

Lost in Cyberspace? Finding American Liberties in a Dangerous Digital World

John D. Podesta and Raj Goyle[†]

“History teaches that grave threats to liberty often come in times of urgency, when constitutional rights seem too extravagant to endure. . . . [W]hen we allow fundamental freedoms to be sacrificed in the name of real or perceived exigency, we invariably come to regret it.”¹

“After 9/11, the emphasis has clearly been on physical infrastructure rather than cybersecurity. That’s understandable. . . . But cyberspace is where the bad guys are going.”²

I. INTRODUCTION

This Policy Essay discusses the emerging security threat of cyberterrorism and the historical impulse to restrict civil rights and civil liberties during times of national crisis. Cyberterrorism poses a significant danger that requires a strong and unequivocal response, but such a response need not sacrifice important constitutional safeguards. Frequently in our past, from the time of the two World Wars to the recent attacks on the World Trade Center, our leaders enacted policies that gave an illusion of enhancing security but in reality failed to provide additional safeguards and in the process abused constitutional rights. We argue that this historical pattern need not continue with regard to cyberterrorism. With proper planning and a sense of urgency, cyberterrorism can be addressed proactively *before* serious harm is done. This will not only reduce the possibility that the same terrorists who turned commercial airplanes into lethal bombs will turn our vast computer networks against us, but it will

[†] John D. Podesta is the President and CEO of the Center for American Progress in Washington, D.C. and a visiting professor of law at Georgetown University Law Center. He served as President William Jefferson Clinton’s Chief of Staff from 1998-2001. Raj Goyle is the Senior Domestic Policy Analyst at the Center for American Progress. This Policy Essay was adapted from a speech delivered by John Podesta at the Cybercrime and Digital Law Enforcement Conference at Yale Law School on March 27, 2004. The authors thank Mirna Galic and Tara Swaminatha for their assistance in preparing this Policy Essay.

1. *Skinner v. Ry. Labor Executives’ Ass’n*, 489 U.S. 602, 635 (1989) (Marshall, J., dissenting).
2. Jon Swartz, *Terrorists’ Use of Internet Spreads*, USA TODAY, Feb. 21, 2005, at 3B (quoting Paul B. Kurtz, a former senior cybersecurity official in the Bush Administration and executive director of the Cyber Security Industry Alliance, a non-profit trade group of hardware and software companies dedicated to the improvement of cybersecurity).

also reduce the risk of unnecessary infringements of our civil liberties.

To understand properly why steps to counter cyberterrorism should be taken now, it is important to discuss briefly how widespread violations of civil liberties occurred in our past, and how they are recurring once again after the September 11 attacks. Only by understanding the context in which violations of civil liberties become prevalent does the need for action become clear. Accordingly, this Policy Essay begins with a general overview of the Bush Administration's response to the September 11 attacks, with a particular emphasis on the disturbing parallels between long-time FBI director J. Edgar Hoover and former Attorney General John Ashcroft. With this background established, the Policy Essay then presents cyberterrorism in detail, along with the Clinton and Bush Administrations' strategies for addressing the threat. The Policy Essay concludes with suggestions for how the problem of cyberterrorism can best be approached in the future—in a manner that will both safeguard our national security while maintaining maximal respect for our civil liberties.

II. THE BUSH ADMINISTRATION'S RESPONSE TO SEPTEMBER 11: SACRIFICING CIVIL LIBERTIES IN THE NAME OF NATIONAL SECURITY

To fully understand the importance of proactively addressing the threat of cyberterrorism now, before a major attack has occurred, it is first necessary to understand the historic pattern of executive-branch abuses that have occurred in the wake of national crises—an historic pattern that continues to this day. Accordingly, this Part of the Policy Essay begins by highlighting the striking parallels between the Bush Administration's response to September 11 and the policies pursued by J. Edgar Hoover during his infamously abusive tenure as director of the FBI.

Hoover came to power soon after World War I and led the FBI during many of the most important events of the twentieth century, including World War II, the Cold War, and the Civil Rights Movement. Unfortunately, his forty-eight-year tenure was also marked by an undeclared war on virtually all subversives, communists, and social activists.³ Hoover worked as a young aide to A. Mitchell Palmer, President Wilson's Attorney General. Together, the two men—in what are now known as the “Palmer Raids”—exploited a series of bombings by anarchists to round up thousands of suspected communists (most were members of labor unions guilty only by association) on trumped-up charges based on the recently passed Espionage and Sedition Acts.⁴ The Palmer Raids were paradigmatic of Hoover's approach to law enforcement: eroding civil liberties in the name of national security. During World War II, Hoover

3. See DAVID COLE, *ENEMY ALIENS: DOUBLE STANDARDS AND CONSTITUTIONAL FREEDOMS IN THE WAR ON TERRORISM* 116 (2003).

4. *Id.* at 111, 117.

Lost in Cyberspace?

deployed a “custodial detention list,” which was nothing more than a listing of foreign nationals based on their ethnic identity rather than on any individualized behavior. After World War II, Hoover developed a list of allegedly dangerous persons that grew to more than 25,000 names by 1954.⁵ As the decades wore on, wiretapping without suspicion of illegal activity or a court-approved warrant became commonplace.⁶ Eventually, files on nearly one half of one million individuals and organizations were compiled by Hoover’s FBI, while Operation COINTELPRO and the CIA’s Operation CHAOS targeted thousands of allegedly dangerous individuals.⁷

Some positive developments resulted from these abuses. The Palmer Raids gave rise to the American Civil Liberties Union and to modern First Amendment doctrine.⁸ In addition, after Hoover’s excesses came to light in the mid-1970s, a number of strong reforms were enacted: Attorney General Edward Levi issued guidelines in 1976 that required the FBI to investigate actual criminal conduct and not simply to monitor the constitutionally protected speech of organizations and individuals;⁹ the Foreign Intelligence Surveillance Court was created in 1978 to impose some judicial review on domestic spying related to foreign intelligence gathering;¹⁰ and finally, a few years later, Congress passed the Electronic Communications Privacy Act of 1986,¹¹ which brought modern communication technologies under the umbrella of federal wiretapping laws. These protections ended many of the extra-constitutional activities of law enforcement and intelligence officials that occurred during the Hoover era.

Hoover’s overzealous yet ineffective approach to law enforcement, however, was recently resurrected by former Attorney General John Ashcroft, perhaps the administrative official whose policies have best exemplified the overall approach of the Bush Administration. In just a few short years, Ashcroft managed to turn the clock back at least thirty years. His Department of

5. *Id.* at 102.

6. *Id.* at 156.

7. *Id.* at 155.

8. See ACLU, *THE AMERICAN CIVIL LIBERTIES UNION: FREEDOM IS WHY WE’RE HERE 2* (1999), available at <http://www.aclu.org/Files/OpenFile.cfm?id=10740> (last visited Mar. 29, 2005); see also SAMUEL WALKER, *IN DEFENSE OF AMERICAN LIBERTIES: A HISTORY OF THE ACLU* 42-45, 52 (2d ed. 1999) (describing the role of the Palmer Raids in the formation of the ACLU).

