LAW AND POLICY EFFORTS TO BALANCE SECURITY, PRIVACY AND CIVIL LIBERTIES IN POST-9/11 AMERICA

U.S. Senator Ron Wyden

with Carol Guthrie, John Dickas, and Alexander Perkins

INTRODUCTION: THE FIGHT BETWEEN SECURITY AND CIVIL LIBERTIES

Of the many hard realizations Americans were forced to absorb after September 11, 2001, one of the most maddening was this: that the treasured openness of our society, with its rights to privacy and its freedom to move and assemble at will, had helped terrorists to strike on our own soil and claim thousands of innocent victims.[1] Since 9/11 violently catapulted domestic security to the fore of the federal government's priorities,[2] one of the chief battles of the war on terrorism has been with ourselves, determining to what extent rights and freedoms will be curbed in an effort to save lives.

Properly navigating security and civil liberties in the post-9/11 world with any success requires abandonment of the prevailing either-or paradigm in which security can be enhanced or privacy preserved, but not both. The new reality thrust upon the United States must not be met simply with heightened vigilance on both "sides" of a stark equation. Those who bear the responsibility to put security first must understand that if civil liberties are not prominent among their concerns, their efforts may diminish the uniquely American freedoms they seek to protect. But in the same way, those who prize and vigorously defend civil liberties must do so with the recognition that a proliferation of security failures and terrorist success would diminish Americans' true freedom to a degree beyond any law. To ensure the safety and liberty of all Americans, advocates and policymakers must agree to a basic premise: the security of the nation and the protection of individual freedoms are not, and must not be drawn as, mutually exclusive.

1. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 383-398 (2004) [hereinafter 9/11 REPORT].

2. *Id.* at 361- 65.

This article is not intended to offer a comprehensive detailing of national security, privacy, and civil liberties law and policy, but rather to provide a view of key episodes and themes in the effort to strike an appropriate balance among these equally compelling interests. It is my firm sense that the United States can fight terrorism aggressively without cannibalizing fundamental freedoms in the process—but challenges abound. The thorny reality is that from expanded governmental authority to new technologies, from information-sharing to classification, every necessary aspect of fighting terror at home has the potential to undermine essential rights. As British Home Secretary Charles Clarke said after the London transit bombings of July 2005, "every intelligence question is also a civil liberties question."[3]

LIBERTY OR SAFETY: THE USA PATRIOT ACT

In the days of shock that followed the attacks on the World Trade Center, the Pentagon, and the crash of United Airlines Flight 93 in Shanksville, Pennsylvania, the United States Congress agreed to a number of immediate changes to existing law. Placing security measures above all other considerations, Congress passed sweeping legislation that transformed immigration, criminal justice, domestic and international finance, and, of course, domestic surveillance law, in some cases granting the government powers that had been expressly rejected before.

The votes to approve the USA PATRIOT Act (the Patriot Act)[4] took place four weeks after the 9/11 attacks. The measure passed by a resounding 357-66 vote in the House of Representatives,[5] and an even more declarative 98-1 vote in the Senate.[6] Many who voted for this legislation, including myself, did so with serious concerns regarding its implications on privacy and civil liberties. But many of us voted for the bill with the knowledge that immediate changes were necessary to fight a terrorist threat now clearly active inside America's borders, the scope and capabilities of which were frighteningly unknown.

Of all the rhetoric bandied about before and after the law's approval, none seemed so apropos as Benjamin Franklin's warning that "[t]hose who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."[7] Before 9/11, that postulate seemed irrefutable. When Americans did not know that terrorists were living in nearby apartment

3. *Britain Wins E.U. Vows of Joint Counter-terror Action*, DEUTSCHE PRESSE-AGENTUR, July 13, 2005.

4. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of the U.S.C.).

5. 147 CONG. REC. H7224 (daily ed. Oct. 24, 2001) (Roll No. 398).

6. 147 CONG. REC. S11, 059-60 (daily ed. Oct. 25, 2001) (Roll No. 313).

7. BENJAMIN FRANKLIN, THE PAPERS OF BENJAMIN FRANKLIN 242 (Leonard W. Labaree ed., Yale Univ. Press 1963).

buildings, enrolling in local flight schools, and eating in local restaurants,[8] the idea of new privacy incursions for the sake of law enforcement was plain anathema to policymakers, and the application of those curbs to fighting terrorism was mostly unconsidered.

For instance, Congress took up the notion of delayed notice search warrants in 2000, but the idea was proposed in the context of counternarcotics rather than counterterrorism. An anti-methamphetamine bill sponsored by then-Senator John Ashcroft included a controversial provision that would have permitted the Federal Bureau of Investigation (FBI) or other law enforcement agencies to delay indefinitely notice of the execution of a search warrant, making it possible to search someone's home without his knowledge, and without telling him even after the search was conducted.[9] Although the Senate agreed to the legislation,[10] the delayed-notice provision was not included in the House version of the bill,[11] and the two versions were not reconciled.[12] An attempt was later made to attach the version that included delayed-notice warrants as a rider to an unrelated bill, but this effort also failed.[13]

After September 11th, of course, the policy dynamic changed dramatically—and so did prospects for the kind of law enforcement powers that Ashcroft, who had then become Attorney General of the United States, had favored in the past. When the Patriot Act sailed through Congress in the fall of 2001, the authority for delayed-notice search warrants was simply the tip of the iceberg; most of its provisions to expand government powers remained submerged and largely unacknowledged in the 151-page bill.

Section 206 of the Patriot Act authorized the FBI to use roving wiretaps in national security investigations.[14] Roving wiretap authority allows the FBI to tap not just a particular phone, but any phone that the person being targeted might use.[15] Unlike in criminal investigations, Section 206 did not require the FBI to ascertain that the person being investigated was using the line.[16] If a suspected terrorist worked in a warehouse, roving wiretap authority could be used to tap the pay phone in that warehouse, and every person who used that

8. 9/11 REPORT, *supra* note 1, at 215-53.

9. S. 486, 106th Cong. § 6(a) (as reported to the Senate, August 5, 1999).

10. S. 486, 106th Cong. § 301 (as passed by the Senate with an amendment by unanimous consent, November 19, 1999).

11. H.R. 2987, 106th Cong. (as introduced by the House, September 30, 1999).

12. H.R. 2987, 106th Cong. (as placed on Union Calendar No. 529, Sept. 21, 2000); S. 486, 106th Cong. (as referred to the S. Comm. on Health and Environment, Feb. 4, 2000).

13. *See* CONG. REC. S14439 (daily ed. Nov. 10, 1999) (Roll No. 360) (amending Bankruptcy Reform Act of 1999, S. 625, to include Methamphetamine Anti-Proliferation Act of 1999, S. Amdt. 2771); H.R. 833, 106th Cong. (as the Senate insisted on its amendment request, Feb. 2, 2000).

14. USA PATRIOT Act, *supra* note 4.

15. USA PATRIOT Act § 206, 50 U.S.C. § 1805 (2006).

16. *Id.*

phone could have their conversation secretly recorded.

