1-1-2007

The Chilling Effect of Government Surveillance Programs on the Use of the Internet By Muslim-Americans

Dawinder S. Sidhu
University of New Mexico - School of Law

THE CHILLING EFFECT OF GOVERNMENT SURVEILLANCE PROGRAMS ON THE USE OF THE INTERNET BY MUSLIM-AMERICANS

DAWINDER S. SIDHU*

I. INTRODUCTION

Al-Qaeda used the Internet to covertly plan and execute the terrorist attacks of September 11, 2001 and each of its subsequent terrorist plots. As the Internet became a vital tool for Muslim extremists, it also became a target of government surveillance measures. In particular, the government developed and utilized several programs to monitor Internet usage and gather relevant electronic evidence about terrorist threats.

Some have suggested that Muslims in the United States have modified aspects of their daily lives to avoid harassment or suspicion. Following 9/11, members of leading Arab and Muslim advocacy organizations informally reported that some U.S. Muslim-Americans are reluctant to use the Internet because they fear that their Internet use is or will be monitored by government officials. These Muslim-Americans fear that the U.S. government will take adverse actions against them, including reviewing their immigration status or placing them on "no-fly" lists. Indeed, one staff attorney said that some Muslim-Americans are so concerned about government surveillance that they resist the use of everyday forms of technology, including telephones.[1]

However, the effect of government surveillance measures on the use of Internet technology has not been formally or scientifically addressed. To fill this void, a survey of Muslim-Americans was commissioned to determine if and to what extent Muslims in the United States, concerned that the government may track their online movements, have changed their use of the Internet after 9/11. The

---

* J.D., George Washington University; M.A., Johns Hopkins University; B.A., University of Pennsylvania. Founding Director, Discrimination and National Security Initiative. This article was completed as part of a fellowship at the Center for Internet and Society at Stanford Law School. I am grateful to Professor Anil Kalhan for reviewing a previous draft, Dr. Mary Outwater for her work on the survey discussed in this article, Raj Gupta for his research assistance, and to my parents for their guidance, encouragement, and love. The views expressed herein, and any errors, are solely my own.

1. E-mail from American-Arab Anti-Discrimination Committee to Dawinder S. Sidhu (July 10, 2006) (on file with author).

survey was conducted in conjunction with The University of Oklahoma's Public Opinion Learning Laboratory (OUPOLL).[2] This article presents the survey's results, which indicate that an overwhelming majority of polled Muslim-Americans believe that the U.S. government monitors their post-9/11 Internet activities, although only a limited segment of the Muslim-American population has changed its online behavior. This article statistically confirms what is known anecdotally—that Muslim-Americans not only believe the government monitors their routine activities, but that such concerns have translated into actual changes in daily behavior.

This article demonstrates that the effect of the post-9/11 climate facing Muslim-Americans pervades even ordinary aspects of contemporary life. Part II of the article discusses the legal paradigm of when discrimination has legal implications and merits government action. Part III explores al-Qaeda's sophisticated use of the Internet and summarizes the government's post-9/11 online surveillance efforts. Part IV discusses OUPOLL's survey results.

I readily acknowledge that this article is of limited focus. While it addresses only a single human consequence of the post-9/11 environment in the United States, I hope that this article will become part of a broader effort to understand the pernicious effects the post-9/11 climate environment has on Muslims and those perceived to be Muslim. Such understanding guards against the alienation and isolation of Muslims in America, which is critically important for the nation's security.[3] Finally, it is important to note that the article does not examine the legality, efficacy, or propriety of any government

2. The term "chilling effect" in this article describes when individuals otherwise interested in engaging in a lawful activity are deterred from doing so in light of perceived or actual government regulation of that activity. *See* Gayle Horn, *Online Searches and Offline Challenges: The Chilling Effect, Anonymity and the New FBI Guidelines*, 60 N.Y.U. ANN. SURV. AM. L. 735, 749 (2005) (describing two different "types of chilling effects").

3. *See* David Cole, *Enemy Aliens*, 54 STAN. L. REV. 953, 958 (2002) ("If authorities have reason to believe that there might be potential terrorists lurking in the Arab immigrant community, they would do better to work with the millions of law-abiding members of that community to obtain their assistance in identifying potential threats, than to alienate the community by treating many of its members as suspect because of their ethnicity or national origin and pursuing others under conditions of secrecy that invite fear and paranoia."); Montgomery E. Engel, Note, *Donating "Blood Money": Fundraising for International Terrorism by United States Charities and the Government's Efforts to Constrict the Flow*, 12 CARDOZO J. INT'L & COMP. L. 251, 286 (2004) ("By marginalizing and alienating Muslim-Americans the government runs the risk of encouraging the kind of anger, resentment, and resultant extremism that Americans have been victims of, at home, in the Arab world, and elsewhere.").

surveillance programs.[4] Moreover, to the extent that this article establishes the chilling effect on the use of the Internet by Muslim-Americans, the article does not argue that the chilling effect itself may serve as part of a constitutional challenge to those measures.[5] This article aims to enrich our understanding of the potential impact of government measures on Muslims in the United States, and more specifically, of the delicate state of pluralism in times of war.

II. THE LEGAL PARADIGM

Over fifty years ago, the United States Supreme Court held that Title II of the Civil Rights Act of 1964, which prohibited racial discrimination in public accommodations,[6] was a proper exercise of Congress's authority under the Commerce Clause of the U.S. Constitution.[7] The Court noted that discrimination against African-Americans by hotels had "a *qualitative* as well as *quantitative* effect on interstate travel by Negroes."[8] The Court said that the qualitative effect "was the obvious impairment of the Negro traveler's pleasure and convenience that resulted when he continually was uncertain of finding lodging."[9] As for the quantitative effect, the Court observed

4. The concern regarding the legality of such programs has been discussed elsewhere. *See, e.g.*, Frederick M. Joyce & Andrew E. Bigart, *Liability for All, Privacy for None: The Conundrum of Protecting Privacy Rights in a Pervasively Electronic World*, 41 VAL. U. L. REV. 1481, 1482 (2007) (noting that "without clear legal limits, the government has begun to expand its electronic surveillance operations to a degree not contemplated by the original laws or supported by the majority of U.S. citizens"); Peter Murphy, Note, *An Examination of the United States Department of Justice's Attempt to Conduct Warantless Monitoring of Computer Networks Through the Consent Exception to the Wiretap Act*, 34 CONN. L. REV. 1317, 1351 (2002) ("The ability of the Justice Department to conduct warrantless monitoring of computer network users through the consent exception to Title III would significantly reduce the privacy protections for communications our system has developed over the past forty years.").