9. The Attorney General’s Guidelines on Domestic Security Investigations (Apr. 5, 1976), reprinted in *FBI Statutory Charter: Hearings on S. 1612 Before the Senate Comm. on the Judiciary*, 95th Cong. 18-26 (1978). The “Levi Guidelines” were revised by President Reagan’s Attorney General William French Smith in 1983. See The Attorney General’s Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations (Mar. 7, 1983), reprinted in 32 *Crim. L. Rep. (BNA)* 3087 (1983).

10. See Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 18 and 50 U.S.C. (2004)).

11. Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C. (2004)).

Justice—recently inherited by former White House Counsel Alberto Gonzales—regularly violated the rights of individuals and pursued immigrant communities in a manner disturbingly reminiscent of Hoover’s FBI. For example, soon after September 11, Ashcroft resurrected Hoover’s infamous creation of a list of foreign nationals through the implementation of the National Security Entry-Exit Registration System (NSEERS), which required tens of thousands of adult males to register with the government solely because they were from predominately Muslim countries.¹² In addition, in May 2002, Ashcroft substantially weakened Attorney General Levi’s Guidelines, removing important safeguards that limit the scope of federal investigations and expanding the potential for the FBI to engage in domestic spying.¹³ Ashcroft also personally directed that hundreds of immigrants of Arab, Middle Eastern, and South Asian descent be rounded up and detained on pretextual charges—or sometimes on no charges at all. Some were beaten, and while many were charged with relatively minor immigration charges, not a single individual was charged with any terrorist crime related to the September 11 attacks.¹⁴

John Ashcroft’s record is clear: He will be remembered, like Hoover, as a law enforcement official who dangerously (yet ineffectively) expanded governmental powers at the expense of our nation’s most valued principles by misleading the public and exploiting people’s fears.¹⁵ In evaluating several of Ashcroft’s policies regarding immigration and law enforcement, the Commission investigating the attacks on September 11 was unable to find evidence that any terrorists were uncovered or that any useful anti-terrorism information was obtained.¹⁶ Even the Department of Justice’s own Inspector

12. Registration and Monitoring of Certain Nonimmigrants, 67 Fed. Reg. 52,584 (Aug. 12, 2002) (codified at 8 C.F.R. §§ 214, 264 (2004)); see also Candida Harty, Current Developments, *National Security Entry-Exit Registration System*, 17 GEO. IMMIGR. L.J. 189 (2002).

13. See Don Van Natta, Jr., *Government Will Ease Limits on Domestic Spying by F.B.I.*, N.Y. TIMES, May 30, 2002, at A1.

14. See OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF JUSTICE, THE SEPTEMBER 11 DETAINEES: A REVIEW OF THE TREATMENT OF ALIENS HELD ON IMMIGRATION CHARGES IN CONNECTION WITH THE INVESTIGATION OF THE SEPTEMBER 11 ATTACKS (2003), available at <http://www.usdoj.gov/oig/special/0306/full.pdf> (last visited Mar. 13, 2005).

15. There is perhaps no better proof of his approach than his now-infamous words to Congress in the weeks after the attacks on September 11:

[T]o those who scare peace-loving people with phantoms of lost liberty[,] my 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.

Preserving Our Freedoms While Defending Against Terrorism: Hearing Before the Senate Comm. on the Judiciary, 107th Cong. 313 (2001) (testimony of Attorney General John Ashcroft), available at 2001 WL 26188084.

16. NAT’L COMM’N ON TERRORIST ATTACKS UPON THE UNITED STATES, STAFF STATEMENT NO. 10: THREATS AND RESPONSES IN 2001, at 12-13 (2004), available at http://www.9-11commission.gov/staff_statements/staff_statement_10.pdf (last visited Mar. 29, 2005); see also THOMAS R. ELDRIDGE ET AL., NAT’L COMM’N ON TERRORIST ATTACKS UPON THE UNITED STATES, 9/11 AND TERRORIST TRAVEL 152-61 (2004) (describing and criticizing various Department of Justice initiatives undertaken in response to the September 11 terrorist attacks), available at http://www.9-11commission.gov/staff_statements/staff_statement_10.pdf

Lost in Cyberspace?

General issued a report—which drew bipartisan praise for its even-handed analysis¹⁷—harshly critical of Ashcroft’s indiscriminate detention of members of certain immigrant communities on the basis of their ethnic identities.¹⁸ Although Homeland Security Secretary Tom Ridge would ultimately concede that the post-9/11 crackdown had crossed the line,¹⁹ Ashcroft offered only this: “We make no apologies”²⁰

Ashcroft’s casual disregard for the protection of civil liberties—and the public’s concern over their erosion—was readily apparent in his defense of the USA PATRIOT Act,²¹ the centerpiece of the Bush Administration’s response to September 11. The Act, passed in the days after September 11, granted broad new powers to the law enforcement and intelligence communities, but also engendered intense criticism and controversy. Rather than meeting this criticism by providing useful information to Congress and the American people about how the government has employed its powers under the Act, Ashcroft instead launched a nationwide tour attacking his critics, complete with a website (www.lifeandliberty.gov) and tour dates—perhaps the first time an Attorney General has done a road show to advocate the retention of a federal statute.²²

Although the new powers granted in the Act carry a potential for abuse, invasion of privacy, and profiling of individuals,²³ many of its provisions address significant problems in existing law.²⁴ The sections related to electronic surveillance,²⁵ for example, are important efforts to update the laws to reflect

11commission.gov/staff_statements/911_TerrTrav_Monograph.pdf (last visited Mar. 29, 2005).

17. See, e.g., Eric Lichtblau, *Report on Detainees Shines a Brighter Spotlight on an Inspector General*, N.Y. TIMES, July 5, 2003, at A9.

18. See OFFICE OF THE INSPECTOR GEN., *supra* note 14.

19. See Mark Baker, *Crackdown Overrode Liberty: Security Chief*, THEAGE.COM, Mar. 10, 2004, at <http://www.theage.com.au/articles/2004/03/09/1078594362827.html>; *Report: Ridge Regrets Some Security Steps*, UPI, Mar. 10, 2004, LEXIS, News Library, Wire Service Stories File.

20. Eric Lichtblau, *U.S. Report Faults the Roundup of Illegal Immigrants After 9/11*, N.Y. TIMES, June 3, 2003, at A1 (quoting Department of Justice spokeswoman Barbara Comstock).

21. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of 8, 12, 18, 21, 22, 28, 31, 47, and 50 U.S.C. (2004)).

22. See Eric Lichtblau, *Ashcroft’s Tour Rallies Supporters and Detractors*, N.Y. TIMES, Sept. 8, 2003, at A14.

23. For example, section 215 of the USA PATRIOT Act permits the government to obtain “any tangible thing” upon a mere certification to a judge without naming a specific target. 115 Stat. at 287-88 (codified as amended at 50 U.S.C. §§ 1861-1862). Section 217 of the Act authorizes individuals to permit law enforcement to monitor their computer for “trespassers” without obtaining a warrant, exposing many computer users to unwarranted surveillance. *Id.* at 290-91 (amending 18 U.S.C. §§ 2510-2511). And section 412 permits the Attorney General to unilaterally detain any alien for up to seven days without judicial review. *Id.* at 350-52 (amending 8 U.S.C. § 1226a).

