foreign intelligence is a "significant purpose" of the investigation, rather than the "primary" purpose as required under the old standards.[240] This standard allows the FBI to evade traditional Fourth Amendment probable cause requirements simply by asserting that investigations at least partly have foreign intelligence purposes.[241]

Section 215 of the USA Patriot Act allows the government to obtain any "tangible thing" regarding any person if it certifies to the FISA Court that such items are "sought for" a foreign intelligence investigation.[242] The law explicitly forbids persons/entities producing such things from revealing that the FBI has sought them.[243] Section 215 has caused much controversy as its provisions vastly expand the government's authority to obtain library, bookstore, medical, and educational records regarding persons who are not involved in terrorist activities.[244] Prior to the amendment, the government could obtain only records pertaining to certain businesses and it had to certify to the FISA Court that it sought such information based upon "specific and

---

239. *See supra* notes 166-68 and accompanying text.

240. USA Patriot Act of 2001 § 218, 50 U.S.C. § 1804(a)(7)(B) (Supp. I 2003).

241. *See* Memorandum from Attorney General John Ashcroft to the Director of the FBI and other senior Justice Department officials on Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI (Mar. 6, 2002), *available at* http://www.fas.org/irp/agency/doj/fisa/ag030602.html (last visited Aug. 14, 2004) (noting that the USA Patriot Act "allows FISA to be used *primarily* for a law enforcement purpose, as long as a significant foreign intelligence purpose remains") (emphasis in original). For a more detailed explanation of USA Patriot Act § 218, see *Assessing the New Normal*, *supra* note 199, at 18-20.

242. USA Patriot Act of 2001 § 215, 50 U.S.C. § 1861.

243. *Id.*

244. For criticism of Section 215, see Kathryn Martin, Note, *The USA Patriot Act's Application to Library Patron Records*, 29 J. LEGIS. 283 (2003); *Assessing the New Normal*, *supra* note 199, at 17; American Civil Liberties Union, *Unpatriotic Acts: The FBI's Power to Rifle Through Your Records and Personal Belongings Without Telling You* 2-9 (2003), *available at* http://www.aclu.org/Files/OpenFile.cfm?id=13245 (last visited Aug. 14, 2004) [hereinafter *Unpatriotic Acts*].

articulable facts" that the target of the order was an agent of a foreign power.[245]

Amendments under the USA Patriot Act and the Intelligence Authorization Act for Fiscal Year 2004 also expand the government's ability to issue "national security letters" to obtain certain information regarding U.S. citizens.[246] Prior to the amendments, the FBI could use national security letters in foreign intelligence investigations to obtain records from financial institutions (banks, credit unions, etc.) if there were "specific and articulable facts" giving reason to believe that the person about whom records were sought was an agent of a foreign power. The amendments, however, allow the government to obtain information about any person simply by certifying that it is "sought for" foreign intelligence purposes.[247] Moreover, they broaden the definition of financial institution to include securities dealers, travel agencies, automobile rental companies, pawn brokers, and jewelers.[248] As with Section 215 of the USA Patriot Act, persons receiving the letters cannot reveal that such records have been requested.[249] Furthermore, national security letters are not subject to oversight of the FISA court, instead issuing simply upon the FBI's certification.[250] As critics have noted, such an expansion allows the government to obtain any record (not simply financial records as originally contemplated) from a vast array of businesses about persons who are not suspected of terrorist activities.[251] Evidence suggests that the FBI has aggressively used this power.[252]

In addition to legislative expansion of powers, the Bush administration also undertook several initiatives to enhance its intelligence-gathering power. Most significantly, Attorney General Ashcroft revised FBI guidelines regarding domestic intelligence investigations. The new guidelines specifically allow the FBI to gather information from a wide variety of sources even

---

245. For an explanation of the amendments, see *Assessing the New Normal*, *supra* note 199, at 17.

246. USA Patriot Act of 2001 § 505(b), 12 U.S.C. § 3414(a)(5)(A); Intelligence Authorization Act for Fiscal Year 2004 § 374, 12 U.S.C.A. § 3414(d) (West Supp. 2004).

247. USA Patriot Act of 2001 § 505(b), 12 U.S.C. § 3414(a)(5)(A).

248. Intelligence Authorization Act for Fiscal Year 2004 § 374, 12 U.S.C. § 3414(d).

249. 12 U.S.C. § 3414(a)(3).

250. *Id.* § 3414(a)(5)(A).

251. *Unpatriotic Acts*, *supra* note 244, at 13; Kim Zetter, Bush Grabs New Power for the FBI, WIRED NEWS, JAN. 6, 2004, *available at* http://www.wired.com/news/print/0,1294,61792,00.html (last visited Aug. 14, 2004).