5. *See* Horn, *supra* note 2, at 737 (arguing that "the existence of a *legally cognizable* chilling effect created by the grant of online investigative tools in the new Guidelines is doubtful") (emphasis added).

6. *See* 42 U.S.C. § 2000a (2000).

7. Heart of Atlanta Motel, Inc. v. U. S., 379 U.S. 241 (1964); *see also* Katzenbach v. McClung, 379 U.S. 294, 298 (1964) (characterizing the "basic holding" of *Heart of Atlanta* as finding Title II of the Civil Rights Act of 1964 to be "a valid exercise of the power to regulate interstate commerce insofar as it requires hotels and motels to serve transients without regard to their race or color").

8. *Heart of Atlanta Motel*, 379 U.S. at 253 (emphases added); *see also* Jil L. Martin, Note, *United States v. Morrison: Federalism Against the Will of the States*, 32 LOY. U. CHI. L.J. 243, 268–69 (2000) ("These combined effects on interstate commerce were found to be sufficient to enable Congress to regulate the conduct of such purely local activities.").

9. *Heart of Atlanta Motel*, 379 U.S. at 253.

that "there was evidence that this uncertainty stemming from racial discrimination had the effect of discouraging travel on the part of a substantial portion of the Negro community."[10]

This seminal ruling placed legal importance on the qualitative and quantitative effects on minorities subject to discrimination in ostensibly everyday circumstances. The ruling also recognized the ability of the legislature to address the qualitative and quantitative effects of discrimination. Moreover, the Court focused not only on the *act* of excluding African-Americans from places of accommodation, but the *experiences* of African-Americans in enduring such exclusion, for instance "having to travel great distances to secure" lodging, or "hav[ing] . . . to call upon friends to put them up overnight" when accommodations were unavailable to them.[11]

Since the terrorist attacks of 9/11, Muslim-, Arab-, Sikh-, and South Asian-Americans have been the recipients of a severe and persistent backlash. In the first week following the attacks, 645 bias crimes were directed at those perceived to be Middle Eastern.[12] In the first eight weeks after 9/11, over a thousand bias incidents were reported, including up to nineteen murders, assaults, harassment, and acts of vandalism.[13] The violence is ongoing. In 2006, for example, a turbaned Sikh in California was stabbed in the neck with a steak knife because, in the words of the local prosecutor, the perpetrator "wanted to seek revenge for Sept. 11 and attack a member of the Taliban."[14]

Reports on the post-9/11 backlash against certain ethnic groups almost exclusively focus on hate crimes and other tangible acts of discrimination. It is understandable that the discussion to combat the post-9/11 backlash focuses on tangible actions—as they are more easily reported, verified, and conveyed. Moreover, authorities, such as the Federal Bureau of Investigation, are charged with the responsibility to address legally cognizable discrimination, such as an assault or act of vandalism. It is beyond question that tangible acts of violence and discrimination deserve the attention of policymakers, the law enforcement community, and the public.

---

10. *Id.*

11. *Id.* at 252–53.

12. S. ASIAN AM. LEADERS OF TOMORROW, AMERICAN BACKLASH: TERRORISTS BRING WAR HOME IN MORE WAYS THAN ONE 3 (2001), *available at* http://old.911digitalarchive.org/documents/BiasReport.pdf.

13. Muneer I. Ahmad, *A Rage Shared by Law: Post-September 11 Racial Violence as Crimes of Passion*, 92 CAL. L. REV. 1259, 1261–62 (2004).

14. John Coté, *Hate Crime Alleged in Stabbing of Sikh; Santa Clara Suspect Could Face Life Term If He Is Convicted*, S. F. CHRON., Aug. 2, 2006, at B10.

However, a lesson of *Heart of Atlanta Motel* is applicable post-9/11: the experiences of the affected minority groups need not rise to the level of a hate crime or punishable act to warrant the public's consideration or a response from the legislature. That is, the human consequences of discrimination can have legal implications and merit governmental action. For example, the Court in *Heart of Atlanta Motel* addressed the act of hotels refusing to lodge African-Americans as well as the fact that African-Americans were discouraged from traveling due to such experiences.[15] Similarly, in the aftermath of 9/11 it is vital to examine not only instances where a turbaned Sikh has been ejected from an airplane on account of his perceived race or religion, but also where Sikh-Americans have "stopped flying altogether in the months and, in some cases, years after 9/11 to avoid potential problems."[16]

Accordingly, to the extent that the experiences of African-Americans during the civil rights era provoked social concern, led to congressional remedy, and earned judicial notice, the experiences of Muslim-, Arab-, Sikh-, and South Asian-Americans should similarly trouble those interested in ensuring that all Americans are treated with equality, dignity, and without regard to their race, religion, or national origin.[17] Indeed, the post-9/11 backlash against Muslims and those perceived to be Muslim has received some press coverage.[18] For example, in 2006 the *San Francisco Chronicle* reported that a Muslim woman, who "removes the *hijab*, as the head scarf is commonly referred to, when she goes to job interviews or has to fly[,] . . . was frustrated by repeated airport security interrogations[.]"[19] In addition, in 2007 a Sikh advocacy organization studied the harassment of Sikh students in New York City Public Schools and found, among other things, that some Sikh students cut their hair—though Sikhs are

15. *Heart of Atlanta Motel*, 379 U.S. at 253.

16. JUNE HAN, DISCRIMINATION AND NAT'L SEC. INITIATIVE, WE ARE AMERICANS TOO: A COMPARATIVE STUDY OF THE EFFECTS OF 9/11 ON SOUTH ASIAN COMMUNITIES 20 (Sept. 2006), *available at* http://www.geocities.com/dnsinitiative/911_Report.pdf.