24. See CENTER FOR AMERICAN PROGRESS ET AL., *STRENGTHENING AMERICA BY DEFENDING OUR LIBERTIES* 16-23 (2003), available at <http://www.cnss.org/Defending%20our%20Liberties%20report.pdf> (last visited Mar. 29, 2005); John Podesta, *USA PATRIOT ACT: The Good, the Bad, and the Sunset*, HUMAN RIGHTS, Winter 2002, at 3.

25. USA PATRIOT Act § 216, 115 Stat. at 288-90 (amending 18 U.S.C. §§ 3121, 3123-3124,

the realities of the digital age. With over two billion e-mails changing hands every day through hundreds of millions of computers, it was reasonable to address the installation of devices that can record all routing, addressing, and signaling information, under appropriate court supervision. Likewise, permitting “roving wiretaps” in foreign-intelligence gathering corrected a loophole in the law prior to 2001.²⁶ That terrorists lived undetected within the country’s borders illustrated another problem that the USA PATRIOT Act addressed—the “wall” that prohibited the sharing of information between domestic law enforcement and foreign intelligence investigations. Although the lack of cooperation between the FBI and the CIA may have largely resulted from institutional resistance within the agencies and legal misinterpretation,²⁷ it undoubtedly complicated counterterrorism efforts. Provisions of the Act like section 203, which permits information from domestic criminal investigations to be shared with the intelligence community,²⁸ address this problem.

USA PATRIOT Act powers are also being used, however, for a host of non-terrorism purposes, including white-collar crime, blackmail, and child-pornography investigations. For example, in a well-publicized case, the Justice Department used the Act to pursue Operation G-String, a Nevada bribery investigation involving alleged payments to local politicians in order to loosen regulations on nude dancing in strip clubs.²⁹ Private Internet communications unrelated to terrorism investigations have also been monitored under PATRIOT Act powers.³⁰ These are but a few examples of the abuses that the Act has engendered.³¹ In its haste to enact the Act, the Bush Administration relied on executive branch supervision—rather than meaningful review by the judiciary—to ensure that such abuses do not occur. The Administration said, in effect, “Trust us.” But the nation’s political system relies on checks and

3127); *see also* Podesta, *supra* note 24, at 3.

26. USA PATRIOT Act § 206, 115 Stat. at 282 (amending 50 U.S.C. § 1805(c)(2)(B)); *see also* Podesta, *supra* note 24, at 4.

27. *See Tenth Public Hearing of the National Commission on Terrorist Attacks Upon the United States* 59 (Apr. 13, 2004) (testimony of former U.S. Attorney General Janet Reno) (“It’s not going to be legislation necessarily. It’s not going to be legal authorities. It’s going to be people sitting down and starting to exchange information, starting to share, starting to trust each other, starting to end the culture that says this is mine, I’ve got to keep it to me because it’s my case.”), at http://www.9-11commission.gov/archive/hearing10/9-11Commission_Hearing_2004-04-13.htm (site archived Sept. 20, 2004); NAT’L COMM’N ON TERRORIST ATTACKS UPON THE UNITED STATES, STAFF STATEMENT NO. 9: LAW ENFORCEMENT, COUNTERTERRORISM, AND INTELLIGENCE COLLECTION IN THE UNITED STATES PRIOR TO 9/11, at 11-12 (2004), *available at* http://www.9-11commission.gov/staff_statements/staff_statement_9.pdf (last visited Mar. 29, 2005); Jamie S. Gorelick, Editorial, *The Truth About “the Wall”*, WASH. POST, Apr. 18, 2004, at B7.

28. USA PATRIOT Act § 203, 115 Stat. at 278-81 (amending FED. R. CRIM. P. 6, 18 U.S.C. §§ 2510, 2517, and 50 U.S.C. § 403-5d); *see also* Podesta, *supra* note 24, at 3-4.

29. *See* Michael Isikoff, *Show Me the Money*, NEWSWEEK, Dec. 1, 2003, at 36; John Johnson, *The Talk of Las Vegas Is Operation G-String*, L.A. TIMES, Dec. 21, 2003, at A24.

30. *See* Eric Lichtblau, *U.S. Uses Terror Law To Pursue Crimes From Drugs to Swindling*, N.Y. TIMES, Sept. 28, 2003, § 1, at 1.

31. *See also supra* note 23.

Lost in Cyberspace?

balances for a reason: One branch of government cannot justify its actions based solely on its word alone.³²

Outside of its expansive exercise of Patriot Act powers for domestic law-enforcement purposes, the Administration's record on terrorism prosecutions is also disturbing. In a report analyzing Department of Justice prosecution data for the two-year period between September 2001 and September 2003, the Transactional Records Access Clearinghouse discovered that—although more than 6400 individuals were recommended for prosecution for terror-related crimes—the median sentence for those convicted of international terrorism was only fourteen days and 1800 cases were closed without conviction.³³ In addition, many terrorism prosecutions announced by the Administration to great fanfare have collapsed due to prosecutorial misconduct.³⁴

The Bush Administration has also revived Hoover's practice of maintaining secret lists. The FBI and the CIA have compiled "no-fly" lists that have targeted political activists engaged in lawful civil disobedience.³⁵ And in the days after September 11, several major airlines, including American, United, and Northwest, secretly handed to the government millions of passenger records that contained private information, including names, travel destinations, and credit-card numbers.³⁶ The government's missteps have not been limited to gathering excessive amounts of information in secret; it has also disseminated faulty information to the general public. Soon after September 11, the FBI released a massive list of individual names to hundreds of companies, including

32. *Cf. supra* notes 12-20 and accompanying text. The error of this approach is vividly displayed in the scandal of American human rights abuses in military prisons across the world. In taking the unprecedented, and unnecessary, step of discarding the protections of the Geneva Conventions after September 11 and insisting that the President's actions in the war on terrorism were beyond review, the Administration's legal positions arguably set in motion the chain of events which resulted in harrowing stories of abuse, humiliation, and—in some cases—torture by American personnel of foreign prisoners of war and detainees. *See* Neil A. Lewis, *Justice Memos Explained How To Skip Prisoner Rights*, N.Y. TIMES, May 21, 2004, at A10; Robert O. Boorstin, *Tossing Aside the Geneva Conventions, Bush Decisions Place U.S. Troops in Greater Danger*, Center for American Progress, at <http://www.americanprogress.org/site/pp.asp?c=biJRJ8OVF&b=79532> (May 18, 2004); *see also* Ali v. Rumsfeld, No. 1:05-CV-01201 (N.D. Ill. filed Mar. 1, 2005) (alleging that Defense Secretary Donald Rumsfeld bears direct responsibility for the torture and abuse of detainees in U.S. military custody, in violation of both the U.S. Constitution and international law).

33. TRANSACTIONAL RECORDS ACCESS CLEARINGHOUSE, CRIMINAL TERRORISM ENFORCEMENT SINCE THE 9/11/01 ATTACKS, at <http://trac.syr.edu/tracreports/terrorism/report031208.html> (Dec. 8, 2003). The Justice Department has also inflated the number of terrorism convictions by misclassifying its data related to terrorism prosecutions. *See* GEN. ACCOUNTING OFFICE, REPORT NO. GAO-03-266, JUSTICE DEPARTMENT: BETTER MANAGEMENT OVERSIGHT AND INTERNAL CONTROLS NEEDED TO ENSURE ACCURACY OF TERRORISM-RELATED STATISTICS (2003), available at <http://www.gao.gov/atext/d03266.txt> (last visited Mar. 29, 2005).