252. An FBI memo obtained by the ACLU reflects that the FBI has used national security letters on numerous occasions since the 9/11 attacks. Federal Bureau of Investigation, Transactional Records NSLs since 10/26/2001, *available at* http://www.aclu.org/patriot_foia/FOIA/NSLlists.pdf (last visited Aug. 16, 2004). For further explanation see Press Release, American Civil Liberties Union, Documents Show Ashcroft is Bypassing Courts With New Spy Powers, ACLU Says (Mar. 24, 2003), *available at* http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12166&c=206 (last visited Aug. 16, 2004).

if it is not engaged in a preliminary or full investigation. They allow FBI officials to surf the Internet, use commercially available data-mining services, and attend public meetings held by various organizations in order to gather information.[253] Ashcroft claimed that such changes were necessary because the previous guidelines unreasonably restricted the FBI's ability to engage in lawful surveillance activities.[254] As critics pointed out, however, the FBI was always able to use data-mining services, the Internet and surveillance of public meetings when they had some suspicion of potential criminal activity. The new guidelines allow the FBI to engage in such actions in order to dredge up possible activity, effectively putting no limits on the FBI's ability to gather intelligence about lawful political organizations.[255] That the new guidelines substantially lengthen the time for preliminary and full investigations without significant oversight and expand the FBI's investigative techniques exacerbates this problem.[256]

In the summer of 2002, the Bush administration proposed Operation TIPS ("Terrorism Information and Prevention System").[257] Recalling tactics used during World War I and the Cold War, the program was designed to recruit average Americans, such as utility workers, postal workers or delivery persons, to report "suspicious activity" observed while in homes and businesses.[258] After

253. The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations § VI(A)-(B) (2002), *available at* http://www.usdoj.gov/olp/generalcrimes2.pdf (last visited Aug. 16, 2004) [hereinafter Ashcroft Guidelines].

254. Department of Justice, Fact Sheet—Attorney General's Guidelines: Detecting and Preventing Terrorist Attacks 1, *available at* http://www.cdt.org/security/usapatriot/020530ag-guidelines.pdf (last visited Aug. 16, 2004).

255. *See, e.g.*, Electronic Privacy Information Center, The Attorney General's Guidelines, *available at* http://www.epic.org/privacy/fbi/ (last visited Aug. 16, 2004).

256. The new guidelines allow preliminary investigations for up 180 days (with two 90 day extensions) without obtaining approval from FBI headquarters. Ashcroft Guidelines, *supra* note 253, § II(B)(3). Previous guidelines allowed only 90 day investigations without prior approval from FBI headquarters. *See* Thornburg Guidelines, *supra* note 190, § II(B)(3). The new guidelines, while still prohibiting mail openings and electronic surveillance in preliminary investigations, now permit mail covers, and further encourage FBI agents to use "any lawful techniques . . . even if intrusive, where the intrusiveness is warranted in light of the seriousness of the crime. Ashcroft Guidelines, *supra*, at § II(B)(4). In contrast the old Guidelines admonished FBI agents to "consider whether information could be obtained in a timely and effective way by less intrusive means." Thornburg Guidelines, *supra*, § II(B)(4). The new guidelines similarly lengthen the time for full investigations. *Compare* Ashcroft Guidelines, *supra*, § III(B)(4) *with* Thornburg Guidelines, *supra*, § III(B)(4)(b).

257. Dan Eggan, *Proposal to Enlist Citizen Spies Was Doomed from Start*, WASH. POST, Nov. 24, 2002, at A11, *available at* 2002 WL 103571596 (last visited Aug. 16, 2004).

258. Eric Lichtblau, *Terrorism Tip Network Scaled Back Surveillance: Workers With Access to Homes Won't Use New Hotline, Justice Department Says*, L.A. TIMES, Aug. 10, 2002, at A1, *available at* 2002 WL 2495625 (last visited Aug. 16, 2004).

significant public outcry, however, Congress banned implementation of the system.[259]

In November, 2002, the Department of Defense announced another experimental surveillance initiative, titled "Total Information Awareness." The program's purpose was to "determine the feasibility of searching vast quantities of data to determine links and patterns indicative of terrorist activities."[260] Intended to allow mining of numerous computer databases with information pertaining to passports, visas, work permits, driver's licenses, credit cards, airline tickets, rental cars, chemical purchases, and gun purchases,[261] the program would have provided law enforcement and intelligence officials with instant access to such information without a search warrant. In response to public criticism, the Defense Department renamed the project the "Terrorism Information Awareness" program and replaced the project's controversial director, Admiral John Poindexter. The program remained in place until the Senate blocked its funding in October, 2003.[262]

Other proposed programs have also caused some concern. Critics of the government's CAPSII program, an airline passenger profiling system designed to identify individuals connected to international terrorism, argue that it is ill-defined, allowing airlines to label as security risks people associated with purely domestic groups, allows information to be shared too freely, and provides little recourse for individuals who are wrongly labeled.[263] Other observers have noted that, reminiscent of 1960s abuses, military intelligence is becoming more involved in domestic law enforcement.[264]

III. CONCLUSION

What are we to think of the Bush administration's actions in light of the historical pattern described in Section I? The results of a purely comparative perspective are mixed. The Bush administration's actions with respect to control of public information, for example, have yet to reach the level of past government actions. The government's reliance on direct censorship, propa-

---

259. 6 U.S.C.A. § 460 (West Supp. 2004).