17. *See* Thomas Ross, *Whiteness after 9/11*, 18 WASH. U. J.L. & POL'Y 223, 237 (2005) (remarking that "Flying While Brown" has "displaced its predecessor, 'Driving While Black'").

18. *See* PEW RESEARCH CTR., MUSLIM AMERICANS: MIDDLE CLASS AND MOSTLY MAINSTREAM 35 –39 (May 22, 2007), *available at* http://pewresearch.org/assets/pdf/muslim-americans.pdf (addressing the worries of Muslims in America, including concerns "about government surveillance, job discrimination, and being harassed in public").

19. Matthai Chakko Kuruvila, *9/11: Five years later: Typecasting Muslims as a Race*, S.F. CHRON., Sept. 3, 2006, at A1.

required by their faith to keep their hair unshorn[20]—in response to physical harassment.[21] Again, the value of these accounts is that they illuminate the human consequences of discriminatory treatment.

III. TERRORISM AND THE INTERNET

A. The Jihad Online

There is ample evidence that the al-Qaeda regime responsible for the terrorist attacks of 9/11 has diligently and deftly used the Internet to further its nefarious agenda.[22] Numerous academic and press sources have detailed al-Qaeda's longstanding and continuing relationship with the Internet.[23]

Al-Qaeda has utilized the power of the Internet for many years. Indeed, "[b]y the late 1990's, al-Qaeda's use of the Internet was well

---

20. *See* KHUSHWANT SINGH, A HISTORY OF THE SIKHS 84 (1978) (listing the five Sikh articles of faith, which include unshorn hair); *see also* Cheema v. Thompson, 67 F.3d 883, 884 (9th Cir. 1995).

21. SIKH COALITION, HATRED IN THE HALLWAYS: A PRELIMINARY REPORT ON BIAS AGAINST SIKH STUDENTS IN NEW YORK CITY'S PUBLIC SCHOOLS 5 (June 2007), *available at* http://www.sikhcoalition.org/advisories/documents/HatredintheHallwaysFinal.pdf. According to the report, one Sikh student noted, "I used to have a turban. I used to get into fights, and then I cut my hair." *Id.*

22. *See* Fletcher N. Baldwin, Jr. & Robert B. Shaw, *Down to the Wire: Assessing the Constitutionality of the National Security Agency's Warrantless Wiretapping Program: Exit the Rule of Law*, 17 U. FLA. J.L. & PUB. POL'Y 429, 433 n.26 (2006) (noting that "it is now widely known that al-Qaeda operatives used (and likely continue to use) Internet chat rooms and free, anonymous e-mail accounts to communicate").

23. *See, e.g.*, Todd M. Hinnen, *The Cyber-front in the War on Terrorism: Curbing Terrorist Use of the Internet*, 5 COLUM. SCI. & TECH. L. REV. 1 (2004); Aaron Nance, Note, *Taking the Fear out of Electronic Surveillance in the New Age of Terror*, 70 UMKC L. REV. 751(2002); Susan W. Brenner & Marc D. Goodman, *In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks*, 2002 U. ILL. J.L. TECH. & POL'Y 1 (2002); ROHAN GUNARATNA, INSIDE AL QAEDA: GLOBAL NETWORK OF TERROR (2002); Kasie Hunt, *Osama bin Laden Fan Clubs Build Online Communities*, USA TODAY, Mar. 9, 2006, at A04; Ronald Marks, Opinion, *Homeland Security's Biggest Challenge: Too Much Information*, CHRISTIAN SCI. MONITOR, Nov. 21, 2005, at 9; Andrew Higgins, *Uploading Terror: How al Qaeda Put Internet in Service of Global Jihad*, WALL ST. J., Nov. 11, 2002, at A1; James Risen & David Johnston, *Traces of Terror: The Intelligence Reports; Agency Is Under Scrutiny For Overlooked Messages*, N.Y. TIMES, June 20, 2002, at A20; David S. Fallis & Ariana Eunjung Cha, *Agents Following Suspects' Lengthy Electronic Trail; Web of Connections Used to Plan Attack*, WASH. POST, Oct. 4, 2001, at A24; *see also* ANTI-DEFAMATION LEAGUE, JIHAD ONLINE: ISLAMIC TERRORISTS AND THE INTERNET (2002), *available at* http://www.adl.org/Learn/internet/jihad_online.pdf, [hereinafter ADL REPORT].

underway in regard to theological and paramilitary training."[24] An insightful report on al-Qaeda and the Internet noted that "[a]l-Qaeda operatives *relied heavily* on the Internet for help in planning and coordinating the September 11 attacks."[25] The 9/11 Commission Report stated that in "the final days" before 9/11, Mohammad Atta, a 9/11 hijacker, and a key al-Qaeda operative used technology to keep in contact.[26] Aside from 9/11, it is well-established that other terrorist plots have involved extensive use of the Internet.[27]

Al-Qaeda uses the Internet for several purposes, including to train and recruit adherents, reestablish damaged cells, obtain financing, and communicate operational information.[28] Al-Qaeda has transformed the Internet into a "virtual training ground," using the Internet to instruct its members about the "cleaning and care of weapons, physical training for its foot soldiers, and the way to set up a safe house, as well as how to stage a kidnapping," among other tasks.[29]

---

24. Michael Scheuer, *Assessing London and Sharm al-Sheikh: The Role of Internet Intelligence and Urban Warfare Training* (Jamestown Found. Terrorism Focus), Aug. 5, 2005, at 7, *available at* http://jamestown.org/terrorism/news/uploads/tf_002_015.pdf.

25. ADL REPORT, *supra* note 23, at 9 (emphasis added); *see also* Nance, *supra* note 23, at 755 ("[T]he al-Qaeda cells behind the Twin Towers and Pentagon attacks used the Internet, email and cell phones to communicate about their plans.").

26. THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 248–49 (2004).

27. *See, e.g.*, Andrew Becker, *Technology and Terror: The New Modus Operandi*, PBS Frontline, Jan. 25, 2005, *available at* http://www.pbs.org/wgbh/pages/frontline/shows/front/special/tech.html ("Ramzi Yousef, the mastermind behind the 1993 World Trade Center attack, used encryption from his base in the Philippines in the mid-1990s when he plotted to blow up 11 U.S. airplanes over the Pacific."); Nathan E. Carrell, Note, *Spying on the Mob:* United States v. Scarfo*—A Constitutional Analysis*, 2002 U. ILL. J.L. TECH. & POL'Y 193, 195 n.17 (2002) ("Suspected shoe-bomber Richard Reid left data on his laptop connecting him to Al Qaeda and sent e-mails from Internet cafes.").

28. Hinnen, *supra* note 23, at 1 ("It has become increasingly clear that terrorist organizations avail themselves of the opportunities afforded by the Internet to recruit and train adherents and foot soldiers, to raise and move funds, and to plan and execute attacks.").

29. *CNN Live Saturday* (CNN television broadcast July 17, 2004), transcript *available at* http://transcripts.cnn.com/TRANSCRIPTS/0407/17/cst.03.html; *see also* Steve Coll & Susan B. Glasser, *Terrorists Turn to the Web as Base of Operations*, WASH. POST., Aug. 7, 2005, at A01 ("With laptops and DVDs . . . jihadists have sought to replicate the training . . . facilities they lost in Afghanistan with countless new locations on the Internet."); Jessica Stern, *The Protean Enemy*, FOREIGN AFF., July–Aug. 2003, at 34 ("Islamist Web sites also offer on-line training courses in the production of explosives and urge visitors to take action on their own."); Jarret M. Brachman, *High-Tech Terror: Al-Qaeda's Use of New Technology*, 30 FLETCHER F. WORLD AFF. 149, 153 (2006) (commenting on al-Qaeda's "virtual combat classrooms"); Benjamin R. Davis, Comment, *Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance*, 15 COMMLAW CONSPECTUS 119, 149 (2006) ("In late 2003, a Web site entitled 'Al Qa'ida University for Jihad Sciences' offered an online instruction manual for various terrorist attacks

For example, the perpetrators of the July 7, 2005, London and July 23, 2005, Egypt attacks "may well have profited fr[o]m the urban-warfare training al-Qaeda has made readily available on the Internet," according to the former Chief of the bin Laden Unit at the Central Intelligence Agency's Counterterrorist Center.[30]

Al-Qaeda's message can reach anyone in the digital world and thus can serve as a powerful recruitment aid.[31] The Director of Research at the Combating Terrorism Center at the United States Military Academy observed that "by leveraging new information and communication technologies, al-Qaeda has transformed itself into an organic social movement, making its virulent ideology accessible to anyone with a computer."[32] The Director further explained that "al-Qaeda's use of the Internet . . . has . . . enabled it to radicalize and empower armies of new recruits by shaping their general worldview."[33]

Similarly, the Internet has a restorative function for al-Qaeda. Following the American military campaign in Afghanistan, al-Qaeda "used the Internet to replace their dismantled training camps, reconnect their weakened organization, and reconstitute their leadership."[34] A senior security analyst noted that the distribution of al-Qaeda material over the Internet has, to a certain degree, "compensated for the loss of Afghanistan as a major training arena in both the ideological and tactical senses."[35] A commentator observed that al-Qaeda Web sites are "central to al-Qaida's strategy to ensure that its war with the US will continue even if many of its cells across the world are broken up and its current leaders are killed or captured."[36] Accordingly, the commentator noted al-Qaeda Web sites

---

including 'suicide operations.'") (citing ILAN BERMAN, AMERICAN FOREIGN POLICY COUNCIL, EURASIA SECURITY WATCH NO. 7 (2003)).

30. Scheuer, *supra* note 24, at 8.

31. *See* ADL REPORT, *supra* note 23, at 3 ("Accessible from almost anywhere on the planet and easily used to transmit thousands of pages of propaganda, the Internet helps Islamist terrorists unify and motivate their zealous adherents.").

32. Brachman, *supra* note 29, at 149.

33. *Id.* at 150.

34. *Id.* at 153.

35. Stephen Ulph, *A Guide to Jihad on the Web*, TERRORISM FOCUS, Mar. 31, 2005, *available at* http://jamestown.org/terrorism/news/article.php?articleid=2369531; *see also* John F. Murphy, *Brave New World: U.S. Responses to the Rise in International Crime—An Overview*, 50 VILL. L. REV. 375, 379 (2005) ("[I]t may be that the United States and coalition forces' invasion of Afghanistan, which caused the dispersal of Al Qaeda forces, led to greater use of the Internet by Islamic fundamentalist forces.").

36. Clive Walker, *Cyber-Terrorism: Legal Principle and Law in the United Kingdom*, 110 PENN ST. L. REV. 625, 637–38 (2006) (quoting Paul Eedle, *Terrorism.com: How Does Al-Qaida Stay Organized When its Members are in Hiding and Scattered Across the World?*,

would serve to "deepen and broaden worldwide Muslim support, allowing al-Qaida or successor organisations to fish for recruits, money and political backing."[37]

Al-Qaeda also uses the Internet to raise money. In 2004, an attorney with the United States Department of Justice's Computer Crime & Intellectual Property Section identified that al-Qaeda raises funds online, in part by soliciting donations "directly via websites, chat groups, and targeted electronic mailings," soliciting funds from charitable organizations "with the express purpose of clothing, feeding, and educating a population, but with the covert intent of exploiting contributors' largesse to fund acts of violence," and "perpetrat[ing] online crimes such as identity and credit card theft, intellectual property piracy, and fraud, and support[ing] their mission with the proceeds of such crimes[.]"[38] As an example of the latter category, a British investigation found that an al-Qaeda cell "used stolen credit card numbers at hundreds of online stores to buy items that fellow jihadists might need in the field. Authorities also say the men laundered money from stolen credit card accounts through more than a dozen online gambling sites,"[39] which could then finance al-Qaeda's mission.

