LEGAL UPDATE

LAW AND TECHNOLOGY OF SECURITY MEASURES IN THE WAKE OF TERRORISM

Stacy Blasberg[*]

I. INTRODUCTION

On September 11th, terrorist attacks on the Pentagon and World Trade Center shook the nation's sense of security and notion of imperviousness on home territory. The emotions of the people of America became immediately apparent: anger towards the attackers, sorrow for those who were lost, fear for lives and the lives of those loved, and pain for a nation that lost so much all at once. Complete and utter astonishment exacerbated these feelings; the coordination and execution of a terrorist attack so large in scope and so damaging was completely missed by a country prided on sophisticated security. The United States government responded by immediately passing legislation intended to put an end to terrorism, fill the void in national security measures, and rebuild the nation's sense of safety.[1]

II. SEPTEMBER 11TH TERRORISM LINKS NATIONAL SECURITY WITH TECHNOLOGY

In the wake of these attacks, the government discovered "that information on the hijackers' activities was available through a variety of databases at the federal, state, and local government levels as well as within the private sector."[2] In light of this discovery, President Bush formally recognized modern information technology as an essential tool for making the United States more secure and resolved to institute a program to use technology to better protect the nation against future terrorism.[3]

In his plan for increased information management, Bush proposed to "build a system that combines threat information and then transmits it as needed to all relevant law enforcement and public safety officials," both among Federal agencies and departments and among the Federal, State and local

---

[*] Candidate for J.D., Boston University School of Law, 2003; M.S., Northwestern, 1998; B.S., Tufts University, 1997.

[1] *See, e.g.*, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub.L. 107-56, 115 Stat. 272.

[2] George W. Bush, *Using 21st Century Technology to Defend the Homeland, available at* http://www.whitehouse.gov/homeland/21st-technology.html (last visited Aug. 20, 2002).

[3] *See id.*

governments.[4] The President hoped to bridge the communication gaps between these groups by establishing "a uniform national threat advisory system to inform Federal agencies, State and local officials, as well as the private sector, of terrorist threats and appropriate protective actions."[5]

Under the constraints of the Fourth Amendment and until Sept. 11, "United States law [set] forth the type of legal processes required before a government authority may compel the production of information from a private individual or organization, as well as the standard that the government must meet before obtaining such process."[6] These laws and governing standards needed to be changed in order to permit the type of surveillance and information compiling to facilitate the President's plan. In preparation of implementing a long-term program for using advanced information management, the government submitted proposals to expand powers of surveillance and data accumulation.[7]

III. FOURTH AMENDMENT LIBERTIES AND LEGISLATION TO INCREASE SURVEILLANCE

The United States Constitution guarantees "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures"[8] and protects against "private property taken for public use."[9] The Fourth and Fifth Amendments imply a right to privacy and seek to balance the protection of "human freedom while accommodating legitimate law enforcement needs."[10] The Fourth Amendment prohibits only unreasonable searches and seizures and the test of reasonableness varies depending on the circumstances.[11] However, in times of an emergency such as terrorist threats and attacks, the government has great latitude in circumventing these Constitutional rights.[12]

---

[4] *Id.*

[5] *Id.*

[6] Wiley Rein & Fielding LLP, *The Search & Seizure of Electronic Information: The Law Before and After the USA Patriot Act*, *available at* http://www.ala.org/washoff/matrix.pdf (Jan. 18, 2001), at note 2.

[7] *See Anti-Terror Legislation So Far*, *available at* http://civilliberty.about.com/library/weekly/ aa100401a.htm (last visited Aug. 22, 2002)*; see also* Jim McGee, *Bush Team Seeks Broader Surveillance Powers*, WASH. POST, Dec. 2, 2001, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A44003-2001Dec1?language=printer (last visited Aug. 22, 2002).

[8] U.S. Const. amend. IV.

[9] U.S. Const. amend. V.

[10] Professor Lewis R. Katz, *Anti-Terrorism Laws: Too Much of a Good Thing*, *available at* http://jurist.law.pitt.edu/forum/forumnew39.htm (last visited Aug. 22, 2002).