Section 215 of the Patriot Act is often known as the "library records" provision, but this misnomer obscures its scope. It modified the Foreign Intelligence Surveillance Act (FISA) to make it easier to obtain warrants from the Foreign Intelligence Surveillance Court for "records" and other items.[17] Prior to the Patriot Act, FBI agents who wished to obtain records held by a third party were required to present "specific and articulable facts" indicating that the person to whom the records pertained was an agent of a foreign power—a terrorist or a spy.[18] Section 215 lowered the standard to let the Bureau simply assert that the records are "sought for an investigation to protect against international terrorism . . . ."[19] It also expanded the scope of warrants from "records" to "any tangible item."[20] This made it possible for FBI agents to obtain a secret warrant to seize not only library records, but also medical records, tax records, video rental transactions—essentially anything at all—simply by claiming some relevance.

The FBI's ability to access this information was doubly expanded through sections that broadened the use of national security letters.[21] Unlike FISA warrants, national security letters do not even require the approval of a judge to obtain financial, telephone, and credit records.[22] The FBI has said that national security letters can be appealed, but the law does not specifically discuss this possibility.[23] In fact, the law bars the recipient of a national security letter from discussing it with anyone, even an attorney, making it nearly impossible for recipients to learn about their rights to appeal.[24] In the 2004 case of *Doe v. Ashcroft*, a federal judge found that the FBI had abused its authority by using a national security letter to demand records from an Internet service provider, without giving the provider company notice of its right to challenge the letter or to obtain legal counsel.[25]

In several places in the Patriot Act, wording that first appears to safeguard civil liberties may in fact expose Americans to unfair scrutiny when they exercise their rights. The law repeatedly prevents the use of various investigative techniques when the investigation is "based solely on the First Amendment activities" of U.S. persons.[26] However, U.S. Senator Carl Levin

17. *Id.* § 215, 50 U.S.C. § 1861 (2006).

18. *See* 18 U.S.C. § 1862(b)(2), *amended* by § 215 of the USA PATRIOT Act.

19. USA PATRIOT Act § 215, 50 U.S.C. § 1861 (2006).

20. *Id.*

21. *Id.* §§ 358, 505, 12 U.S.C.§ 3414 (2006); 15 U.S.C. §§ 1681u, 1681v (2006); 18 U.S.C.§ 2709 (2006), *invalidated by* Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

22. *Id.*

23. Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

24. USA PATRIOT Act §§ 358, 505, 12 U.S.C. § 3414 (2006); 15 U.S.C. §§ 1681u, 1681v (2006); 18 U.S.C. § 2709 (2006), *invalidated* by Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

25. *Doe*, 334 F. Supp. 2d at 494.

26. *See, e.g.*, 50 U.S.C. § 1842(a)(1), (c)(2) (2006); 50 U.S.C.A. § 1843(a), (b)(1)

has wisely noted the troubling implications of the word "solely," and the possible indication that it is now permissible to investigate Americans *largely*, or even *primarily* on the basis of their First Amendment activities.[27] Revelations in the summer of 2005 that the FBI had compiled files on numerous activist groups, including the American Civil Liberties Union and Greenpeace, only engendered further concerns.[28]

The bill presented to Congress in the fall of 2001 did acknowledge the need to consider the effect of new government powers on privacy and civil liberties. Notably, it made it possible for citizens to file civil suit against the government for violations of laws regarding wiretapping, pen registers, and communications and e-mail records.[29] These abuses were considered federal crimes before passage of the Patriot Act, but it was not previously possible for the victims of these offenses to collect damages from the government.[30] The new law also mandated that agencies whose employees are involved in privacy violations must either initiate disciplinary action, or explain to their Inspectors General why no action would be taken.[31]

The Patriot Act also specifically instructed the Inspector General of the Department of Justice to designate an official who would "review information and receive complaints alleging abuses of civil rights and civil liberties by employees and officials of the Department of Justice."[32] The Inspector General's office complied with this instruction by establishing a special section of its investigations office to handle such complaints.[33] Congress took this protection a step further in 2004, recognizing that because of the secrecy involved, individuals would be unlikely to know that their rights had been violated. The Intelligence Reform and Terrorism Prevention Act of 2004 created an independent board to consider and investigate privacy and civil liberties concerns, and oversee adherence to laws and guidelines designed to safeguard the privacy of individuals.[34] The Board has unfortunately not yet

(2006); 50 U.S.C. § 1861 (a)(1), (a)(2)(B) (2006); 18 U.S.C.A. § 2709 (b)(1-2) (2006); 12 U.S.C.§ 3414(a)(5)(A) (2006); 15 U.S.C. § 1681u(a-c) (2006).

27. *U.S. Senate Select Committee on Intelligence Holds a Hearing on the USA Patriot Act*, 109th Cong. (2005) (statement of Sen. Levin, Vice-Chairman, S. Select Comm. on Intelligence).

28. Mark Sherman, *FBI Says it Has Files on Rights Groups*, AP NEWSWIRES, July 18, 2005.

29. USA PATRIOT Act § 223, 18 U.S.C. §§ 2520, 2707, 2712 (2006).

30. CHARLES DOYLE, THE USA PATRIOT ACT: A LEGAL ANALYSIS (Cong. Research Serv. 2002).

31. USA PATRIOT Act § 223, 18 U.S.C.§§ 2520(f), 2707(d), 2712(c) (2006).

32. Inspector General Act of 1978, 5 U.S.C.A. app. 3 § 8E (West 2006).

33. U.S. Dep't of Justice, How to Report a Complaint about [sic] Violation of your Civil Rights or Civil Liberties by a Department of Justice Employee, http://www.usdoj.gov/oig/FOIA/hotline2.htm (last visited Mar. 14, 2006).

34. Intelligence Reform and Terrorism Prevention Act of 2004 § 1061, 5 U.S.C. § 601 (2006).

demonstrated its effectiveness, as the Administration was slow to nominate and appoint its members, and has provided it with little budgetary support.[35] The intent of Congress is clear nonetheless.

The final safeguard in the Patriot Act was the sunset provision applied to some of the law's most controversial provisions.[36] These sixteen sunset provisions set expiration dates on portions of the law that were recognized as being particularly sweeping—or particularly susceptible to abuse—so the provisions' impact on privacy and civil liberties could be fully considered at reauthorization in 2005.[37]

When the time came for the reauthorization debate, questions of security, privacy and civil liberties were no closer to being answered. In fact, distance from the attacks of 9/11 made the Patriot Act's proper resolution less clear. The benefits of calm, hindsight, and case law prompted many members of Congress to seek greater balance between protecting Americans' security and protecting their privacy rights and civil liberties. The certain persistence of the terrorist threat and the specter of possible subsequent attacks on U.S. soil pointed others toward even stronger government powers to investigate and stop extremist violence.

Proposals to strengthen privacy protections in a renewed Patriot Act ranged from raising the standards for FISA warrants—adding requirements, for instance, that the FBI explain why records would be relevant instead of simply stating that they are, and creating higher hurdles for obtaining credit or medical records—to increased reporting requirements for some provisions to expose any pattern of abuse. Making individuals' rights clear under the law—for instance, in the case of national security letters—was considered a common-sense step. The "sunset" issue also figured prominently in efforts to safeguard privacy, whether that meant allowing controversial provisions to expire or setting end dates for additional provisions of the law.