Furthermore, the Internet allows al-Qaeda to transmit information about its terrorist operations.[40] Al-Qaeda has used the Internet to select targets, sometimes by "prob[ing] vulnerabilities in the U.S. and elsewhere."[41] Al-Qaeda has also used the Internet to provide additional instructions in the execution of terrorist attacks, including the 2004 blasts in Egypt's Sinau Peninsula.[42]

Al-Qaeda not only developed the Internet into a valuable tool, but also conceived of creative ways to avert surveillance. For example, al-Qaeda reportedly uses e-mail to communicate without actually sending the drafted messages, thus reducing the possibility of the

---

GUARDIAN, July 17, 2002, at 4); *see also A World Wide Web of Terror*, ECONOMIST, July 14, 2007, at 36 (noting that the Internet "enabl[ed] al-Qaeda to reconstitute itself after the fall of the Taliban and its eviction from Afghanistan").

37. Walker, *supra* note 36, at 638.

38. Hinnen, *supra* note 23, at 9.

39. Brian Krebs, *Three Worked the Web to Help Terrorists: British Case Reveals How Stolen Credit Card Data Bought Supplies for Operations*, WASH. POST, July 6, 2007, at D01.

40. *See* Brachman, *supra* note 29, at 154 ("Al-Qaeda has increasingly looked to the Internet as a way of shaping military operations on the battlefield."); Davis, *supra* note 29, at 150 ("[C]ertain instructional documents illustrate a nexus between online extremist communications and subsequent terrorist operations.").

41. James W. Conrad, Jr., *The Information Quality Act—Antiregulatory Costs of Mythic Proportions?*, 12 KAN. J.L. & PUB. POL'Y 521, 531 (2003).

42. Davis, *supra* note 29, at 150.

messages' interception. Members allegedly log into a designated e-mail account, draft messages to each other, and save those messages to the account without sending them, thereby avoiding an electronic communication trail.[43] Khalid Sheik Mohammed, an al-Qaeda operative and "key planner" of 9/11, is said to have employed this strategy:[44]

> Mohammed or his operatives would open an account on a free, public e-mail service such as Hotmail, write a message in draft form, save it as a draft, then transmit the e-mail account name and password during chatter on a relatively secure message board[.] The intended recipient could then open the e-mail account and read the draft—since no e-mail message was sent, there was a reduced risk of interception, the researchers said.[45]

When al-Qaeda actually sends e-mails, it allegedly uses encryption technology or passwords to ensure that only specified recipients can read the messages.[46] Moreover, if an e-mail is intercepted, it is difficult to track down its author.[47] For example, to

---

43. *See* Renwick McLean, *Madrid Suspects Tied to E-mail Ruse; Using a Simple Trick to Avoid Detection*, INT'L HERALD TRIB., Apr. 28, 2006, at 1 ("Instead of sending the messages, the suspect . . . saved them as drafts on accounts he shared with other radicals . . . . They all knew the password and so they could access the accounts to read his comments and post replies . . . . The ruse meant that there was no digital trail that the authorities could easily trace, according to the judge and government. Had the messages been e-mailed, the government might have monitored them, as is common across Europe.").

44. Coll & Glasser, *supra* note 29, at A01.

45. *Id.*

46. *See* ADL REPORT, *supra* note 23, at 4 ("In planning the September 11 attacks, Al-Qaeda members sent each other thousands of messages in a password-protected section of an extreme Islamic Web site . . . . It is easy for terrorists to access and use the Internet anonymously, and by using encryption programs, it is simple for them to encode the messages they send to each other."); Posting of Evan Kohlmann to *Al Qaeda and the Internet*, http://www.washingtonpost.com/wp-dyn/content/discussion/2005/08/05/DI2005080501262.html (Aug. 8, 2005, 15:00 EST) ("There are numerous mailing lists, chat rooms, and sympathizer web sites that immediately advertise the new locations to Al-Qaida supporters. Increasingly, these forums are being password protected and carefully vetted so that only apparently-genuine terrorist sympathizers get advance notice of new releases on the Internet.").

47. *See* Phillip Carter, *Al Qaeda and the Advent of Multinational Terrorism: Why "Material Support" Prosecutions Are Key in the War on Terrorism*, FINDLAW, Mar. 12, 2003, http://writ.news.findlaw.com/student/20030312_carter.html ("With easily available encryption and spoofing (electronic concealment of Internet addresses) techniques, Al Qaeda operatives can send encrypted e-mail from hidden locations on the Internet to and from their commanders in the Middle East. Even with sophisticated Internet surveillance systems such as Carnivore, U.S. authorities have little hope of sorting through the vast amounts of e-mail sent every day,

protect the identity of an e-mail account holder, Hotmail "does not use a traceable IP address (which can be achieved by using an Internet terminal in a public library, Internet café, or shopping mall), and does not download information to a traceable storage mechanism like a hard-disk or floppy disk."[48]

Surprisingly, those behind the distribution of online terrorist materials may not be al-Qaeda members at all. A terrorism analyst noted that al-Qaeda outsources some of its technology needs to Internet savvy individuals willing to volunteer their time and abilities to al-Qaeda. [49] In other words, "[w]hat [Abu Musab al-] Zarqawi is unable to do on the Internet, [an unaffiliated and particularly able computer specialist] does for him."[50] Moreover, the Web sites that these individuals create are shuffled around the Internet, "sometimes several times a day," to avoid penetration by government counterterrorism officials and others.[51]

In addition to enabling al-Qaeda to covertly conduct operations, the Internet is also a potential target of al-Qaeda's terrorist activity. As the *Washington Post* noted in 2002, "[u]nsettling signs of al Qaeda's aims and skills in cyberspace have led some government experts to conclude that terrorists are at the threshold of using the Internet as a direct instrument of bloodshed."[52] In particular, al-Qaeda may use the Internet to corrupt computer networks and thus disrupt the government and business entities, such as railways and basic utilities, that rely on the smooth operation of those networks.[53] Service

---

to find the few notes sent by terrorists."); Douglas Farah & Peter Finn, *Terrorism, Inc.; Al Qaeda Franchises Brand of Violence to Groups Across World*, WASH. POST, Nov. 21, 2003, at A33 ("[A]l Qaeda members have taught individuals from other groups how to use the Internet to send messages and how to encrypt those communications to avoid detection.").