34. *See* David Cole, Editorial, *The D.C. Gang that Couldn't Shoot Straight*, L.A. TIMES, Sep. 19, 2004, at M5; Danny Hakim & Eric Lichtblau, *After Convictions, the Undoing of a U.S. Terror Prosecution*, N.Y. TIMES, Oct. 7, 2004, at A1.

35. *See* Dave Lindorff, *Grounding the Flying Nun*, SALON.COM, July 25, 2003, at http://www.salon.com/news/feature/2003/07/25/no_fly.

36. *See* John Schwartz & Micheline Maynard, *Airlines Gave F.B.I. Millions of Records on Travelers After 9/11*, N.Y. TIMES, May 1, 2004, at A10.

rental car agencies, data collection companies, and casinos, in an effort called Project Lookout. The list was riddled with so many errors, and changed hands so many times, that differing versions ended up all over the country and the world. Soon after releasing the list, the FBI determined that it was obsolete, but due to distribution over the Internet, it was too late to retrieve the list.³⁷

The Bush Administration's response to September 11 has presented the American people with a false choice: that either we can maintain our nation's proud heritage of robust protection for civil liberties *or* that we can effectively secure our nation from the threat of terrorism. From John Ashcroft's Hoover-like assault on due process standards and other constitutional rights, to the continually expanding reach of executive branch authority, many of the Bush Administration's policies after September 11 have unfortunately inflicted damage *not* on the ability of terrorists to harm our nation, but instead on the basic freedoms guaranteed to all Americans by the very Constitution that we are supposed to be defending.

III. THREATS OF CYBERTERRORISM

Cyberterrorism remains in many ways an enigmatic threat, the danger of which depends on its very definition.

At its most extreme, cyberterrorism refers to the potential for a debilitating, full-scale digital assault—often referred to as a “Digital Pearl Harbor”—in which multiple attacks are launched against telecommunications networks, city power grids, and/or air traffic control systems, causing widespread destruction and possible loss of life.³⁸ When the electricity blackout struck a large swath of the United States on August 14, 2003, many initially wondered whether terrorists were responsible.³⁹ Although the blackout fortunately did not signal the beginning of a long-feared era of such large-scale cyberattacks, two-thirds of the nearly 1300 technology experts polled by the Pew Internet & American Life Project believe a “devastating” attack will be launched on the Internet or power grid in the next decade.⁴⁰ Robert Gates, the director of the CIA during

37. See Ann Davis, *FBI's Post-Sept. 11 'Watch List' Mutates, Acquires Life of Its Own*, WALL ST. J., Nov. 19, 2002, at A1.

38. For various descriptions of “cyberterrorism” and how a large-scale cyberattack might affect the United States, see David Talbot, *Terror's Server*, TECH. REV., Feb 2005, at 46, available at http://www.techreview.com/articles/05/02/issue/mag_toc.asp (last visited Mar. 13, 2005); Chris Cobbs, *'Digital Pearl Harbor' Worries Computer Experts*, ORLANDO SENTINEL, Mar. 24, 2004, at C1; Swartz, *supra* note 2; Council on Foreign Relations, *Cyberterrorism*, at http://cfrterrorism.org/terrorism/cyberterrorism_print.html (last visited Mar. 29, 2005); and Robert Lemos, *What Are the Real Risks of Cyberterrorism?*, ZDNET.COM, Aug. 26, 2002, at http://news.zdnet.com/2100-1009_22-955293.html.

39. See Philip Shenon, *Agency Quickly Concludes No Terrorists Were Involved*, N.Y. TIMES, Aug. 15, 2003, at A24.

40. SUSANNAH FOX ET AL., PEW INTERNET & AMERICAN LIFE PROJECT, *THE FUTURE OF THE INTERNET 14-15* (2005), available at http://www.pewinternet.org/pdfs/PIP_Future_of_Internet.pdf (last visited Mar. 13, 2005).

Lost in Cyberspace?

the 1990s, said cyberterrorism could be the most potent weapon of mass destruction facing the nation,⁴¹ while some fear that cyberterrorism's most lethal application could come as a "force multiplier" in conjunction with a more conventional terrorist attack (for example, a digital attack on emergency-communications infrastructures in the aftermath of a traditional bombing or chemical attack).⁴² Cyberterrorism can also be considered to encompass the problem of lax cybersecurity, which permits viruses, worms, and other tools to propagate in cyberspace at a cost of approximately fifteen billion dollars per year to the global economy.⁴³ Poor cybersecurity for critical infrastructure such as dams, chemical plants, and power plants has the potential to inflict significant harm on the public.⁴⁴ Complicating protection, nearly ninety percent of our nation's critical infrastructure is owned by the private sector rather than the government.⁴⁵ In the second half of 2002 alone, sixty percent of power and energy companies experienced at least one severe cyberattack;⁴⁶ thankfully, none was catastrophic.

Many experts, however, consider the potential danger of cyberterrorism and cybersecurity to be overblown and misdirected.⁴⁷ Rather than securing the nation against the specter of a catastrophic digital attack, they argue that attention must be paid to the more routine uses of the Internet by terrorists—communication, fundraising, and spreading propaganda. The very features that have fueled the Internet's exponential growth—"ease of access, lack of regulation, vast potential audiences, and fast flow of information"⁴⁸—are in many ways the same factors that attract terrorists. For example, in just the last eight years, the number of websites sponsored by

41. See Brian Kladko, *Experts See 'Devastating' Attack on the Internet in Next 10 Years*, RECORD (Bergen County, N.J.), Jan. 10, 2005, at A1.

42. See Gellman, *supra* note 44; Council on Foreign Relations, *supra* note 38.

43. See Joshua Green, *The Myth of Cyberterrorism*, WASH. MONTHLY, Nov. 2002, at 8, 9.

44. See *Virtual Threat, Real Terror: Cyberterrorism in the 21st Century: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108th Cong. (2004) (testimony of Dan Verton), at <http://judiciary.senate.gov/hearing.cfm?id=1054> (last visited Mar. 29, 2005); CLAY WILSON, CONG. RESEARCH SERVICE, COMPUTER ATTACK AND CYBER TERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 7-10 (2003), available at <http://www.fas.org/irp/crs/RL32114.pdf> (last visited Mar. 29, 2005); Barton Gellman, *Cyber-Attacks by Al Qaeda Feared*, WASH. POST, June 27, 2002, at A1; Jon Marino, *Cyber-Terrorism Warning Sounded*, L.A. TIMES, Feb. 25, 2004, at A17.

45. Robert L. Hutchings, Chairman of the National Intelligence Council, Speech Before the International Security Management Association (Jan. 14, 2004), available at www.cia.gov/nic/speeches_terror_and_econ_sec.html (last visited Mar. 29, 2005).

