The Controversies over Data Mining and Warrantless Searches in the Wake of September 11

by

Jeffrey A. Hart
Professor
Department of Political Science
Indiana University
Bloomington, IN 47405

Paper prepared for a panel on "Information Access, Power, and Rights," at the annual meeting of the International Studies Association, San Francisco, California, March 25-29, 2008.

Abstract: In 2004, the Congress voted to end funding for a Defense Advanced Research Projects Agency (DARPA) data mining program called Total Information Awareness (TIA) that was supposed to be used for preventing terrorist attacks. Because this was not the only data mining project established by the U.S. government after September 11, this paper examines the likely impact of the TIA cancellation on future efforts. It summarizes the controversy over warrantless wiretaps in the more recent past and then turns to the broader question of the tradeoffs between privacy and security.

Introduction

One of the greatest potential promises and threats of the information age is the ability to generate, store, transmit, and process huge amounts of data quickly and economically. The promise consists mainly in accelerating the generation and diffusion of knowledge globally; the threat derives from the possibility that governments, corporations, and other institutions might use their control over information for oppressive purposes. The concept of *surveillance* – the monitoring or close observation of behavior from above – is frequently used in works warning of the dangers associated with the rapid spread of information and computing technologies (ICTs).[1]

Surveillance, of course, was around before the information age. During the Spanish Inquistion, for example, the Inquisitor General deployed agents to uncover and report on heretical activities.

[1] See, for example, David Lyon, *The Electronic Eye: The Rise of the Surveillance Society* (Minneapolis: University of Minnesota Press, 1994); William Bogard, *The Simulation of Surveillance: Hyper Control in Telematic Societies* (New York: Cambridge University Press, 1997); David Lyon, *Surveillance Society: Monitoring Everyday Life* (Philadelphia: Open University Press, 2001).

Louis XIV deployed a large network of spies to detect and arrest dissidents. Inspector Javert, the fictional anti-revolutionary police officer of *Les Miserables*, was a notable practitioner of pre-electronic surveillance. The totalitarian governments of the twentieth century employed the secret police to spy on the citizenry and to intimidate them in order to stifle dissent. George Orwell in *Nineteen Eight-Four* envisioned a future in which "thought police" would be employed to uncover and punish "thoughtcrimes."

Michel Foucault's interest in surveillance began with his research into techniques used to control prisoners in penitentiaries and mental patients in hospitals. He uses Jeremy Bentham's idea of the *panopticon* (a sort of ideal prison) as a starting point for his theories. Foucault generalized the concept of surveillance as an essential element of power, and extended it to "self-surveillance" – the internalization of social norms and values that enables authority to be exercised invisibly.[2] Followers of Foucault, like Jean Baudrillard, Gilles Deleuze, Paul Virilio, David Lyon, and Bill Bogard, later created a school of thought called surveillance studies.[3]

An example that is frequently mentioned by critics of the contemporary trend toward electronic surveillance is the national network of closed circuit television (CCTV) cameras set up by the British government as a crime-fighting and terrorism-prevention measure. As of 2002, it was estimated that there were 500,000 CCTV cameras in London, or about one for every 14 inhabitants.[4]

In a popular Hollywood film, *Enemy of the State* (1998), Robert Clayton Dean, the character played by Will Smith, is tracked in real time by video cameras, satellite imaging, telephone wiretaps, bugging devices, and database searches. While this film clearly exaggerated the surveillance capabilities of the U.S. government of the time, it is also clear that many people in the military and in law enforcement dreamt about a future in which all this was possible.

After September 11, 2001, members of the military and law enforcement agencies saw an opportunity to realize their dreams as the country reorganized itself around the shared goal of preventing future terrorist attacks. The USA Patriot Act of 2001 and the Homeland Security Act of 2002 represented a major restructuring of the U.S. government. The Patriot Act expanded the powers of existing U.S. law enforcement agencies for the stated purpose of fighting terrorism, while the Homeland Security Act created a new cabinet-level agency, the Department of Homeland Security.

---

[2] Michel Foucault, *Surveillir et punir: Naissance de la prison* (Paris: Gallimard, 1975).

[3] For more information see the web site for the Surveillance Studies Network at http://www.surveillance-studies.net/.

[4] Michael McCahill and Clive Norris, " CCTV in London," Working Paper No. 6 in *On the Threshold to Urban Panopticon? Analyzing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts*, June 2002, http://www.urbaneye.net/results/ue_wp6.pdf.

The 9/11 Commission noted that there were a number of major intelligence failures that if avoided might have made it possible to prevent the attacks. The Immigration and Naturalization Service (INS) had records of the hijackers' entry into the country, some of whom had used their true names. The airline companies had some of the names on their reservation logs. Two of the hijackers' names were on a terrorist watch list. The Commission criticized the intelligence agencies and particularly the FBI and CIA for failing to share critical information, perhaps because of the fear of violating the Insurrection Act of 1807 that limited the role of the federal government in dealing with domestic violence and the *Posse Comitatus* Act of 1878 that limited the use of the armed forces for domestic law enforcement. The Commission called for the appointment of a Director of National Intelligence to coordinate all the intelligence activities in the U.S. government, the establishment of a National Counterterrrorism Center, and a new commitment to share counterterrorism information across agencies.[5]

One of the results of the soul searching that followed the September 11 attacks was a new willingness to beef up the capabilities of the intelligence agencies and the new Department of Homeland Security to detect and apprehend potential terrorists inside the United States. One of the technologies thought to be available to help in doing this was data mining.