48. Walker, *supra* note 36, at 636.

49. Kohlmann, *supra* note 46.

50. *Id.*

51. Lawrence Wright, *The Terror Web: Were the Madrid Bombings Part of a New, Far-Reaching Jihad Being Plotted on the Internet?*, THE NEW YORKER, Aug. 2, 2004, at 40; *see also* ECONOMIST, *supra* note 36 ("*Jihadi* websites constantly come and go, sometimes taken down by service providers only to reappear elsewhere, sometimes shifted deliberately to stay ahead of investigators.").

52. Michelle E. Boardman, *Known Unknowns: The Illusions of Terrorism Insurance*, 93 GEO. L.J. 783, 796 (2005) (quoting Barton Gellman, *Cyber-Attacks by Al Qaeda Feared*, WASH. POST, June 27, 2002, at A1).

53. *See* Boardman, *supra* note 52, at 797 ("[T]errorists can target the Internet itself, thereby disrupting or destroying the free flow of data, leading to potentially large economic loss."); *see also* Brenner & Goodman, *supra* note 23, at 31(describing a "real-life example" in which "an Australian man hacked into a computerized waste management system . . . and 'caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel'") (quoting Tony Smith, *Hacker Jailed for Revenge Sewage*

interruptions can have considerable financial consequences for the targeted networks. For example, "Yahoo!, Amazon.com, and CNN, among others, were shut down for hours as a result of a denial of service attack attributed to a fifteen-year old boy that was estimated to have caused $1.2 billion in damage."[54]

There is little doubt that al-Qaeda regularly uses Internet technology, including e-mail and data encryption, to further its terrorist operations[55] and successfully execute its international plots.[56] The Internet holds such an important place in al-Qaeda's structure that the group specifically trains members on Internet usage. In 2002, CNN reported that "investigators discovered a house in Pakistan run by al Qaeda that was devoted solely to training for cyber-warfare and hacking, according to coalition intelligence officials. One official described it as a place to study tactics, calling it a 'cyber-academy.'"[57] As a U.S. Army War College publication stated, quite bluntly, "al Qaeda loves the Internet."[58]

B. The Government's Response

While the Internet may potentially enable al-Qaeda to spread its messages and instruct its members in covert and undetected ways, it does not provide an absolute cloak of secrecy. Technology is a double-edged sword; it can conceal identities and activities, but it can also leave "digital trails of evidence."[59] Indeed, "police hunted down the suspected kidnappers of *Wall Street Journal* journalist Daniel Pearl by

---

Attacks, REGISTER (LONDON), Oct. 31, 2001, *available at* http:// www.theregister.co.uk/ content/4/22579.html).

54. Brenner & Goodman, *supra* note 23, at 30.

55. Mary W.S. Wong, *Electronic Surveillance and Privacy in the United States After September 11 2001: The USA Patriot Act*, 2002 SING. J. LEGAL STUD. 214, 260 (2002); *cf.* Daniel Sieberg, *Bin Laden Exploits Technology to Suit his Needs*, CNN.COM, Sept. 21, 2001, http://www.cnn.com/2001/US/09/20/inv.terrorist.search/index.html (noting that while some analysts contend that Osama bin Laden has not abandoned technology, others believe "bin Laden has ditched his satellite-linked phones, mobile handsets and Internet access in favor of 'Stone Age' messaging techniques to elude law enforcement").

56. Ulph, *supra* note 35.

57. Kelli Arena & David Ensor, *U.S. Infrastructure Information Found on al Qaeda Computers*, CNN.COM, June 27, 2002, http://archives.cnn.com/2002/US/06/27/alqaeda.cyber. threat/index.html.

58. Timothy L. Thomas, *Al Qaeda and the Internet: The Danger of "Cyberplanning,"* 23 PARAMETERS 112, 112 (2003).

59. Tom Spring, *Al Qaeda's Tech Traps: Investigations, Arrests Highlight How Technology Aids and Weakens Terror Network*, PC WORLD, Sept. 1, 2004, *available at* http://www.pcworld.com/article/id,117658-page,1/article.html.

tracking e-mail that was designed to be anonymous."[60] Moreover, the frequency of e-mails sent by al-Qaeda, even if encrypted, can indicate an attack is imminent, as was the case with 9/11.[61] As a result, the Internet is an arena, just like physical space, where both terrorists and sovereigns guarding against terrorists enter to effectuate their own disparate ends.

In light of al-Qaeda's multifaceted use of the Internet to communicate and coordinate terrorist activities, as well as the intelligence that can be gained from the Internet, it is not surprising that the U.S. intelligence community has taken significant interest in the Internet. As one commentator noted, "[g]iven indications that Al Qaeda used the Internet in planning the 9/11 attacks and continues to use the Internet to spread the word of jihad and to communicate with its supporters about possible future plans, surveillance of online activity seems relevant to a police function."[62]

The government, however, took time to recognize the Internet as a critical instrument for Muslim extremists. For example, on May 8, 2002, then Federal Bureau of Investigation (FBI) Director Robert S. Mueller testified before the Senate Judiciary Committee that, "[a]s best we can determine, the actual hijackers had no computers, no laptops, no storage media of any kind."[63] As discussed above, one of the hijackers, Mohammad Atta, had used e-mail and instant messaging to communicate with an operative prior to the 9/11 attacks.[64] The FBI may have known of al-Qaeda's reliance on e-mail and instant messaging a few months later when it had evidence that the alleged twentieth hijacker, Zacarias Moussaoui, "had utilised three Hotmail accounts through his written pleadings in July and August 2002."[65] The implications of the extremists' Internet usage are now clear. A declassified summary of a 2006 National Intelligence Estimate noted that the radicalization process is occurring more quickly, more widely, and more anonymously in the Internet age, and that such groups "will

60. *Id.*

61. *See* ADL REPORT, *supra* note 23, at 5 ("Messages were discovered on Al-Qaeda computers after September 11th, by federal officials. The first relevant messages were dated May 2001 and the last were sent on September 9th, two days before the attack. The frequency of the messages was highest in August 2001. Even when messages sent by Islamist terrorists are encrypted, their increased frequency serves as a warning sign and a signal indicating that further investigation is necessary.").

62. Horn, *supra* note 2, at 758 n.128.

63. *Reforming the FBI in the 21st Century: Hearing Before S. Comm. on the Judiciary*, 107th Cong. 248, 254 (2002) (statement of Robert S. Mueller, Director, Federal Bureau of Investigation).