[11] *See id.*

[12] *See* Dan Levine, *What Now? War and Our Civil Liberties*, HARTFORD ADVOCATE, *available at* http://www.hartfordadvocate.com/articles/whatnow.html (last visited Aug. 22, 2002). Levine notes:

The United States government has a dubious history of disregarding civil liberties in

The FBI began installing "Carnivore", its Internet monitoring system, on Internet services providers (ISPs) within hours of the September attacks.[13] The FBI also invoked the Foreign Intelligence Surveillance Act ("FISA")[14] to compel AOL and Earthlink to produce their email records.[15] Two days later, the United States Senate unanimously approved the Combating Terrorism Act 2001[16] expanding state surveillance powers by limiting the statutory need for a court approval before Carnivore and wiretapping surveillance can take place.[17] On September 20, Bush sent the draft "Mobilization Against Terror Act" to Congress.[18] The proposed legislation would further expand the power of authorities to install Carnivore in computer systems, use the Echelon[19] data collection system in violation of the Fourth Amendment, wiretap phones, obtain voicemail messages, peruse the records of businesses, credit card companies and ISPs, and obtain DNA samples from convicted felons.[20]

However, the most sweeping legislation was enacted on October 26, 2001

---

wartime. In 1861, President Abraham Lincoln suspended the writ of habeas corpus, which allowed authorities to detain citizens without bringing charges against them. And in 1942, over 100,000 Japanese Americans were taken from their homes on the West Coast and thrown into internment camps.

Id.

[13] *See* Declan McCullagh, *Anti-Attack Feds Push Carnivore*, *at* http://www.wired.com/news/politics/0,1283,46747,00.html (Sept. 12, 2001). "The FBI's controversial Carnivore spy system, which has been renamed DCS1000, is a specially configured Windows computer designed to sit on an Internet provider's network and monitor electronic communications." *Id.*

[14] Pub. L. No. 95- 511, 92 Stat. 1783 (1978) (codified as amended at 18 U.S.C. §§ 2511, 2518- 2519 (2000), 47 U.S.C. § 605 (2000), 50 U.S.C. §§ 1801-1811 (2000)). FISA allows federal agents to conduct electronic surveillance for the purpose for foreign intelligence purposes.

[15] *See Web Helps FBI Terror Investigation*, TECH TV.COM, *available at* http://www.techtv.com/news/specialreport/print/0,23102,3347518,00.html (Sept. 13, 2001); *see also* Paul Eng, *Scouring Cyberspace: Tapping the Internet for Clues on the Attack on America*, *at* http://abcnews.go.com/sections/scitech/DailyNews/WTC_netsearch010913.html (Sept. 13, 2001).

[16] *See* Senate Amendment 1562, 147 Cong. Rec. S9401 (daily ed. Sept. 13, 2001).

[17] *See* Declan McCullagh, *Senate Oks FBI Net Spying*, WIRED.COM, *avilable at* http://www.wired.com/news/politics/0,1283,46852,00 (Sept. 14, 2001).

[18] *See* Declan McCullagh, *Bush Submits His Laws for War*, WIRED.COM, *available at* http://www.wired.com/news/politics/0,1283,47006,00.html (Sept. 20, 2001).

[19] *See* Mike Zarrilli Jr., *The History of Echelon*, *at* http://www.skidmore.edu/~m_zarril/History.htm (last visited Aug. 23, 2002). Echelon is a automated global interception and relay system operated by the UK-USA intelligence agreement, which gathers communications (including phone calls, e-mail messages, Internet downloads, etc.) and then distributes the information that is most desired to the country that desires the information. *Id.*

[20] See *id.*; *see also* Sandy Starr, *Online Insecurity*, *at* http://www.spiked-online.com/articles/00000002D288.htm (Oct. 19, 2001).