46. See Rick White & Stratton Sclavos, Editorial, *Targeting Our Computers*, WASH. POST, Aug. 15, 2003, at A27.

47. See, e.g., GABRIEL WEIMANN, WWW.TERROR.NET: HOW MODERN ISLAM USES THE INTERNET (U.S. Inst. of Peace, Special Report No. 116, 2004), available at <http://www.usip.org/pubs/specialreports/sr116.pdf> (last visited Mar. 29, 2005); Green, *supra* note 43, at 8; Louise Richardson, Executive Dean of the Radcliffe Institute of Advanced Study, *The Myth of Cyberterrorism: The Internet as a Tool or Target of the Terrorists*, Lecture Before the Center for Research on Computation and Society (Feb. 24, 2005).

48. WEIMANN, *supra* note 47, at 1.

terrorists has increased from a dozen to 4350,⁴⁹ and new tools for encrypting messages are used nearly every day.⁵⁰ In addition, terrorists have been some of the leading culprits behind the growing problem of cyberfraud, as they have used the Internet as a “cash cow,” swiping credit card numbers, phishing for personal finance information, and stealing business documents.⁵¹ Credit card companies and banks lost more than \$1.2 billion in the United States to online fraud in 2003 alone.⁵² Cyberfraud has become such a pervasive method of terrorist financing that Imam Samudra, the mastermind of the October 2002 bombings in Bali, Indonesia, entitled a chapter of his recent jailhouse autobiography “Hacking, Why Not?”⁵³ The chapter details basic information on money laundering, online credit-card fraud, and computer programming languages, exhorting all would-be terrorists to use cyberspace to further jihad.⁵⁴

The diverse aspects of cyberterrorism are in many ways unsurprising. Technological advances occur on a daily basis, and terrorist networks evolve constantly, making threat assessment an inexact science at best. However, while serious questions have been raised about the technological capacity of terrorist groups to execute an attack approximating a “Digital Pearl Harbor”—or even penetrate critical infrastructure because of poor cybersecurity—it is known that al Qaeda and other terrorist operatives have researched extensive computer networks in the United States⁵⁵ and that terrorists generally gravitate to a target’s largest vulnerabilities.⁵⁶ Hence, despite differing opinions about the precise nature of the threat, there is little dispute that the threat must be met swiftly before it is too late. And in doing so, constitutional rights and liberties can be, and must be, scrupulously observed. Society’s widespread reliance on computer networks demands that those networks, and cyberspace itself, become more secure while adequate civil-liberties safeguards are observed.

A. *The Clinton Years: Problem Recognized, but Not Enough Done*

The Clinton Administration recognized cyberterrorism as a serious problem

49. See Swartz, *supra* note 2.

50. See Todd M. Hinnen, *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet*, 5 COLUM. SCI. & TECH. L. REV. 3, at 5-6 (2003-2004), at <http://www.stlr.org/cite.cgi?volume=5&article=5>; Tom Zeller Jr., *On the Open Internet, a Web of Dark Alleys*, N.Y. TIMES, Dec. 20, 2004, at C1.

51. See Swartz, *supra* note 2; Talbot, *supra* note 38, at 46.

52. See Talbot, *supra* note 38, at 46.

53. See Alan Sipress, *An Indonesian’s Prison Memoir Takes Holy War into Cyberspace*, WASH. POST, Dec. 14, 2004, at A19.

54. See *id.* In this chapter of his book, Sumada reportedly boasts: “Any man-made product contains weakness because man himself is a weak creature. So it is with the Americans, who boast they are a strong nation.” See *id.*

55. See Gellman, *supra* note 44; Green, *supra* note 43, at 11; Marino, *supra* note 44.

56. See WILSON, *supra* note 44, at 31-32; Hutchings, *supra* note 45.

Lost in Cyberspace?

and made it a primary component of national security strategy, but the Administration also recognized the critical importance of concomitantly safeguarding of our civil liberties. The President's Commission on Critical Infrastructure Protection led to the issuance of Presidential Decision Directive 63, which established a cyberterrorism command structure in the federal government and committed the government to addressing critical vulnerabilities in its information systems.⁵⁷ The Administration also established the Cyber Corps program, in which top students were paid to study computer security for two years in exchange for their commitment to work for the government upon completion of their studies.⁵⁸

The Clinton Administration also took seriously the essential role of the private sector in combating cyberterrorism and the need to encourage both the government and the private sector to elevate the low priority often given to cybersecurity. A survey has found that only seventeen percent of CEOs from small to midsized companies have taken steps to secure their information systems.⁵⁹ Former counterterrorism official Richard Clarke was fond of saying that the typical company spends one-quarter of one percent of its information technology budget on cybersecurity—slightly less than it spends on coffee.⁶⁰ Although many discussions were held with private-sector representatives, cooperation was not always easy. Industry leaders often said the networked world moves too fast and the competition is too fierce for them to collaborate with government on security.⁶¹ The principle that the market—not governmental involvement—would produce optimal solutions was constantly invoked.⁶² Initiatives aimed at increasing the responsibility of the private sector for policing its networks, closing security vulnerabilities, or helping to uncover terrorist activity were almost uniformly resisted.

Part of the reason the Clinton Administration did not succeed in this effort was because the threat from terrorism seemed too distant and abstract, and the discussions lacked a sense of urgency. Then came September 11.

57. See Presidential Decision Directive/NSC-63 on Critical Infrastructure Protection (May 22, 1998), available at <http://www.fas.org/irp/offdocs/pdd/pdd-63.pdf> (last visited Mar. 29, 2005); see also Press Briefing by Richard Clarke, National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, & Jeffrey Hunker, Director of the Critical Infrastructure Assurance Office (May 22, 1998) (explaining the Decision Directive), available at <http://www.fas.org/irp/news/1998/05/980522-wh3.htm> (last visited Mar. 29, 2005).

58. See Jim Landers, *In Cyber Wars, Uncle Sam Wants Youth*, DALLAS MORNING NEWS, Sept. 9, 1999, at 1A.

59. See White & Slavos, *supra* note 46.

60. See Green, *supra* note 43, at 12-13.

61. See John Podesta, Editorial, *Tools for Counterterrorism*, WASH. POST, Sept. 19, 2001, at A33.

62. See, e.g., Jonathan Krim, *Who Should Keep Out the Hackers?*, WASH. POST, Apr. 22, 2004, at E1.

B. The Bush Administration: Opportunity Missed

September 11 provided a tragic opportunity to make badly needed reforms, as government and industry alike realized the need to move at warp speed to assess new threats, evaluate vulnerabilities, and build on steps already taken. Unfortunately, the Bush Administration missed this historic opportunity. As a result, it is not clear that the nation is safer from the threat of cyberterrorism today than it was four years ago—indeed, many experts have suggested that the opposite is true⁶³—while civil liberties have simultaneously been disregarded in alarming ways.