Sunset provisions, however, also provided an opportunity for those who wished to expand the Patriot Act's power. Those who favored greater investigative authority, or who felt that concerns regarding privacy were overstated, seized upon the reauthorization debate to argue for greatly expanded authorities. Perhaps the most notable action taken by the Senate Select Committee on Intelligence (SSCI) in its reauthorization bill was the simple striking of the original law's sunset provisions. That move, echoed at least in part by the House Judiciary Committee, the House Permanent Select Committee on Intelligence, and the Senate Judiciary Committee as they considered their own versions of Patriot Act reauthorization, would

35. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, BUDGET OF THE UNITED STATES GOVERNMENT, FISCAL YEAR 2006 (2005).

36. USA PATRIOT ACT § 224, 18 U.S.C.§ 2510 (2005).

37. *See* 147 Cong. Rec. S10990 - S10992 (daily ed. Oct. 25, 2001) (Statement of Sen. Patrick Leahy).

permanently codify some of the Act's most debated authorities.[38]

Additional proposals would have expanded those powers even further. In the Intelligence Committee's debate, a number of senators suggested giving the FBI authority to write its own administrative subpoenas for foreign intelligence investigations.[39] This change would have dramatically increased federal investigative power and undermined the accountability created by the FISA Court warrant process, which requires agents to go before a judge and explain why the information is relevant, in the most general terms, to a terrorism or espionage investigation.[40] Indeed, giving the FBI administrative subpoena power to obtain credit records, video rentals, medical records, gun purchases and other information would remove the last judicial safeguard between the government and Americans' personal data. For instance, the head of a local FBI field office could subpoena every medical record at a hospital in his jurisdiction simply by claiming that the records were relevant to an investigation. A judge would only see the subpoena if the hospital director were properly notified of his or her rights and lodged a successful legal challenge.[41] Otherwise, if the FBI invoked its authority to prohibit the recipient of a subpoena from discussing it with anyone other than legal counsel, the records would be turned over and patients would never know of the seizure.[42]

Proponents of administrative subpoena power in a new Patriot Act attributed their concerns to the time required to complete FISA warrant requirements in time-sensitive emergency situations and not to the fact that existing tools precluded the government from obtaining information that it might need.[43] In light of this reasoning, it was unclear why an amendment creating a FISA business warrant emergency-use provision and an amendment imposing an emergency-use requirement on the administrative subpoena authority failed on party-line votes during the Senate Select Committee on Intelligence mark-up.[44]

It is important to note, however, that partisan politics did not dictate support for or opposition to administrative subpoenas across the Congress. Just weeks after the Senate Intelligence Committee finished drafting its version of

---

38. H.R. REP. NO. 109-174, pt. 2, at 1-2, 7 (2005); S. 1389, 109th Cong. §§ 1(b), 9 (2005).

39. S. SELECT COMM. ON INTELLIGENCE, REPORT ON A BILL TO PERMANENTLY AUTHORIZE CERTAIN PROVISIONS OF THE USA PATRIOT ACT, S. REP. NO. 109-85, (2005); S. 1266, 109th Cong.§ 213 (2005).

40. USA PATRIOT Act § 215, 50 U.S.C. §§ 1861(a)(1)-(2) (2005).

41. *Id.*

42. *Id.*

43. *Hearing on the Reauthorization of the USA PATRIOT Act of 2001 Before the S. Select Comm. on Intelligence*, 109th Cong. (2005) (statement of Valerie Caproni, FBI General Counsel) ("To stay a step ahead of the terrorists, investigators need tools allowing them to obtain relevant information as quickly as possible.").

44. *See* S. REP. NO. 109-85 (2005).

reauthorization legislation, the House Judiciary Committee and the House Permanent Select Committee on Intelligence, and then the full House, approved a different version.[45] That bill was a much more straightforward reauthorization of the Patriot Act, and while it did not include many new safeguards, it also lacked any expansion of surveillance authority whatsoever.[46] The Senate Judiciary Committee's bill went further to include substantial new safeguards for privacy and civil liberties and did not contain any administrative subpoena authority. That legislation was approved by the committee and adopted by unanimous consent in the Senate on July 29, 2005.

The House of Representatives approved its version of the reauthorization on July 21, 2005.[47] However, the conference to reconcile the House and Senate versions of the bill did not get underway until mid-October.[48] Once negotiations began, Democrats were afforded little opportunity to provide input,[49] and even before the report was formally issued, its content was met with hostility from Democrats *and* Republicans in the Senate.[50] When the conference report was finally issued, the opposition remained steadfast and soon announced it would filibuster.[51]

The House of Representatives passed the conference report on December 14, 2005.[52] On the eve of the Senate cloture vote to end debate on the report, the *New York Times* reported that after September 11th, under the authority provided by a secret executive order, the National Security Agency (NSA) began wiretapping the phone calls of Americans without first obtaining a warrant.[53]

Almost inevitably, the issues raised by that wiretapping story—the balance between security and civil liberties, and the accountability of the executive branch—influenced the Patriot Act reauthorization conference report cloture

45. 151 CONG. REC. H6308-09 (daily ed. July 21, 2005) (Roll No. 414) (recording 214 Republicans and 43 Democrats voting "yae" and 14 Republicans and 156 Democrats voting "nay").

46. H.R. REP. NO. 109-174, §§ 1-2 (2005).

47. H.R. 3199, 109th Cong. (2005).

48. Michael Sandler, *Conferees Whittle Down Differences Over Renewing Provisions of Act*, CQ TODAY, Nov. 10, 2005.

49. Michael Sandler, *Mood Sours Among Democrats in Conference Over Patriot Act Extensions*, CQ TODAY, Nov. 15, 2005.

50. *See* Press Release, Senators Durbin, Feingold, Salazar, Murkowski, Craig, and Sununu, Safe Act Co-Sponsors Say PATRIOT Act Conference Report Unacceptable (Nov. 16, 2005), *available at* http://murkowski.senate.gov/pressapp/record.cfm?id=248955.

51. *See* Charles Babington & Dan Eggen, *GOP Accepts Deal on Patriot Act: Hill to Vote Next Week on Extending Provisions for 4 Years*, WASH. POST, Dec. 9, 2005, at A4; *see also* Press Release, Wyden To Oppose Patriot Act Renewal (Dec. 14 , 2005), *available at* http://wyden.senate.gov/media/2005/12142005_oppose_patriot_act.html.

52. 151 CONG. REC. H11543 (daily ed. Dec. 14, 2005) (Roll No. 627) (recording 251 "yae" votes and 174 "nay" votes).

53. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

vote debate.[54] Indeed, one could argue fairly easily that the story played an instrumental role in ensuring the success of the filibuster by members of the Senate.[55]

After the successful filibuster of the Patriot Act reauthorization, a majority of Senate Democrats and Republicans proposed a three-month extension of the existing law while members pursued a compromise.[56] After first vociferously opposing the idea, the Republican leadership and the White House eventually agreed to a one-month extension.[57] A second extension of the original Patriot Act was passed in late January 2006, allowing deliberations concerning the reauthorization to continue.[58]

Soon after the passage of the second extension, Senator John Sununu, one of the four Republicans who supported the filibuster of the conference report, introduced a separate bill intended to bolster civil liberties protections neglected by the report.[59] However, the improvements were limited. For instance, while the Sununu bill provided for judicial review of the gag orders placed on recipients of Section 215 business record orders, review could only occur a year after receipt of the Section 215 order.[60] Additionally, to succeed, the recipient would have to prove that the government had acted in bad faith.[61] Despite the deficiencies, the remaining three Republicans who had supported the filibuster in December, along with a number of Democrats, expressed support for the Sununu bill.[62]

A final effort, spearheaded by Senator Russ Feingold, was made to further strengthen the Patriot Act reauthorization's civil liberties protections. Senator Feingold proposed amending the Sununu bill and adding a four-year sunset on

54. *See, e.g.*, CONG. REC. S.13708 (daily ed. Dec. 16, 2005) (statements of senators Daniel Akaka, Edward Kennedy, Russell Feingold and Ken Salazar).

55. *See* Sheryl Gay Stolberg & Eric Lichtblau, *Senators Thwart Bush Bid to Renew Law on Terrorism*, N.Y. TIMES, Dec. 17, 2005, at A1.

56. S. 2082, 109th Cong. (2005); *see also* Letter from fifty-two senators to Senate Majority Leader Bill Frist (Dec. 21, 2005), *available at* http://leahy.senate.gov/press/200512/122105.html; *see also* S. 2082, 109th Cong. (2005).

57. S. 2167 109th Cong. (2005) (enacted); *see* Laurie Kellman, *House OKs Five-Week Patriot Act Extension*, ASSOC. PRESS, Dec. 22, 2005; Reuters, *Bush Signs Patriot Act Extension, Military Bill; He had objected to both*, REUTERS, Dec. 31, 2005.

58. H.R. 4659, 109th Cong. (2006) (enacted).

59. S. 2271, 109th Cong. (2006) (enacted).

60. *See* Foreign Intelligence Surveillance Act of 1978 § 501 (f)(2)(A)(i), 50 U.S.C. § 1861, *amended by* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006).

61. *See* Foreign Intelligence Surveillance Act of 1978 § 501(f)(2)(C)(ii), 50 U.S.C. 1861, *amended by* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006).

62. Sheryl Gay Stolberg, *Key Senators Reach Accord On Extending the Patriot Act*, N.Y. TIMES, Feb. 10, 2006, at A14.

the National Security Letter authority,[63] raising the standard of proof necessary to obtain a Section 215 order,[64] making judicial review of the Section 215 gag order and the National Security Letter gag order more meaningful by removing the "bad faith" standard of proof and the one-year waiting period,[65] and reducing the time limit for presumptive notification for "sneak and peek" searches to seven days after the search. However, the Republican Senate leadership successfully blocked Senator Feingold's attempt to offer these amendments.[66] Subsequently, the effort he led to filibuster the Sununu bill and the conference report also failed.[67]

On March 1, 2006, the Senate passed the Sununu bill.[68] While the additional protections it provided were very limited, I joined with a number of Democrats in voting for the bill to affirm its modest improvements to the status quo.[69] The next day, the Senate passed the separate reauthorization of the Patriot Act.[70] Along with nine of my Democratic colleagues, I maintained my opposition and voted against that conference report because, in my view, even with the Sununu bill modifications, the report still failed to strike the appropriate balance between providing security and preserving civil liberties. On March 9, 2006, President Bush signed the Patriot Act reauthorization into law.[71]

It is apparent that the same tensions that existed at the Patriot Act's inception persist, and if anything, are more sharply felt. Congress will undoubtedly continue to struggle in its quest for balanced dedication to the goals of gathering and sharing vital intelligence, and protecting privacy rights and civil liberties as well.

THE DOUBLE-EDGED SWORD: TECHNOLOGY AND TOTAL INFORMATION AWARENESS

Three months after passage of the 2001 Patriot Act, the Defense Advanced Research Projects Agency (DARPA) created a new entity called the

63. S. Amend. 2891, 109th Cong. (2006) (proposed amendment to the Sununu bill, S. 2271, 109th Cong. (2006)).

64. S. Amend. 2892, 109th Cong. (2006).

65. S. Amend. 2893, 109th Cong. (2006).

66. S. Amend. 2894, 109th Cong. (2006).

67. Michael Sandler, *Anti-Terror Act Reauthorization Moves Along With Steady Democratic Protest*, CONG. Q., Feb. 28, 2006.

68. *See* 152 CONG. REC. S1379 (daily ed. Feb. 16, 2006) (Roll No. 22) (on the motion to invoke cloture on the motion to proceed to the Sununu bill); 152 CONG. REC. S1523 (daily ed. Feb. 28, 2006) (Roll No. 23) (on the motion to invoke cloture on the Sununu bill); 152 CONG. REC. S1557 (daily ed. Mar. 1, 2006) (Roll No. 24) (on the motion to invoke cloture on the USA Patriot Act reauthorization amendments).

69. 152 CONG. REC. S1559 (daily ed. March 1, 2006) (Roll No. 25).

70. 152 CONG. REC. S1631-32 (daily ed. March 2, 2006) (Roll No. 29).

71. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006).

Information Awareness Office (IAO), designed to bring together a number of projects already in play at DARPA and to provide a home for a new "program of programs" called "Total Information Awareness" (TIA).[72] By the fall of 2002, news reports were beginning to detail how technologies planned under TIA would help the intelligence community "mine" government and commercial databases for transactions and patterns that might point to terrorists living in our midst.[73] There was good reason to seek this kind of technological advantage. Prior to 9/11, U.S. intelligence had connected multiple September 11th hijackers to al-Qaeda and had information that these individuals possessed U.S. visas.[74] However, this information was not collected in any single database, or even in the hands of any single agency, and disseminated nationwide.[75] If it had been, future hijackers who were stopped by authorities in Maryland and Florida might have been scrutinized more carefully, possibly leading to the detection or disruption of their plot.[76]

For pundits, policymakers, and the populace alike, the parameters of the TIA program crystallized the image of technology and privacy concerns at loggerheads in the war on terror. The logical goal of spotting the kind of terrorist planning and activity that had clearly occurred unchecked before 9/11 clashed mightily with the disconcerting prospect of the government snooping on millions of law-abiding citizens in the process. In an echo of the widespread concern expressed over the passage of the Patriot Act, TIA was roundly criticized by a diverse list of conservative and liberal groups ranging from the Eagle Forum to the American Civil Liberties Union.[77] One of the most troubling aspects of the proposal was that prospects for congressional oversight on behalf of the American people seemed immediately uncertain in light of the IAO's leader: Admiral John Poindexter. Poindexter, who had been convicted of lying to Congress and obstructing congressional investigations during the Iran-Contra scandal,[78] was a veritable poster boy for government secrecy run

72. DEF. ADVANCED RESEARCH PROJECTS AGENCY, REPORT TO CONGRESS REGARDING THE TERRORISM INFORMATION AWARENESS PROGRAM 1-3 (2003) [hereinafter DARPA REPORT].