when Congress passed, and Bush signed into law, the USA Patriot Act ("the Act"), an acronym for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism."[21] The Senate voted 98-1 for the bill, with only Senator Russ Feingold opposing it, and the House voted 357 to 66 to pass it.[22] The Act makes changes to over fifteen different statutes including the Electronic Communications Private Act of 1986 ("ECPA"),[23] the Computer Fraud and Abuse Act ("CFFA"),[24] the Foreign Intelligence Surveillance Act of 1978 ("FISA"),[25] the Family Education Rights and Private Act ("FERPA"),[26] the Cable Act,[27] the Federal Wiretap Statute,[28] and the Federal Rules of Criminal Procedure.[29] The Act was in accordance with Bush's umbrella plan to formulate methods of isolating and protecting critical governmental information carrying vital communications and to provide alerts and warning for terrorist threats.[30]

The Act gives broad new powers of surveillance to the government and law enforcement agencies and eliminates much of the judicial oversight established in the 1970s.[31] In criminal cases, law enforcement officials must no longer obey the rules of criminal law before conducting searches.[32] People can be subjected to roving wiretaps or have their homes and offices secretly searched without any demonstration of "probable cause" of a crime.[33] Surveillance can follow a targeted individual to any computer or telephone he or she might have used based on a single warrant useable anywhere in the United States.[34] Internet communications of Americans can be subject to surveillance if law

---

[21] George W. Bush, *President Signs Anti-Terrorism Bill: Remarks by the President at Signing of the Patriot Act, Anti-Terrorism Legislation* (Oct. 26, 2001), *available at* http://www.whitehouse.gov/news/releases/2001/10/20011026-5.html (last visited Aug. 22, 2002).

[22] *See* American Library Association, *USA Patriot Act: Chronology*, *at* http://www.ala.org/washoff/patriotchron.html (last visited Mar. 26, 2002).

[23] Pub. L. No. 95- 511, 92 Stat. 1783 (1978) (codified as amended at 18 U.S.C. §§ 2511, 2518- 2519 (2000), 47 U.S.C. § 605 (2000), 50 U.S.C. §§ 1801-1811 (2000)).

[24] 18 U.S.C. § 1030 (2000).

[25] 50 U.S.C. § 1801 et seq. (2000).

[26] 20 U.S.C. § 1232(g) (2000).

[27] 47 U.S.C. § 551 (2000).

[28] 18 U.S.C. § 2510 et seq. (2000).

[29] Pub. L. 107-56, 115 Stat. 272 (2001).

[30] Bush, *supra* note 1.

[31] Professor Susan Herman, *The USA Patriot Act and the US Department of Justice: Losing Our Balances?*, *available at* http://jurist.law.pitt.edu/forum/forumnew40.htm (last visited Aug. 20, 2002).

[32] *See* American Civil Liberties Union, *How the USA-Patriot Act Enables Law Enforcement to Use Intelligence Authorities to Circumvent the Privacy Protections Afforded in Criminal Cases*, *at* http://www.aclu.org/congress/l102301i.html (last visited Aug. 20, 2002).

[33] *See id.*

[34] Herman, *supra* note 30.

enforcement agents tell a judge that the surveillance is "relevant" to an ongoing criminal investigation.[35] The CIA and FBI can monitor computers and phones without having to demonstrate use by a suspect or a target of a court order.[36] If the FBI certifies to a court that it needs this information to conduct an "intelligence" investigation, it can obtain access to sensitive educational, medical, financial, mental health and other personal records.[37]

Some of the above expanded surveillance powers "sunset" after four years, and will expire on December 31, 2005 unless re-authorized by Congress.[38] However, this expiration date embedded in the law applies only to a tiny part of the massive bill. Police will have the permanent ability to conduct Internet surveillance without a court order in some circumstances.[39] Also exempt from the expiration date are investigations underway by December 2005 and any future investigations of crimes that took place before that date.[40]

The Act as written provides for very limited reporting requirements, and it is difficult to see how Congress will evaluate whether the "sunset" provisions should be renewed in four years.[41] Additionally, "Bush's war on terror is not a traditional military conflict with a clear end that can be met after US soldiers capture a city, eliminate a Taliban command post or snare Osama bin Laden himself."[42] Without this conceptual end, new surveillance powers that police receive today have the potential to become permanent.