President Bush's National Strategy to Secure Cyberspace,⁶⁴ released with little fanfare in early 2003, originally contained important mandates on the private sector. Some of these included: requiring Internet Service Providers (ISPs) to provide firewalls to consumers; holding ISPs liable for traffic that attacked the Internet; establishing an industry-supported cybersecurity fund; holding companies' boards of directors responsible for computer security; and forming corporate security councils to regularly review business-continuity plans and risks posed by vendors. But these reforms were pulled at the last minute in order to give more time for "industry input," an example of the Administration's unwillingness to prod businesses to improve cybersecurity.⁶⁵ It appears that cyberterrorism has become another problem like global warming, where accepted wisdom is turned on its head based on industry demands, making our nation less secure as a result. The National Strategy also reflected the Administration's lack of emphasis on protecting civil liberties—civil liberties are referenced just four times in the seventy-six page document.⁶⁶

One of the most glaring problems with the Administration's approach has been its inability to elevate concerns over cybersecurity *within* the government; in the process, it has failed to implement the recommendations outlined in its own National Strategy after September 11. Prior to the creation of the Department of Homeland Security (DHS), responsibility for cybersecurity and cyberterrorism was located within the White House, with a direct line to the President.⁶⁷ Such responsibility now lies in a small agency within DHS—the

63. See, e.g., Bob Keefe, *Net Without a Safety Net; Tech Industry Says Feds Aren't Doing Enough*, ATLANTA J.-CONST., Dec. 5, 2004, at 1Q; Brian Krebs & Jonathan Krim, *Another Computer Security Official Quits; Critics Say Division Lacks Aggressiveness*, WASH. POST, Jan. 12, 2005, at E1.

64. WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003), available at http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf (last visited Mar. 29, 2005); see also Aaron Davis, *Internet Security Strategy Released*, SAN JOSE MERCURY NEWS, Feb. 15, 2003, at 1C; Jonathan Krim, *Cyber-Security Strategy Depends on Power of Suggestion*, WASH. POST, Feb. 15, 2003, at E1; Jennifer 8. Lee, *White House Scales Back Cyberspace Plan*, N.Y. TIMES, Feb. 15, 2003, at A14.

65. See Davis, *supra* note 64; Green, *supra* note 43, at 13; Krim, *supra* note 64; Lee, *supra* note 64.

66. WHITE HOUSE, *supra* note 64, at x, 3, 14-15, 20.

67. See Jonathan Krim, *Cyber-Security to Get Higher-Profile Leader*, WASH. POST, Oct. 13, 2004,

Lost in Cyberspace?

National Cyber Security Division—which has been in virtual disarray since its creation.⁶⁸ The cybersecurity division's director reports only to an assistant secretary of DHS. Concern over this diluted authority was so widespread that bipartisan legislation, supported by industry and many members of Congress, would have elevated the director to an assistant secretary level.⁶⁹ Although it appeared close to passage, the Administration blocked it from becoming law.⁷⁰

DHS's own inspector general concluded that DHS efforts to combat cyberterrorism and improve cybersecurity were hobbled by poor coordination, poor communication, and the absence of clear priorities.⁷¹ For example, the Administration initially announced that nearly 800 people were scheduled to transfer from the FBI to Homeland Security to work on cybersecurity; only twenty-two did.⁷² The division's director stepped down last October due to his frustration over the low priority the Administration has placed on cybersecurity.⁷³ He was the third person to leave the position in just eighteen months; the division's deputy director recently departed as well.⁷⁴ Unsurprisingly, confusion remains on how government agencies will respond to a cyberattack and whether an adequate cyberterrorism threat assessment has been conducted.⁷⁵

The Administration's failure to take active steps to address cybersecurity is also evident in its approach to policymaking. For example, despite its \$60 billion technology budget, it has not effectively used the federal government's leverage as one of the nation's largest purchasers of software to spur change, nor has it effectively leveraged government contractors to raise security standards.⁷⁶ Even the private sector has—most tellingly—concluded that not

at A11.

68. See Keefe, *supra* note 63; Krim, *supra* note 67.

69. See Krim, *supra* note 67; Jonathan Krim, *Report Faults Cyber-Security*, WASH. POST, July 23, 2004, at E1 [hereinafter Krim, *Report Faults Cyber-Security*].

70. See Krebs & Krim, *supra* note 63; Krim, *Report Faults Cyber-Security*, *supra* note 69. Curiously, in an October 2004 speech, former DHS Secretary Tom Ridge announced the elevation of the director of the cyber division to an assistant secretary level, only to have his comments refuted by the Administration hours later. See Krim, *supra* note 67.

71. OFFICE OF INSPECTOR GEN., DEP'T OF HOMELAND SEC., PROGRESS AND CHALLENGES IN SECURING THE NATION'S CYBERSPACE 10-14 (2004), available at http://www.dhs.gov/interweb/assetlibrary/OIG_CyberspaceRpt_Jul04.pdf (last visited Mar. 29, 2005); see also Krim, *Report Faults Cyber-Security*, *supra* note 69.

72. See John Mintz, *Government's Hobbled Giant; Homeland Security Is Struggling*, WASH. POST, Sept. 7, 2003, at A1; Telephone Interview with Michael Vatis, Founding Director of the National Infrastructure Protection Center (Feb. 26, 2004).

73. See Robert O'Harrow, Jr. & Ellen McCarthy, *Top U.S. Cyber-Security Official Resigns*, WASH. POST, Oct. 2, 2004, at A18.

74. See Krebs & Krim, *supra* note 63.

75. See Drew Clark, *Senators Press Bush Administration on Cybersecurity Effort*, NAT'L J.'S CONGRESSDAILY (morning ed.), Feb. 25, 2004, at 20.

76. See Davis, *supra* note 64; Jonathan Krim, *U.S. Goals Solicited on Software Security; Task Force Suggests Limited Regulation*, WASH. POST, Apr. 2, 2004, at E2; Lee, *supra* note 64.

enough has been done to secure cyberspace.⁷⁷ The Business Roundtable has called attention to the need for increased cybersecurity,⁷⁸ and an alliance of technology companies has advocated for greater administrative efforts to guard against cyberterrorism. A leader of this effort stated simply, “The executive branch must exert more leadership.”⁷⁹

Compounding the Administration’s inadequate response to cyberterrorism is that it has, in the process, needlessly infringed on civil liberties. Rather than pursuing common-sense steps to secure cyberspace and critical infrastructure, the Administration has pursued policies that have violated constitutional principles without increasing our security. A recent effort by the Administration illustrates the point. In an attempt to gain more information about terrorist activity online, the Justice Department has begun to investigate terrorist websites—an unobjectionable and worthwhile endeavor. However, those investigations have now led to government attempts to charge criminally, under the USA PATRIOT Act’s prohibition against disseminating “expert advice or assistance” to terrorist groups, individuals operating websites that include objectionable material,⁸⁰ even if those individuals did not create the material. The government’s first target was Sami Omar Al-Hussayen, a doctoral student in Idaho who maintained websites that the government alleged contained jihadist-related activities.⁸¹ The sites did contain both information praising terrorists as martyrs as well as anti-Semitic material, but even the government admitted that the “most militant” were not authored by Al-Hussayen.⁸² Despite a month-long trial in which the government presented evidence from more than 20,000 emails and 9000 phone calls, a jury acquitted

77. See Brian Krebs, *Tougher Cyber-Security Measures Urged*, WASH. POST, Dec. 8, 2004, at E5; Krim, *Report Faults Cyber-Security*, *supra* note 69.