64. THE 9/11 COMMISSION REPORT, *supra* note 26, at 248.

65. Walker, *supra* note 36, at 636.

increasingly use the Internet to communicate, propagandize, recruit, train, and obtain logistical and financial support."[66]

Because it knows key al-Qaeda individuals took advantage of the Internet to plan the 9/11 attacks, the government has a national security interest in "monitoring and intercept[ing] communications in the electronic arena."[67] The government has consequently undertaken steps to counter al-Qaeda's online presence.[68] The Department of Homeland Security created an office that is specifically responsible for "coordinat[ing] defense against and responses to cyber attacks across the nation."[69]

In addition, the government uses several electronic surveillance programs to monitor al-Qaeda's Internet use. The government reportedly uses Carnivore, a "computer program [that] can read a suspect's e-mail and other electronic data on a real-time basis and print, or store the information for FBI agents to view or save as electronic evidence for prosecution."[70] The government also uses Echelon, a "global eavesdropping system"[71] that "links supercomputers throughout the world to 'automatically search through the millions of intercepted messages for ones containing pre-programmed keywords or fax, telex and e-mail addresses.'"[72] Echelon allegedly "played a key role in the capture of the alleged September 11 mastermind, Khalid Sheikh Mohammed . . . ."[73] The FBI reportedly also uses Key Logger Systems (KLS), which are "devices or software programs [that] are installed on a target computer and make a record of

---

66. Press Release, Dir. of Nat'l Intelligence, Declassified Key Judgments of the National Intelligence Estimate "Trends in Global Terrorism: Implications for the United States" (Apr. 2006), *available at* http://www.dni.gov/press_releases/Declassified_NIE_Key_Judgments.pdf.

67. Murphy, *supra* note 4, at 1318.

68. *See* Orin S. Kerr, *Internet Surveillance Law after the USA PATRIOT Act: The Big Brother that Isn't,* 97 NW. U. L. REV. 607, 636 (2003) ("[T]errorists groups such as Al-Qaeda were known to favor the latest Internet technologies to communicate with each other, which meant that updating the Internet surveillance laws could assist law enforcement in terrorism-related cases."); Boardman, *supra* note 52, at 796.

69. United States Computer Emergency Readiness Team, http://www.us-cert.gov.

70. John Lewis, *Carnivore—The FBI's Internet Surveillance System: Is it a Rampaging E-Mailasaurus Rex Devouring Your Constitutional Rights?*, 23 WHITTIER L. REV. 317, 318 (2001).

71. Kevin J. Lawner, *Post-Sept.11th International Surveillance Activity—A Failure of Intelligence: The* Echelon *Interception System & The Fundamental Right to Privacy in Europe*, 14 PACE INT'L L. REV. 435, 452 (2002).

72. *Id.* at 453 (quoting NICKEY HAGER, SECRET POWER 29 (1996)).

73. Oliver Burkeman & Zaffar Abbas, *How Mobile Phones and an £18m Bribe Trapped 9/11 Mastermind*, GUARDIAN, Mar. 11, 2003, *available at* http://www.guardian.co.uk/alqaida/story/0,12469,911860,00.html.

every keystroke entered while the computer is running."[74] Magic Lantern, a KLS program developed by the FBI, "is a Trojan horse computer virus that can be inadvertently activated by the target opening an email attachment or by being coaxed into visiting a predetermined website configured to release the virus."[75]

In sum, there is little doubt that al-Qaeda used the Internet and similar technology to plan and coordinate 9/11 as well as other terrorist efforts, and that al-Qaeda continues to utilize the Internet to further its goal to harm the United States and its interests.[76] Therefore, the U.S. intelligence community has implemented programs to monitor the Internet for evidence of terrorist planning and to protect against an attack on the infrastructure of the Internet itself. The question that will be explored in the next section is whether these facts—both the terrorists' use of the Internet and the government's efforts to track the Internet for information on terrorist activity—have resulted in Muslims-Americans altering their Internet use.

IV. SURVEY OF MUSLIM-AMERICANS

A. Methodology

The following presents the methodological details for a survey of United States residents who identify themselves as Muslim-American conducted in May, June, and July of 2007 by OUPOLL.[77] The survey attempts to gauge any changes in Internet use among Muslim-American respondents since the events of 9/11.

The survey was conducted solely by telephone.[78] Interviewers were provided with scripted introductions and fallback statements designed to help them gain the cooperation of respondents.[79] The

74. Nance, *supra* note 23, at 768.

75. *Id.* at 770.

76. *See, e.g.*, Murphy, *supra* note 35, at 379 (noting, in 2005, that "there are now more than four thousand terrorist Web sites").

77. This survey would not have been possible without the tireless efforts of Dr. Mary Outwater, the principal investigator of the survey. This section is adapted from a report provided by Dr. Outwater on July 6, 2007 (on file with author).

78. Each interviewer underwent a project briefing before making any calls. The questionnaire in its entirety was reviewed and all aspects of the survey were discussed during this training session. Interviewers then reviewed the questionnaire multiple times individually before making any calls.

79. The scripted introductions and fallback statements are available online. *Survey Questionnaire*, DISCRIMINATION & NATIONAL SECURITY INITIATIVE, http://www.dnsi.org/research/internet/appendices.html (last visited Nov. 20, 2007).

questionnaire consisted of fifteen questions, and it can be located online.[80]

The study targeted a sample of 2,800 telephone numbers purchased from Survey Sampling, Inc. OUPOLL interviewers made 13,368 call attempts to complete the interview process.[81]

Three hundred and eight complete interviews and three partially complete interviews were conducted.[82] These 311 interviews represent a margin of error of plus or minus 5.6% at a 95% confidence level. A 95% confidence level means that if the survey were conducted one hundred times with one hundred different random samples, the actual obtained results would fall within the limits of error at least ninety-five times.

B. Survey Results

Identity: Of the 311 respondents, all identified themselves as Muslims.[83]

General Internet Usage: A vast majority of respondents (80.1%) used the Internet prior to 9/11, while the rest did not. After 9/11, the Internet usage of the respondents increased 7.7%, with 87.8% stating that they have used the Internet after the terrorist attacks, while only 11.9% reporting that they have not. The trend towards greater Internet usage continued, as 90.4% of respondents note that they "currently use" the Internet, and only 9.3% state that they do not.