73. John Markoff, *Threats and Responses: Intelligence—Pentagon Plans a Computer System That Would Peek at Personal Data of Americans*, N.Y. TIMES, Nov. 9, 2002, at A12; Robert O'Harrow Jr., *U.S. Hopes to Check Computers Globally: System Would Be Used to Hunt Terrorists*, WASH. POST, Nov. 12, 2002, at A4.

74. *See, e.g.*, 9/11 REPORT, *supra* note 1, at 266-76.

75. *Id.*

76. *See id.* at 253, 417.

77. Press Release, Eagle Forum Capitol Alert, Senators: Have You Read the Homeland Security Bill? (Nov. 18, 2002), *available at* http://www.eagleforum.org/alert/2002/homeland-11-18-02.shtml; Press Release, ACLU, ACLU Calls on President Bush to Disavow New Cyber-Spying Scheme That Seeks to Put Every American Under Scrutiny (Nov. 14, 2002), *available at* http://www.aclu.org/safefree/general/17109prs20021114.html.

78. United States v. Poindexter, 951 F.2d 369 (1991).

amok.[79]

Despite Poindexter's history—or perhaps because of it—Congress moved swiftly to investigate whether TIA could achieve its positive purpose in a way consistent with privacy law, and whether existing privacy law, particularly since the passage of the Patriot Act, was adequate to meet the challenges the program would present. I was successful in amending the Fiscal Year 2003 omnibus spending bill to make TIA funding contingent on the delivery of a report from the Department of Defense (DoD) outlining plans, costs, and scope for the program and its implications for issues of privacy and civil liberties.[80] The same amendment provided a stopgap measure prohibiting the deployment against U.S. citizens on U.S. soil of any technology stemming from TIA research, absent the express consent of Congress.[81]

The report that arrived from the DoD three months later was telling, right from the cover page. Congress had mandated a report on a program called "Total Information Awareness," but DARPA took pains at the outset to correct what had been a major cosmetic problem: the chilling nature of the program's name.[82] "Total Information Awareness," with its hint that the government might access every conceivable bit of information about Americans' lives, became "Terrorism Information Awareness"—ostensibly to reflect more accurately the program's goals, but clearly to calm fears as well.[83] The original name, combined with the program's dual-edged motto of "*Scientia Est Potentia*" (knowledge is power), had not done TIA's public image any favors.[84]

Image improvements aside, DARPA's apologia for its frankly interesting technology proposals consistently fell short on one front. If it effectively made the case for the potential efficacy of TIA tools, it repeatedly ducked the privacy concerns that actual deployment of those tools would raise.[85] DARPA took as a mandate the findings of the joint report of the SSCI and the House Permanent Select Committee on Intelligence (HPSCI), which indicated that while the U.S. intelligence community possessed information that might have helped thwart the 9/11 attacks, it had failed to detect, share, and analyze the information to an actionable stage.[86] DARPA could promise that TIA would create the technology to remedy those flaws in full compliance with all American privacy laws, but admitted that additional and more serious privacy issues could arise at

79. William Safire, *You Are a Suspect*, N.Y TIMES, Nov. 14, 2002, at 35.

80. Consolidated Appropriations Resolution of 2003 Div. M, § 111(b), Pub. L. No. 108-7, 117 Stat. 11, 535 (2003).

81. *Id.* § 111(c).

82. DARPA REPORT, *supra* note 72, at cover page.

83. *Id.* at 1 n.1.

84. Safire, *supra* note 79.

85. DEP'T. OF DEF., OFFICE OF THE INSPECTOR GEN., INFORMATION TECHNOLOGY MANAGEMENT – TERRORISM INFORMATION AWARENESS PROGRAM (D-2004-033) 4 (2003).

86. S. REP. NO. 107-351, at 10-32 (2002).

deployment.[87] While DARPA could suggest actions to mitigate those concerns beforehand, it could not indicate whether a number of the components being developed could ever be deployed under existing law regarding investigation of U.S. persons.[88]

A clear and primary goal of TIA was to create technology that would enable the linking of multiple and separate databases into a "'virtually' centralized database" suitable for large-scale information mining.[89] However, while TIA would populate its test databases with fictitious persons, questions remained about what sources of information TIA would use when the technology was perfected and deployed. A stated hypothesis of the program was that "it would be highly beneficial to supplement access to existing government data with access to transaction data not already in government databases," but the legal and policy questions raised by the use of actual outside data were to be weighed only after the technology was proven effective and useful.[90] Descriptions of the use of "public" material were clear thanks to earlier Defense Department directives,[91] but promises to use only "legally obtained" material raised more questions,[92] particularly in light of the rise of commercially available databases full of information about Americans' financial transactions and private lives.[93] Additionally, the laws that protect consumer privacy do not apply uniformly to the government's use of commercial databases.[94] The specter of "mission creep" from anti-terrorist activity to general and even local law enforcement loomed large in descriptions of the technologies' potential.[95] This was of particular concern with regard to additional TIA programs that aimed to develop biometric technologies to spot terrorists in public places. DARPA noted that Activity, Recognition and Monitoring (ARM), Next Generation Face Recognition, and Human Identification at a Distance (HumanID) would clearly face hurdles to

87. DARPA REPORT, *supra* note 72, at 27.

88. *Id*. at 18-20.

89. *Id.* at app. A, 11.

90. *Id.* at app. A, 5.

91. *Id.* at app. A, 17; UNDER SEC'Y OF DEF. FOR POLICY, PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT U.S. PERSONS 7 (1982), *available at* http://www.dtic.mil/whs/directives/corres/html/52401r.htm.

92. Letter from author to Dr. Anthony Tether, Director, Defense Advanced Research Projects Agency (June 24, 2003); DARPA REPORT, *supra* note 72, at 3-4, 6, 27-28, 32, app. A 5.

93. ROBERT O'HARROW, NO PLACE TO HIDE 1-6 (2005).

94. James Dempsey & Lara Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459 (2004) (citing GINA MARIE STEVENS, PRIVACY: TOTAL INFORMATION AWARENESS PROGRAMS AND RELATED INFORMATION AWARENESS PROGRAMS AND RELATED INFORMATION ACCESS, COLLECTION, AND PROTECTION LAW, CRS REPORT FOR CONGRESS (2003)).

95. DARPA REPORT, *supra* note 72, at 3-4, 6, 27-28, 32, app. A 18.

deployment under existing case law.[96]

Vague answers combined with clear statutory restrictions presented several unappetizing and ultimately unacceptable scenarios. First among these was the creation of technologies that would give the government unprecedented power to invade Americans' privacy. In addition, there was the possibility that tens of millions of taxpayer dollars could be spent to fund those technologies, only to find they could never be deployed or used properly under existing law.[97] Finally, some envisioned an eventual push to weaken privacy protections radically so that the newly created technologies could be used.