IV. PUBLIC REACTION TO NEWLY ENACTED SURVEILLANCE LEGISLATION

A CBS/New York Times poll conducted in September 2001 asked respondents whether American's had to give up some personal freedoms in order to make the country safe from terrorist attacks.[43] Seventy-nine percent replied in the affirmative. [44] Another poll conducted late last September

---

[35] *See id.*

[36] *See id.*

[37] American Civil Liberties Union Massachusetts, *The USA Patriot Act: A Civil Liberties Briefing*, *at* http://www.aclu-mass.org/legal/USApatriotact.html (last visited Aug. 22, 2000).

[38] *See EFF Analysis of the Provisions of the USA Patriot Act that Related to Online Activities*, *at* http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html (Oct. 31, 2001).

[39] *See id.*

[40] *See id.*

[41] *Id.*

[42] Declan McCullagh, *Spying: The American Way of Life?*, WIRED.COM, *at* http://wired.com/news/print/0,1294,50964,00.html (Mar. 11, 2002).

[43] *See* Cynthia Tucker, *Barr Serving as Reasonable Voice on Law Enforcement Powers*, FREE REPUBLIC.COM http://freerepublic.com/focus/news/532845/posts (Sept. 26, 2001); *see also* Public Agenda Online, *Special Edition - Terrorism*, *at* http://www.publicagenda.org/specials/terrorism/terror_pubopinion2.htm (last visited Aug. 21, 2002).

[44] *See* Public Agenda Online, *Special Edition - Terrorism*, *at* http://www.publicagenda.org/specials/terrorism/terror_pubopinion2.htm (last modified Aug. 21, 2002).

showed that 63 percent of respondents favored video monitoring on public places such as street corners.[45] The American people express the need to feel more secure and want to place more power and trust in the government to use this power properly to end terrorism.[46] Those in favor of expanded police powers feel that only by allowing the government to expand surveillance, will the government gain the information they need to put an end to the clear and present danger of the United States.[47]

But "[t]here are some signs that as September 11's shock fades, Americans are becoming more skeptical of government proposals that limit privacy and civil liberties."[48] More recent surveys show that the public support of government surveillance and electronic eavesdropping diminishes as time passes without any new attacks.[49] A national ID card system, aimed at eliminating identification counterfeiting, was initially widely accepted by the public after the attacks.[50] However these ID cards that would database information about the cardholder such as travel plans, signature, fingerprint, medical records and even gun ownership, become less accepted as time passes.[51]

The newly adopted provisions deeply concern privacy advocates, who say the new laws make it possible for snooping technologies like the FBI's Carnivore to be used indiscriminately on anyone using an Internet connection, and not just on those under suspicion for criminal acts.[52] Jill Dempsey, deputy director of the Center for Democracy and Technology, feels that "[g]iving the government more authority to collect information is likely to dramatically erode the privacy rights of Americans" and may not improve security as a tradeoff.[53] Further, privacy advocates are concerned that limiting civil liberties will actually be movement in the wrong direction in the war against terrorism.[54] As the single opposing Senator to the USA Patriot bill, Russ

---

[45] *See* Neal Boortz, *Enough About the Coalition, Let's Move!*, *at* http://www.newsmax.com/archives/articles/2001/10/4/142918.shtml (Oct. 4, 2001).

[46] Public Agenda Online, *supra* note 43; *see also* Press Release, NDAA, *Nation's Prosecutors Support Reforms to Combat Terrorism* (Oct. 3, 2001), *available at* http://www.ndaa.org/newsroom/pr_combat_terrorism.html (last visited Aug. 22, 2002).

[47] *See* Public Agenda Online, *supra* note 43

[48] McCullagh, *supra* note 40.

[49] Public Agenda Online, *supra* note 43.