78. See Jonathan Krim, *Old Economy Fed Up with Cyber-Security*, WASH. POST, May 20, 2004, at E1.

79. See Krebs, *supra* note 77 (quoting Paul B. Kurtz, a former senior cybersecurity official in the Bush Administration and executive director of the Cyber Security Industry Alliance, a non-profit trade group of hardware and software companies dedicated to the improvement of cybersecurity). Congressional attention to cybersecurity has unfortunately been lacking as well, complicating meaningful oversight. Three different committees in the House of Representatives—Energy and Commerce, Homeland Security, and Judiciary—have retained jurisdiction over various aspects of cyberterrorism and cybersecurity. See Tim Starks, *Players: In His Second Term as a House Freshman, Dan Lungren Takes Charge of Critical Homeland Issues*, CQ.COM, Mar. 7, 2005, available at http://www.house.gov/apps/list/speech/ca03_lungren/030705Playersprofileofdanlungren.html (last visited Mar. 29, 2005). “Congress’ reluctance to reform its internal structures means that [Homeland Security Secretary] Tom Ridge’s successor will still be reporting to scores of committees and subcommittees. . . . Until meaningful reform of congressional oversight occurs, our national security will suffer.” Martin Kady II, *House Package of Rules for 109th Muddies Homeland Panel’s Turf*, CONG. Q. WEEKLY, Jan. 10, 2005, at 68, 68 (quoting Thomas H. Keat and Lee H. Hamilton, chairman and vicechairman of the National Commission on Terrorist Attacks Upon the United States) (alteration in original).

80. See Eric Lipton & Eric Lichtblau, *Online and Even Near Home, a New Front Is Opening in the Global Terror Battle*, N.Y. TIMES, Sept. 23, 2004, at A12.

81. See Talbot, *supra* note 38, at 49.

82. See Lipton & Lichtblau, *supra* note 80.

Lost in Cyberspace?

Al-Hussayen of the terrorism-related charges.⁸³ Jurors interviewed after the trial said the government was trying to convict Al-Hussayen for exercising his First Amendment right to free speech.⁸⁴

In other areas, the government has likewise spent precious resources collecting information in cyberspace, in a manner that could violate constitutional rights, with little security benefit. For example, the revised FBI Guidelines, implemented by former Attorney General Ashcroft, remove important safeguards on the FBI's ability to indiscriminately peruse websites and chat rooms on the Internet.⁸⁵ In addition, an FBI bulletin in 2003 advised local police to monitor anti-war rallies because anti-war protestors "often use the internet" and engage in "peaceful techniques that can create a climate of disorder."⁸⁶ And recently, it was revealed that a CIA-funded effort is developing technologies to monitor chat room conversations.⁸⁷ Perhaps the most notorious project launched during the Bush Administration was Total Information Awareness (T.I.A.), spearheaded by Admiral John Poindexter, President Reagan's former national security adviser convicted of lying to Congress, conspiracy, obstruction of justice, and destroying evidence in connection with the Iran-Contra scandal (a conviction later overturned on procedural grounds).⁸⁸ T.I.A. promised to be a grand database capable of searching all other databases, tracking vast amounts of digital and physical

83. See Timothy Egan, *Sensing the Eyes of Big Brother, and Pushing Back*, N.Y. TIMES, Aug. 8 2004, § 1, at 20.

84. See *id.*; see also Lipton & Lichtblau, *supra* note 80.

85. The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations 6 (May 30, 2002), available at <http://www.usdoj.gov/olp/generalcrimes2.pdf> (last visited Mar. 29, 2005). For a critical assessment of the new Guidelines and their potential to erode civil liberties without measurably improving security, see JERRY BERMAN & JAMES X. DEMPSEY, CTR. FOR DEMOCRACY AND TECH., CDT'S GUIDE TO THE FBI GUIDELINES: IMPACT ON CIVIL LIBERTIES AND SECURITY—THE NEED FOR CONGRESSIONAL OVERSIGHT, at <http://www.cdt.org/wiretap/020626guidelines.shtml> (June 26, 2002); see also GEN. ACCOUNTING OFFICE, REPORT NO. GAO-03-759T, FBI REORGANIZATION: PROGRESS MADE IN EFFORTS TO TRANSFORM, BUT MAJOR CHALLENGES CONTINUE 26-32 (2003) (instructing Congress, as well as the Department of Justice, to exercise vigilant oversight and to ensure the existence of adequate internal controls in implementing the Guidelines, which otherwise have great potential to lead to civil liberty abuses), available at <http://www.gao.gov/new.items/d03759t.pdf> (last visited Mar. 29, 2005).

86. Fed. Bureau of Investigation, FBI Intelligence Bulletin No. 89 (Oct. 15, 2003), reprinted in Fed. Bureau of Investigation, *FBI Response to Media Misinterpretation of its Law Enforcement Sensitive Intelligence Bulletin*, dated 10/15/2003, at <http://www.fas.org/irp/agency/doj/fbi/fbi112503.html> (last visited Mar. 29, 2005); see also Sixth Public Hearing of the National Commission on Terrorist Attacks Upon the United States 28-29 (Dec. 8, 2003) (statement of Richard Ben-Veniste, Member of the National Commission on Terrorist Attacks Upon the United States) (criticizing the Bulletin as containing a "particularly squishy" definition of terrorism and questioning whether "we [are] overreacting . . . creating a climate in this country that is so counterproductive to our ideals that we ought to look at it midcourse and make some suggestions regarding correcting it"), at http://www.9-11commission.gov/archive/hearing6/9-11Commission_Hearing_2003-12-08.pdf (site archived Sept. 20, 2004).

87. See Zeller, *supra* note 50.

88. *United States v. Poindexter*, 951 F.2d 369 (D.C. Cir. 1991); see also David Johnston, *Poindexter Wins Iran-Contra Case in Appeals Court*, N.Y. TIMES, Nov. 16, 1991, § 1, at 1.

personal information—email, credit card transactions, travel reservations, and medical care—in order for the government to anticipate and thwart terrorist plots and activities. After a public outcry, Total Information Awareness became “Terrorism Information Awareness,” despite keeping the same focus and scope. Even this was too much for Congress, which cut its funding for domestic use.⁸⁹

The Administration’s approach to airline security—an area in dire need of improvement in the wake of September 11—exemplifies the Administration’s approach to sacrificing civil liberties in ways that do not materially enhance our safety. An airline passenger screening system, known as CAPPs (Computer Assisted Passenger Pre-Screening System) was first developed to identify suspicious patterns among air travelers. After September 11, the Administration developed CAPPs II, a system designed to authenticate passengers’ identities and assign them color-coded risk levels through the use of extensive commercial databases. Serious errors with the system prompted Congress to withhold funding for deployment and implementation. The Administration claimed to replace CAPPs II with the new “Secure Flight” program, but it too will rely on commercial data to conduct automated analysis of passenger records.⁹⁰ The government recently required airlines to submit millions of passenger records in order to test the system,⁹¹ yet a special report issued in February by the FBI and Homeland Security concluded that commercial aviation remains vulnerable to a major terrorist attack.⁹² Rather than continuing its ever-expanding acquisition of personal information, a promising alternative approach is an identification card that would permit “trusted travelers” to bypass long security lines in exchange for their voluntary submission of personal information; a pilot program doing just that began last June.⁹³

Based on nearly all independent standards of measurement, the Administration has failed to meet the challenge that cyberterrorism poses; in the process, our nation is less safe and less free.