Senate appropriators, alerted to the potential dangers of TIA, called for the closure of the IAO and the de-funding of TIA's most troubling proposals in the FY2004 Defense Appropriations bill.[98] As that legislation moved forward, the exposure of a little-known component of TIA—which, ironically, had no privacy or civil liberties concerns attached—served as the final nail in the program's coffin. The "Futures Markets Applied to Prediction" (FutureMAP) component of TIA would have used "market-based techniques for avoiding surprise and predicting future events" by allowing anonymous traders to purchase futures on suggested terrorist events, and to receive a payout when the event did or did not occur.[99] Widespread and vociferous opposition to FutureMAP forced the shutdown of that TIA component within twenty-four hours of its exposure.[100] John Poindexter resigned shortly thereafter.[101] These events almost certainly cemented the Defense Appropriations bill conferees' final decision to close IAO and zero out funding for the many components of TIA regarding which privacy concerns could not be satisfactorily resolved.[102] Meanwhile, a number of research programs for technologies that did not pose privacy threats were allowed to continue at DARPA, and the use of technologies formerly under the TIA umbrella remained available for some military and foreign intelligence investigations.[103]

This was a valiant effort to strike an appropriate balance among vital concerns: the simultaneous curtailing of initiatives that threatened the privacy of U.S. persons, affirmation of technologies that did not appear to pose such threats, and permission to use powerful investigative technologies in

96. *Id.* at app. A 18-22, 35 (citing Kyllo v. United States, 533 U.S. 27 (2001)).

97. DEP'T. OF DEFENSE, OFFICE OF THE INSPECTOR GEN., INFORMATION TECHNOLOGY MANAGEMENT – TERRORISM INFORMATION AWARENESS PROGRAM (D-2004-033) 4 (2003).

98. Department of Defense Appropriations Act of 2004, S. 1382, 108th Cong. § 8120(a) (2004).

99. DARPA REPORT, *supra* note 72, at app. B, 8-9.

100. Carl Hulse. *Swiftly, Plan for Terrorism Futures Market Slips Into Dustbin of Idea Without a Future*, N.Y. TIMES, July 30, 2003 at A10; Bradley Graham, *Poindexter to Leave Pentagon Research Job*, WASH. POST, Aug. 1, 2003, at A1.

101. *Id.*

102. Department of Defense Appropriations Act, Pub. L. No. 108-87, § 8131(a), 117 Stat. 1054 (2004).

103. *Id*. at § 8131(b).

appropriate foreign intelligence venues. However, in a post-mortem review of TIA, the Defense Secretary's own Technology and Privacy Advisory Committee found that if potential terrorists are inside the United States, fundamental goals will remain unmet by the "line at the border" approach taken by the conferees and embodied in much of privacy law.[104] The legal parsing of when and where it is permissible to data-mine and use bioinformatics neither closes the door completely on targeting U.S. persons nor ensures the fullest appropriate use of new technologies to track terrorists who may already be here. Also, despite TIA's demise, other government data-mining efforts remained in existence, some posing threats to privacy even as they offered legitimate advances in the fight against terrorism.[105] On July 22, 2005, the Government Accountability Office found that the Transportation Security Administration (TSA) had violated the Federal Privacy Act in testing its "Secure Flight" screening program by comparing passenger information from airlines with additional information from commercially available databases.[106] After this was made public, TSA immediately reiterated its intention to use commercially available data in its screening efforts.[107] So the need for congressional vigilance did not evaporate with TIA.

The need for new and responsible approaches to balance valuable security technology with privacy and civil liberties concerns persists as well. The same facts that prompted TIA's overreach have inspired a number of more appropriately designed and targeted initiatives to create the kind of information sharing among government agencies that is an essential part of counterterrorist strategy. For instance, in May 2002 the SSCI noted again the obvious problems with information access that preceded the September 11th attacks. The Committee found that, although the Intelligence Community did have a significant amount of intelligence concerning known or suspected international "terrorists and terrorist organizations, the main databases used to store this information were not well-configured to provide it to those responsible for protecting American citizens from international terrorists."[108]

Subsequently, the Committee and the full Congress approved legislation that established a national database for the collection and analysis of information regarding international terrorism suspects.[109] The database law provides an excellent example of how to strike the proper balance between

---

104. TECH. AND PRIVACY ADVISORY COMM., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM ix (2004).

105. *Id.* at 4.

106. Leslie Miller, *Report: Government Broke Laws over Commercial Data*, AP NEWSWIRES, July 22, 2005.

107. Leslie Miller, *Government to Test If Air Passenger Screening Can ID Terror Cells*, AP NEWSWIRES, July 23, 2005.

108. S. REP. NO. 107-149, at 19 (2002).

109. Intelligence Authorization Act for Fiscal Year 2003 § 343, Pub. L. No. 107-306, 116 Stat. 2383, 2399-401 (2002).

security and privacy rights: as evidence suggests that an individual is involved in terrorism, information is to be collected and entered into the database now being operated by the FBI as part of its terrorist screening center[110] where it can be accessed by all of the relevant law enforcement and intelligence officials. It remains critical, of course, to ensure that the information gathered is focused on legitimate terrorist suspects, so that the personal information of law-abiding individuals is not swept up in a wide net. Continued and vigorous congressional oversight is essential in this regard.

The SSCI-authored database law serves as evidence that access to information can be substantially improved without necessarily compromising the rights of innocent Americans. The United States is in no way obligated to forgo the benefits of technology in the war on terror to satisfy privacy concerns; on the contrary, it is the job of federal policymakers to ensure the aggressive *and* responsible use of technology to safeguard the American people.

HIDDEN FROM VIEW: SECRECY, CLASSIFICATION, AND OVERSIGHT

In his definitive 1998 book *Secrecy*, U.S. Senator Daniel Patrick Moynihan (D-N.Y.) wrote that "[i]n the United States, secrecy is an institution of the administrative state that developed during the great conflicts of the twentieth century."[111] As the opening conflict of the twenty-first century unfolds, this institution has swollen to the point at which it threatens both national security efforts and the protection of privacy and civil liberties. The unnecessary shielding of documents prevents information from being accessed effectively by the people who need it,[112] and it also prevents them from being examined by the public. Every major panel study of the 9/11 attacks found that hoarding of information at federal agencies contributed to the intelligence failure of that day; likewise, rampant overclassification and underreporting have demonstrably limited the opportunity for congressional oversight of many anti-terrorism measures.

The information classification system designed in the early twentieth century to prevent the dissemination of information whose release might compromise national security interests thickened long ago into a veil of secrecy that envelops information that would be embarrassing or politically damaging, along with information whose classification serves no purpose at all. This transformation began long before the terrorist attacks of September 11th. As Moynihan so clearly chronicled, it has its deepest roots in the Cold War,[113]

110. Statement of Donna A. Bucella to the National Commission on Terrorist Attacks Upon the United States (Jan. 26, 2004), *available at* http://www.9-11commission.gov/hearings/hearing7/witness_bucella.htm.

111. DANIEL PATRICK MOYNIHAN, SECRECY: THE AMERICAN EXPERIENCE 59 (1998).

112. 9/11 REPORT, *supra* note 1, at 417.

113. MOYNIHAN, *supra* note 111, at 59; *see also id.*

when the agencies of the Executive Branch, dogmatic about keeping all conceivably useful information out of Soviet hands, came to routinely treat information as treasure to be guarded even from other government agencies as well as the public.