[50] *See* Julia Scheeres, *Support for ID Cards Waning*, WIRED.COM, *at* http://www.wired.com/news/business/0,1367,51000,00.html (March 13, 2002).

[51] *See id.*; *see also* Boortz, *supra* note 44.

[52] *See* Senator Russ Feingold, Statement of U.S. Senator Russ Feingold On the Anti-Terrorism Bill (Oct. 24, 2001), *available at* http://www.senate.gov/~feingold/releases/01/10/102501at.html (last visited Aug. 22, 2002).

[53] William Matthews, *Privacy, Security Sides Clash*, FEDERAL COMPUTER WEEK, *at* http://www.fcw.com/fcw/articles/2002/0318/web-ppi-03-18-02.asp (last visited Aug. 22, 2002); *see also* William Matthews, *Privacy, Security Sides Clash*, *at* http://www.fcw.com/fcw/articles/2002/0318/web-ppi-03-18-02.asp (Mar. 18, 2002).

[54] Feingold, *supra* note 51 (stating that security can only be improved with the ability to

Feingold strongly cautioned that "[p]reserving our freedom is one of the main reasons that we are now engaged in this new war on terrorism. We will lose that war without firing a shot if we sacrifice the liberties of the American people."[55]

V. REALITIES OF THE LEGISLATION AT THE PRESENT TIME

The powers granted by the Act have already been enforced and the expanded surveillance has begun on many levels.[56] For example, a Justice Department ruling on October 31, 2001 permitted government agents to monitor communications between a federal detainee and his lawyers when the attorney general deems it "reasonably necessary" to deter acts of terrorism.[57] This is a large departure from the preexisting constitutional rule requiring prior court authorization for such monitoring and receives both strong support and opposition.[58]

However, beyond privacy concerns, skeptics doubt that a newly digital police force will actually even work.[59] While some spokesmen claim that terrorists and criminals are just too savvy to be caught using this increased technology and surveillance, others think that ineffectiveness has already been demonstrated.[60] Carole Samdup, spokesperson for the Democracy & Rights watchdog groups, states that "[a]ll this technology has existed for years and we still haven't arrested anyone [using it]."[61] Wiretapping and other electronic monitoring may provide evidence of the terrorism and crime after the fact rather than helping to prevent it, or may actually place vital information into the hands of terrorists.[62]

VI. CONCLUSION

It has been widely recognized that today's society operates on highly sophisticated methods and technologies.[63] Bush has stated that the proposed

---

analyze the collected information).

[55] *Id.*

[56] Katz, *supra* note 10.

[57] *See* George Lander Jr., *U.S. will Monitor Calls to Lawyers*, WASH. POST, Nov. 9, 2001, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A64663-2001Nov8?language=printer (last visited Aug. 22, 2002).

[58] *See id.*

[59] *See* Bob Sullivan, *Warming to Big Brother*, *at* http://msnbc.com/news/654959.asp (Nov. 14, 2001).

[60] *See id.*

[61] *Id.*

[62] *See id.*

[63] *See* Robyn Weisman, *Is Your Internet Service Provider Spying on You?*, *available at* http://www.newsfactor.com/perl/printer/14545 (Nov. 2, 2001).

and passed legislation "takes into account of the new realities and dangers posed by modern terrorists [and] will help law enforcement identify, dismantle, disrupt, and punish terrorists before they strike."[64] History has shown that "[t]here have been periods in our nation's history when civil liberties have taken a back seat to what appears at the time to be the legitimate exigencies of war."[65] The American people are crying out for the government to do something, anything, to end terrorism and restore the nation's sense of security. However, notwithstanding these new realities, there is much discussion of whether the recent legislation, and most importantly the USA Patriot Act, is a serious detriment to this nation's civil liberties. The recent legislation increases the government's powers, as well as the scope of technology used to enforce these powers. Only time will tell whether this legislation will achieve its goals with a proper balance to civil liberties, or whether the government will overstep it's bounds, calling the judicial system to step in and determine what is constitutionally permissible.

---

[64] *Id.*

[65] *See* Feingold, *supra* note 51.