Views Regarding Government Surveillance: 71.7% of respondents believe (48.9% strongly, 22.8% somewhat) that the government is currently monitoring the activities of Muslims in the United States. By contrast, only 4.2% (1.6% somewhat and 2.6% strongly) disbelieve that such monitoring is taking place. Similarly, 70.7% of respondents believe (45.0% strongly, 25.7% somewhat) that

---

80. *Appendices*, DISCRIMINATION & NATIONAL SECURITY INITIATIVE, http://www.dnsi.org/research/internet/questionnaire.html (last visited on Nov. 2007).

81. In processing the sample for this study, twelve dialing attempts were allowed to reach eligible households to complete interviews. If a respondent wished to be called back at a specific time, interviewers entered an appointment time into the computer and, at the specified time, the callback would automatically be sent to an interviewer to be called. *Survey Results*, DISCRIMINATION & NATIONAL SECURITY INITIATIVE, http://www.dnsi.org/research/internet/surveyresults.html (last visited Nov. 20, 2007).

82. "Partially completed interviews" are those that were cut off before the end of the interview, for various reasons, but we were still able to obtain responses to a portion of the substantive questions.

83. The complete survey results are available, in table format, at *Survey Results*, DISCRIMINATION & NATIONAL SECURITY INITIATIVE, http://www.dnsi.org/research/internet/surveyresults.html (last visited Nov. 20, 2007).

the government is currently monitoring the Internet activities of Muslims in the United States. Only 4.8% disbelieve (2.9% somewhat, 1.9% strongly) that such monitoring is taking place.

Alterations in Behavior—Generally: 86.8% of respondents said they have not changed at all their general activities after 9/11 due to a concern that the government may be monitoring their activities. Only 11.6% of respondents changed their general activities (6.1% made slight changes, 2.3% made moderate changes, 1.6% made many changes, 1.6% made significant changes) due to this concern.

65.9% of respondents stated that they were not personally aware of any other Muslims in the United States who changed, in any way, their general activities after 9/11, because of a concern that the government may be monitoring their activities. 25.4% of respondents stated they were personally aware of any other Muslims in the United States who changed, in any way, their general activities after 9/11, because of a concern that the government may be monitoring their activities.

Alterations in Behavior—Internet Usage: 89.1% of respondents said they have not changed their Internet usage at all—the sites they visit or the amount of time they spend on the Internet—after 9/11 due to a concern that the government may be monitoring their activities. Only 8.4% of respondents changed their Internet usage (3.9% made slight changes, 1.6% made moderate changes, 1.9% made many changes, 1.0% made significant changes) due to this concern. Of those who stated that they have made changes in their Internet usage, 57.6% noted that they did not visit websites after 9/11, because of a concern that the government may be monitoring their online activities.

77.2% of respondents stated that they were not personally aware of any other Muslims in the United States who changed, in any way, their Internet usage after 9/11, because of a concern that the government may be monitoring their activities. 11.9% of respondents stated they were personally aware of any other Muslims in the United States who changed, in any way, their Internet usage after 9/11, because of a concern that the government may be monitoring their activities. Of these respondents, 45.6% stated that they are personally aware of other Muslim-Americans who have not visited certain web sites after 9/11, because of a concern that the government may be monitoring their online activities.

V. CONCLUSION

The survey indicates that Muslim-Americans overwhelmingly believe that since 9/11 the U.S. government has monitored their general and online activities. The government has a clear interest in tracking the behavior, online and otherwise, of terrorists. It appears, though, that Muslim-Americans believe that the post-9/11 government surveillance measures reach not only suspected terrorists, but also ordinary Muslims in the United States; the net cast by the electronic monitoring is, in other words, over inclusive.

The percentage of Muslim-Americans that have altered their use of the Internet, however, is modest when compared to the percentage of those who believe they are under the government's watchful eye. What accounts for the difference between the belief that the government is monitoring the Internet activities of Muslim-Americans and resultant changes in online behavior is unclear and must be addressed in another forum; it would be mere speculation at this point to provide possible reasons for this gulf.

Nonetheless, the survey results demonstrate that there is a segment of the Muslim-American population that has modified its Internet usage to avoid the government's intelligence programs. This begs the question: how else have Muslim-Americans changed the quality of their lives because of a concern that they may be swept up as part of the government's search for terrorists and terrorist-related intelligence? This also needs to be further explored.

There are measures to ensure that such human consequences do not occur and that the concern underlying those urges to alter one's life are minimized, if not eliminated. Perhaps the most important of these is to develop stronger ties between federal agencies and the Muslim-American community, allowing agencies to assure the Muslim-American community of its interest in terrorists, not Muslims, and to cultivate a culture of trust, mutual cooperation, and appreciation.[84]

Finally, senior members of the U.S. government should sever the harmful association between the Muslim religion and terrorism to help convince Muslim-Americans that Muslims are not categorically suspect or considered part of monitoring programs solely because of their religion. In this respect, American leadership may want to borrow

84. A stronger relationship between the federal agencies and the Muslim-American community would not only help to reduce the human consequences of the post-9/11 environment in America, but would also aid the United States in its intelligence gathering efforts, as tips from moderate Muslims may help expose more radical and extremist individuals.

a poignant statement from Indian Prime Minister Manmohan Singh, a Sikh, who said after the July 7, 2005, bombings in London: "I do believe that terrorism has no religion, terrorists have no religion and that they are a friend of no religion. No religion in the world preaches atrocities against innocent men, women and children . . . ."[85]

85. Press Briefing, Tony Blair, Prime Minister of Great Britain and Manmohan Singh, Prime Minister of India (Sept. 8, 2005), *available at* http://www.number-10.gov.uk/output/Page8152.asp. Dr. Singh also said more recently, after the failed terrorist plots in London and Glasgow, "A terrorist is a terrorist and has no religion or community." Emily Wax, *Indian Doctors Fear Bomb Plot Backlash*, WASH. POST, July 6, 2007, at A10.