Unfortunately, secrecy did not recede after the Cold War ended. In many respects, secrecy continued to grow. In a 2000 report with Senator Moynihan, I recounted the government's tendency toward excessive secrecy on issues from environmental law[114] to the murder of two Americans in Chile.[115] Conducting research at our request, the Congressional Research Service found more than 1500 Sunshine Act exemption notices in the Federal Register in 1998 alone, closing meetings on subjects from assassinations to consumer product safety.[116] Senator Moynihan and I wrote at the time that "[b]ehind closed doors, there is no guarantee that the most basic of individual freedoms will be preserved. And as we enter the 21st Century, the great fear we have for our democracy is the enveloping culture of government secrecy and the corresponding distrust of government that follows."[117] When we look at the secrecy that cost America so many lives on 9/11 and the growing concern surrounding secret government anti-terror activities, it does not appear that this fear was misplaced.

As I have noted, both the Congressional Joint Inquiry into 9/11 and the 9/11 Commission concluded that the Intelligence Community had acquired information prior to September 11, 2001 that could have led to the detection or disruption of the terrorist plot, but failed to connect the dots in part due to limits on access to information.[118] Some of these limits were due to a sensitivity to due process concerns that seems to have exceeded the administrative rules governing the handling of intelligence suspects[119]—for instance, investigators failed to search the property of "twentieth hijacker" Zacarias Moussaoui after arresting him because they erroneously believed more evidence was needed to allow a search. Other factors limiting information, however, were due to a pervasive culture of restricting access in

---

114. RON WYDEN & DANIEL PATRICK MOYNIHAN, SECRECY IN INTERNATIONAL AND DOMESTIC POLICY MAKING: THE CASE FOR MORE SUNSHINE (2000), http://www.fas.org/sgp/library/wyden.html.

115. *Id*.

116. HAROLD RELYEA, CONG. RESEARCH SERV., 1998 SUNSHINE ACT: MEETING CLOSURE NOTICES 2-5 (1999), *cited in* WYDEN & MOYNIHAN, *supra* note 114.

117. WYDEN & MOYNIHAN, *supra* note 114.

118. S. SELECT COMM. ON INTELLIGENCE & H. PERMANENT SELECT COMM. ON INTELLIGENCE, 107TH CONG., JOINT INQUIRY INTO INTELLIGENCE COMMUNITY ACTIVITIES BEFORE AND AFTER THE TERRORIST ATTACKS OF SEPTEMBER 11, 2001, S. REP. NO. 107-351, H. REP. NO. 107-792, at pt. 1, sec. 3, finding 5 (Dec. 2002) [hereinafter JOINT INQUIRY]; 9/11 REPORT, *supra* note 1, at 417.

119. JOINT INQUIRY, *supra* note 118, at pt. 1, sec. 3, finding 5(f).

the intelligence community, sometimes even within a single agency.[120] Perhaps the most memorable instance of this was the FBI's failure to disseminate a memo from its Phoenix, Arizona office to other field branches across the country, who would have been alerted to look specifically for potential al-Qaeda members learning to fly planes.[121] It cannot be said definitively whether improved information access alone could have stopped the September 11th attacks, but it is clear that the likelihood of catching the terrorists before they could carry out their plot would have been greater, not less.

As Senator Moynihan pointed out, history proves that secrecy has engendered bad policy decisions that have made the American people less secure. During the 1980s, clear signals were beginning to emerge that suggested a Soviet Union on the brink of collapse.[122] Had the Intelligence Community been willing to share some of its data or conclusions about the strength of the Soviet economy, other government agencies or outside experts might have seen that U.S. policy was being formulated based on flawed premises—that the Soviet economy remained strong, and that the country would continue to compete with the United States.[123] Instead, their blinkered process supported unwise policy choices such as the eventual decision to supply Stinger missiles and other advanced weapons to the Afghan *mujahideen*.[124] It is clear in hindsight that Americans would have been far safer had those weapons been kept out of the hands of the Taliban and their allies.[125]

Many contend that American security has been damaged—and a new front opened in the war on terror—by the use of the classification process to help build support for war in Iraq. In the fall of 2002, after multiple requests from the SSCI, Director of Central Intelligence (DCI) George Tenet ordered the Intelligence Community to prepare a National Intelligence Estimate (NIE) regarding Iraq's weapons of mass destruction capabilities.[126] The NIE, published by the National Intelligence Council, was produced extremely quickly, but it nonetheless presented a fairly comprehensive picture of the intelligence community's assessments regarding WMD and Iraq.[127] Three days later, DCI Tenet, who was noted for having reportedly described the

120. *Id.* at finding 9, 10.

121. *Id.* at finding 5(e).

122. Daniel Patrick Moynihan, *Will Russia Blow Up?*, NEWSWEEK, Nov. 19, 1979, *cited in* Richard Gid Powers, *Introduction* to DANIEL PATRICK MOYNIHAN, SECRECY: THE AMERICAN EXPERIENCE 1, 3-4 (Yale Univ. Press, 1998).

123. MOYNIHAN, *supra*, note 111, at 79, 105.

124. Steve Coll, *Anatomy of a Victory: CIA's Covert Afghan War*, WASH. POST, July 19, 1992, at A1.

125. *See generally*, CHRISTOPHER BOLKCOM, CONG. RESEARCH SERV., OPERATION ENDURING FREEDOM: POTENTIAL AIR POWER QUESTIONS FOR CONGRESS (2003).

126. S. SELECT COMM. ON INTELLIGENCE, 108TH CONG., REPORT ON THE U.S. INTELLIGENCE COMMUNITY'S PREWAR INTELLIGENCE ASSESSMENTS ON IRAQ 298-303 (2004), *available at* http://intelligence.senate.gov/iraqreport2.pdf [hereinafter PREWAR INTELLIGENCE REPORT].

127. *Id.* at 302.

intelligence regarding WMD as a "slam dunk,"[128] published an unclassified "white paper" on the same topic.[129] In its review of intelligence failures leading up to the Iraq war, the SSCI found the differences between the two documents significant. Nuances and caveats contained in the original classified document (which has since become public) were eliminated from the unclassified version, and those cautionary notes in the case for war were not presented to the American people.[130] As a result, the public heard a much more alarming perspective on Saddam Hussein's capabilities and intentions.

In its *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*, the Committee concluded that "[t]he intelligence Community's elimination of the caveats from the unclassified White Paper misrepresented their judgments to the public which did not have access to the classified National Intelligence Estimate containing the more carefully worded assessments,"[131] and that "[t]he key judgment in the unclassified October 2002 White Paper on Iraq's potential to deliver biological agents conveyed a level of threat to the United States homeland inconsistent with the classified National Estimate."[132] In the end, the overclassification of cautions regarding the intelligence conclusion allowed the Administration to present a much more forceful case for war than would have otherwise been possible. Overclassification made it less likely that members of Congress, when called upon to authorize military action in Iraq, would have the information necessary to cast an informed vote in the interest of American security.

The government's tendency toward secrecy has made it difficult for Congress to safeguard privacy and civil liberties as well. As the Patriot Act is emblematic of so many post-9/11 concerns, it is also a case study of the damage secrecy can do in the struggle for both security and freedom. Details regarding the Act's use are often not reported, and when they are, these reports are often classified. This creates significant barriers to both accountability and oversight.