89. See Carl Hulse, *Congress Shuts Pentagon Unit Over Privacy*, N.Y. TIMES, Sept. 26, 2003, at A20; see also Robert Pear, *Panel Urges New Protection on Federal ‘Data Mining’*, N.Y. TIMES, May, 17, 2004, at A12 (discussing recommendation of a federal advisory committee that Congress pass laws more protective of Americans’ civil liberties to counteract intrusive government data-mining techniques that “resemble the Pentagon program initially known as Total Information Awareness”).

90. See Jay Boehmer & Jay Campbell, *CAPPs II Curbed, ‘Trusted’ Traveler Test Gets Okay*, BUS. TRAVEL NEWS, Mar. 29, 2004, at 1; Sara Kehaulani Goo, *Report Faults TSA on Privacy; New Computer Screening System Could Be Delayed Again*, WASH. POST, Feb. 13, 2004, at A7; Sara Kehaulani Goo & Robert O’Harrow, Jr., *TSA Readies Revised Aviation Screening*, WASH. POST, Aug. 26, 2004, at A12.

91. See Sara Kehaulani Goo, *Air-Travel Screening Snagged*, WASH. POST, Nov. 20, 2004, at E1.

92. See Eric Lichtblau, *Security Report On U.S. Aviation Warns of Holes*, N.Y. TIMES, Mar. 14, 2005, at A1.

93. See Wilson P. Dizard III, *TSA Will Test Registered Traveler Pilot*, NEWSBYTES, Apr. 5, 2004, LEXIS, News Library, Computing & Technology Stories File.

Lost in Cyberspace?

IV. CONCLUSION: WHERE TO GO FROM HERE

Combating cyberterrorism while safeguarding civil liberties is not an easy task. Were a major act of cyberterrorism to occur, it is likely the Administration's tendency to intrude on rights and liberties in the physical world and cyberspace would continue its expansion.⁹⁴ Yet we know many steps could be implemented that would be effective and protect our liberties. The following steps should be considered:⁹⁵

1) Empowering the recently created Privacy and Civil Liberties Oversight Board through the appointment of seasoned advocates and technological experts who understand and take seriously the protection of civil liberties in digital age.⁹⁶

2) Promoting the director of cybersecurity to an assistant secretary position within the Department of Homeland Security.

3) Requiring the federal government's procurement contracts for purchasing software and technological equipment to include security patches and increased protection from programming vulnerabilities.⁹⁷

In addition, the following steps—designed to safeguard our constitutional liberties by scaling back some of the Administration's most unnecessary and potentially abusive policy initiatives—should also be considered:

4) Tightening the authority on roving wiretaps by requiring the identification of the targeted person and confirmation that the targeted person is using the particular device. Without these changes, the government has unchecked authority to conduct widespread surveillance, including, for example, the innocent online activities of computer users at public terminals.⁹⁸

94. One survey found that fifty-nine percent of technology experts predict that the public will be subjected to increased surveillance in the future as electronic devices continue to proliferate. FOX ET AL., *supra* note 40, at 22-23.

95. The Center for American Progress, along with the Center for National Security Studies and the Center for Democracy and Technology, has detailed dozens of specific legislative and regulatory recommendations, many of which are outlined in a report released in October 2003. See CENTER FOR AMERICAN PROGRESS ET AL., *supra* note 24.

96. See CTR. FOR AMERICAN PROGRESS, SECURING AMERICA, PROTECTING OUR FREEDOMS AFTER SEPTEMBER 11, at 14-15 (2005), available at http://www.americanprogress.org/atf/cf/{E9245FE4-9A2B-43C7-A521-5D6FF2E06E03}/pp_civil_liberties.pdf (last visited Mar. 29, 2005); Richard A. Clarke, *Real ID's, Real Dangers*, N.Y. TIMES, Mar. 6, 2005, § 6 (Magazine), at 20.

97. See Krim, *supra* note 76.

98. See CENTER FOR AMERICAN PROGRESS ET AL., *supra* note 24, at 16-17.

5) Requiring the Attorney General to publicly report appropriate data to Congress regarding delays in notification of the search and seizure of property and the use of the surveillance authority provided by the Foreign Intelligence Surveillance Act.⁹⁹

6) Strengthening meaningful judicial oversight of law enforcement and intelligence investigations carried out under USA PATRIOT Act authorities, particularly with regard to web surfing, the use of grand jury testimony, and wiretapping by intelligence authorities. Judicial oversight provides an important check on potentially unconstitutional actions, improves the quality of investigations, and ensures confidence in the legal system.¹⁰⁰

7) Requiring that surveillance and monitoring of South Asian, Middle Eastern, and Arab American communities be tied to suspicion of actual criminal conduct. Crude racial and ethnic profiling creates a culture of fear and suspicion in the very communities whose cooperation is vital for successful counterterrorism efforts, thereby undermining law-enforcement efforts.¹⁰¹

Public-private partnerships are also critical in addressing the threat of cyberterrorism. Five years ago, the federal government tackled a threat of unknown dimensions in averting the Y2K crisis. Although the seriousness of the crisis was undetermined, the government and industry acted responsibly, working together to avert possible disaster. This was accomplished not by pushing for draconian regulations or statutory mandates, but simply by requiring that businesses disclose their Y2K efforts to their shareholders. The right incentives were created by government; market forces then took hold.¹⁰²

More innovation along these lines is needed. In 2001, California enacted a law requiring government agencies and private companies to give timely notice to consumers when personal data is stolen from government or company databases.¹⁰³ Requiring notice—without mandating substantive measures—incinivizes both companies and the government to improve security and respect the privacy of consumers. Senator Dianne Feinstein has proposed similar legislation that would expand California's law to the nation.¹⁰⁴

99. *See id.* at 17-18, 22-23.

100. *See id.* at 16-23.

101. *See id.* at 9; COLE, *supra* note 3, at 53-54.

102. *See* Green, *supra* note 43, at 13.

103. CAL. CIV. CODE § 1798.92-.97 (West 2004).

104. Notification of Risk to Personal Data Act, S. 115, 109th Cong. (2005).

Lost in Cyberspace?

Such disclosure could be extended to internet service providers, requiring them to disclose in SEC filings when they have been hacked. This would create a win-win situation: Consumers would have more information about the services and privacy protections for which they pay, and companies would likely take swift steps to reduce their vulnerabilities in order to maintain consumer confidence and avoid legal liability. Lack of disclosure has been one of the chief obstacles to improved cybersecurity. After all, as Justice Brandeis wrote decades ago: “Sunlight is said to be the best of disinfectants”¹⁰⁵

* * *

History reminds us of the need to be diligent in guarding our civil liberties in times of great threat. Our pursuit of terrorists has expanded from airports and highways to cyberspace and the digital world, making the choice we face all the more stark: to learn from the mistakes of the past or simply to repeat them. With this history in mind, we offer one final suggestion: removing J. Edgar Hoover’s name from the FBI Building in Washington D.C. In its fight against terrorism, this Administration has taught us that symbols are important and can have a significant effect on policy; removing Hoover’s name would be a powerful symbol that the government will no longer treat civil liberties as expendable in times of crisis.

105. LOUIS D. BRANDEIS, *OTHER PEOPLE’S MONEY: AND HOW THE BANKERS USE IT* 62 (1914).