260. Alexander Cockburn, *Total Information, Total Confusion*, THE NATION, Dec. 16, 2002, at 9 (quoting Under Secretary of Defense for Acquisition, Edward Aldridge), *available at* 2002 WL 2211090 (last visited Aug. 16, 2004).

261. *Id.*

262. Robert Block & Gary Fields, *Is Military Creeping into Domestic Spying and Enforcement?*, WALL STREET J., Mar. 9, 2004, at B1, *available at* 2004 WL 56922304 (last visited Aug. 16, 2004).

263. *Assessing the New Normal, supra* note 199, at 24-26; Letter from various civil liberties groups to Congressman Don Young (Feb. 17, 2004), *available at* http://www.cdt.org/security/usapatriot/20040217 cappsii.pdf (listing shortcomings of CAPS II and requesting congressional hearings) (last visited Aug. 16, 2004).

264. Block & Fields, *supra* note 262.

ganda, and stigmatization during World War I and the Cold War were far more onerous and widespread than the current administration's. This is not to imply that the Bush administration's attempts to criminalize certain forms of expression or to coerce public sentiment are without problems. But they have not yet been applied in as widespread or arbitrary a manner as past incidents.

The Bush administration's actions regarding surveillance are harder to assess as there is little available information regarding the administration's actual use of them. Certainly, however, the administration has proposed intrusive surveillance operations, including enlistment of public citizens—a situation that caused much abuse in past incidents. Moreover, evolving technology allows potentially far-reaching surveillance operations unlike anything seen during past crises. The lack of enforceable legal restrictions on such surveillance, combined with the government's roll back of voluntary restrictions resulting from past reform efforts, cause additional concern.

The Bush administration's actions with respect to secrecy are of great concern. Numerous commentators have noted that the Bush administration's "penchant for secrecy" exceeds any past administrations.'[265] Far more information, including routine material, has been withheld from public disclosure out of "national security" concerns. The administration's attempts to blockade public access to information are as or more vigorous than any previous administrations'. The Bush administration's actions are more worrisome as its secrecy is the primary source of difficultly in assessing the administration's intelligence-gathering activities, a power historically subject to abuse.

This relationship between the Bush administration's secrecy and its potential abuse of intelligence activities highlights a significant point regarding the government's tools of information control. Although we tend to think of and discuss these tools separately, historically they compliment one another in a way that often leads to abuse. The FBI's abuse of its intelligence-gathering power, for example, could not have occurred without control of confidential and public information. Secrecy associated with the "national security" rationale extended far beyond issues of legitimately classified information, to become a "culture of secrecy"[266] that protected many government actions from scrutiny, including the FBI's extensive surveillance network. That "culture of secrecy" was either accepted or unquestioned because the government controlled public information by (1) engaging in extensive propaganda

265. *See, e.g.*, David E. Rosenbaum, *The World: Top Secret; When Government Doesn't Tell*, N.Y. TIMES, Feb. 3, 2002, § 4, at 1; Mark Tapscott, Editorial, Too Many Secrets, WASH. POST, Feb. 20, 2002, at A25, *available at* 2002 WL 102573378 (last visited Aug. 16, 2004).

266. *Secrecy Report*, *supra* note 1, at A41-A63.

campaigns regarding the FBI's important mission,[267] or (2) stigmatizing individuals with different views essentially coercing them into silence.[268] The government also controlled public information by selectively leaking information it found helpful for the public to know and burying or punishing publication of information under a "national security" rationale that detracted from its actions.[269] Thus, the FBI's illegal intelligence-gathering continued because Hoover had firm control over all levels of information. That the Bush administration also apparently desires to control all levels of information is cause for concern in light of past events.

This concern is not allayed by the fact that some of the Bush administration's expanded powers are not yet as expansive as in the past or are merely small incremental changes to already-existing powers. The historical pattern of information control and abuse described above rarely resulted from radical changes in government practices. Rather, abuse of government power usually resulted from incremental change. Excessive secrecy in the name of national security came about as a result of incremental changes in executive orders and administration practice. The government's abuse of surveillance reflected an ebb and flow, with government officials extending their power too far, retrenching, and then slowly expanding again over time. That such change is incremental is precisely why it is so dangerous.

The practice of implementing small changes all tending towards secrecy, instead of taking dramatic steps to restrain access, makes it harder to evaluate the impact and, indeed, to fight the changes. It is, undoubtedly, more difficult to garner public support for opposition to minor changes when more pressing issues, like an impending war, are competing for public attention.[270] Thus, it behooves the public to pay attention to even the smallest changes in government power.

The Bush administration's fight against terrorism and other national security threats is sure to be ongoing, as it evolves, so too will the tools it employs. In order to protect against the abuse so often historically present, the public must watch both the larger pattern of information control and its evolution.

---

267. DONNER, *supra* note 103, at 90-96.

268. *See supra* notes 96-102 and accompanying text.

269. For a general discussion of this phenomenon, see White, *supra* note 215, at 1100.

270. *National Security Archive, The Ashcroft Memo*, *supra* note 205, at 28.