For example, under the Patriot Act, the Department of Justice must report to Congress semiannually regarding the use of FISA business records warrants to collect information in national security investigations.[133] As these reports are routinely submitted in classified form, they cannot be reviewed even by most congressional staffers,[134] and this in turn makes it less likely that members of

128. James Risen, *C.I.A. Held Back Iraqi Arms Data, U.S. Officials Say*, N.Y. TIMES, July 6, 2004 at A1.

129. PREWAR INTELLIGENCE REPORT, *supra* note 126, at 286.

130. *Id.*

131. *Id.* at 295.

132. *Id.* at 296.

133. USA PATRIOT Act § 215, 50 U.S.C. § 1862 (2005).

134. The United States Senate permits two cleared staffers and one cleared fellow for work in personal offices. If the Senator is on the Armed Services, Foreign Relations, Intelligence, or Appropriations Committees, then they may have three cleared staffers.

Congress will see them.[135] Certainly, many details relevant to national security investigations should be kept secret, since making them public would allow targeted groups to evade investigators more effectively; however, simply revealing how often particular authorities are used does not make these authorities less effective. Making particular information public could make it easier for Congress to determine whether granted authorities are being used appropriately.

When such information is not disclosed, the public has little choice but to take even subjective statements from governments officials at face value. In testimony before the Senate Intelligence Committee, FBI Director Robert Mueller stated that the FBI was not using FISA warrants as frequently as it could, because alternatives such as national security letters were available.[136] Since the total number of requests made with national security letters is classified, it is not possible for the public independently to evaluate this statement or its implications.[137]

Such information is often declassified, however, when it is politically expedient to do so. As congressional committees began to hold hearings on reauthorization of the Patriot Act in spring 2005, the Administration released substantial amounts of previously classified information regarding the law's use,[138] pointing to the newly released documents as evidence that some Patriot Act authorities are not being used excessively or inappropriately. The sunshine that allowed for such a glowing review of the Patriot Act, however, has not been allowed to shed light on possible abuses of the law through the routine declassification of reports. While in theory administrative rules prohibit information from being classified to conceal violations of the law, or to protect individuals and agencies from embarrassment,[139] in reality classification decisions are made all too often to shield officials and agencies from accountability and stifle debate on politically sensitive issues.

In response to this problem, I was joined by U.S. Senators Trent Lott (R-Miss.), Bob Graham (D-Fla.), and Olympia Snowe (R-Maine) in the summer of 2004 to propose a broad overhaul of the classification system.[140] Several of our ideas were accepted into law as part of the Intelligence Reform and Terrorism

135. Members of Congress are not permitted to store classified documents in their personal offices. If a member does not have an appropriately cleared staffer to research the document for them, they must go to a secure area and do so themselves.

136. *USA PATRIOT Act of 2001: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. (2005) (comments of Robert S. Mueller, Director of the FBI).

137. At the time of the hearing, the Department of Justice was also several months late in submitting its most recent report. During my questioning of the witnesses, I asked that the report be submitted as soon as possible. It was completed the next day.

138. *USA PATRIOT Act of 2001: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. (2005); *Oversight of the USA PATRIOT Act: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. (2005); *USA PATRIOT Act: A Review for the Purpose of Its Reauthorization: Hearing Before the H. Comm. on the Judiciary*, 109th Cong. (2005).

139. Exec. Order No. 12,958 § 1.8(a), 60 Fed. Reg. 19,825 (Apr. 17, 1995).

140. S. 2672, 108th Cong. (2004).

Prevention Act of 2004.[141] Most significantly, we expanded the mandate of the Public Interest Declassification Board to make it possible for members of Congress to appeal classification decisions.[142] We also directed the new Director of National Intelligence to establish and implement classification guidelines for the entire intelligence community, with the role of reducing overclassification and maximizing access to critical information.[143] Unfortunately, the current Administration has been very reluctant to address this problem. When the first Director of National Intelligence, John Negroponte, had his confirmation hearing before the Intelligence Committee, I asked him about overclassification. To my surprise and disappointment, he not only declined to discuss solutions, but he refused to acknowledge that overclassification might be a national security issue.[144] Since his confirmation, the Administration has refused to take a fresh look at classification guidelines or address them at a comprehensive, community-wide level.[145] The Administration has also been reluctant to support the Declassification Board; the President did not fund it in his Fiscal Year 2006 budget request.[146]

The government's responsibility to increase security and its latitude to impact individual freedoms were exponentially increased by the attacks of September 11 and by the laws passed in the aftermath of that day. In both respects, the American people are best served—that is to say, they can be safer and more certain of their individual rights and freedoms—by the strongest possible allegiance to openness and by the fullest possible acceptance of accountability. Simply put, rampant secrecy and overclassification inhibit the ability of intelligence agencies, the President, and Congress alike to protect citizens' lives and their most cherished rights. Supreme Court Justice Louis D. Brandeis observed that "sunlight is said to be the best of disinfectants; electric light the most efficient policeman."[147] In the new struggle against terrorism, transparency may be the American people's most essential guardian.

---

141. Intelligence Reform and Terrorist Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004).

142. *Id*. at § 1102.

143. *Id*. at § 1011.

144. *Nomination of John Negroponte to be Director of National Intelligence: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. (2005).

145. *See* Press Release, White House, President Bush Administration Actions to Implement WMD Commission Recommendations (June 29, 2005), http://www.whitehouse.gov/news/releases/2005/06/20050629-5.html.

146. BUDGET OF THE UNITED STATES GOVERNMENT, FISCAL YEAR 2006 (2005).

147. Louis D. Brandeis, *What Publicity Can Do*, *in* HARPER'S WEEKLY, Dec. 20, 1913, *reprinted in* LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY 92 (1932).

CONCLUSIONS

Balancing security, privacy, and civil liberties in federal policy is not a finite task; it is a perpetual struggle with a many-headed Hydra. Difficult questions will seldom be permanently settled, and new, uncharted ambiguities will continually arise as America's anti-terrorism efforts evolve. Since no one solution will end the debate, the best approach for policymakers is to apply intellectual rigor to each new dilemma. Thoughtful leaders will be guided by two bedrock principles: that concerns for security and privacy must be approached in tandem, with neither relegated to an afterthought; and that if a proposed solution abandons one goal for the other, a different solution must be sought.

In some of the darkest days of the last century, President Franklin Delano Roosevelt declared that the only thing America had to fear was fear itself. In crafting law and policy for the post-9/11 world, America's leaders would do well to remember his words. What terrorists can do to us is sobering and awful, but bombs and murderous plots will never topple this nation. Fear that eclipses good governance, on the other hand, could. The tragedy of the September 11th attacks would be sadly compounded by a wholesale shift away from the principles that make America great in an effort to make America impenetrable—a terrible forfeiture in pursuit of an understandable, but ultimately unattainable, goal. Sacrifices must be made, and compromises must be struck, but leaders must not let the debris of our shattered safety occlude the path to sound public policy. If that happens, far more than security will be lost. What Americans are so frequently told about the war on terror is absolutely true: freedom itself is at stake.