Definition of Data Mining

Data mining is the "use of data analysis tools to discover previously unknown, valid patterns and relationships in large data sets."[6] Data mining is one step in a broader "knowledge discovery" process. Data mining technologies employ advanced computers and computer software to identify patterns that are not easily discerned by other methods. Data mining goes beyond data collection, access, and analysis by applying computer algorithms to detect patterns across linked data bases. The distinction is clarified in Table 1 below.

Table 1. The Evolution of Data Mining

Evolutionary Step	**Enabling Technologies**	**Product Providers**	**Characteristics**
Data Collection (1960s)	Computers, tapes, disks	IBM, CDC	Retrospective, static data delivery
Data Access	Relational databases (RDBMS),	Oracle, Sybase,	Retrospective, dynamic data

[5] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Executive Summary*, http://govinfo.library.unt.edu/911/report/911Report_Exec.htm.

[6] Jeffrey Seifert, *Data Mining and Homeland Security: An Overview* (Washington, D.C.: Congressional Research Service, updated January 18, 2007), p. 1.

(1980s)	Structured Query Language (SQL), ODBC	Informix, IBM, Microsoft	delivery at record level
Data Warehousing & Decision Support (1990s)	On-line analytic processing (OLAP), multidimensional databases, data warehouses	Pilot, Comshare, Arbor, Cognos, Microstrategy	Retrospective, dynamic data delivery at multiple levels
Data Mining (Emerging Today)	Advanced algorithms, multiprocessor computers, massive databases	Pilot, Lockheed, IBM, SGI, numerous startups (nascent industry)	Prospective, proactive information delivery

Source: Adapted from Kurt Thearling, "An Introduction to Data Mining," http://www.thearling.com/text/dmwhite/dmwhite.htm.

ChoicePoint, LexisNexis, and Acxiom are three large and successful companies that sell access to multiple databases that are maintained in their data warehouses. Table 2 provides a list of companies that sell data mining software and services.

Table 2. A List of Data Mining Vendors

Company	Headquarters	URL
Business Objects	San Jose, CA	www.businessobjects.com
Informatica	Redwood City, CA	www.informatica.com
ProClarity	Boise, ID	www.proclarity.com
Ascential Software	Westboro, MA	www.ascential.com
Cognos	Burlington, MA	www.cognos.com
Coremetrics	San Mateo, CA	www.coremetrics.com
Hyperion	Santa Clara, CA	www.hyperion.com
IBM	San Jose, CA	www.ibm.com
Microstrategy	McLean, VA	www.microstrategy.com
NCR Teradata	Dayton, OH	www.teradata.com
SAS	Cary, NC	www.sas.com
Clear Forest	Waltham, MA	www.clearforest.com

SPSS	Chicago, IL	www.spss.com
Hummingbird	Mountain View, CA	www.hummingbird.com
I-Impact	Israel	www.i-impact.com

Source: http://www.data-mining-guide.net/Data-Mining-Vendors.html.

Two of these companies, SAS and SPSS, are companies that also sell statistical analysis software frequently used in social scientific research.

Commercial applications of data mining are many and various. Amazon and Google use data mining to create focused advertisements based on a customer's past purchases or searches. Credit card companies use data mining to spot potential identity thefts.[7] Non Obvious Relationship Awareness (NORA) software developed by a company called Systems Research and Development (SRD) is used in Las Vegas to prevent fraud, cheating and theft in gambling casinos.

Before September 11, U.S. government agencies began to use data mining for a variety of purposes. For example, from the early 1990s on, the U.S. Department of the Treasury had used data mining to detect money laundering operations through its Financial Crimes Enforcement Network (FinCEN). [8]

Able Danger

U.S. government data mining efforts for counterterrorism began well before September 11. In October 1999, the chairman of the Joint Chiefs of Staff issued a directive to U.S. Special Operations Command (USSOCOM) to create a classified anti-terrorism program called Able Danger. Able Danger experimented with data mining of both classified and open source information to identify potential terrorists and terrorist operations. It targeted Al Qaeda specifically -- because of the attacks in New York (the first attack on the World Trade Towers), Kenya, Tanzania, and Yemen (on the USS Cole) – but it targeted also the paramilitary forces that U.S. troops were encountering in Bosnia. According to Patience Wait:

> For instance, as the Army prepared troops for deployment to Bosnia, "we were asked what the troops will see," the source said. "We mined information on the [Bosnian] paramilitary, on organized crime, the condition of the infrastructure, etc. And we started to see linkages."
>
> Able Danger researched small arms manufacturers in the region, and determined that American soldiers could figure out alliances by identifying which paramilitary forces or gangsters carried whose guns. It purchased photos from paparazzi in Paris that

[7] Markle Foundation, *Creating a Trusted Information Network for Homeland Security*, December 2003, http://www.markletaskforce.org/Report2_Full_Report.pdf.

[8] Mary DeRosa, *Data Mining and Analysis for Counterterrorism* (Washington, D.C.: CSIS, March 2004), pp. 4-5.

> showed crime figures out on the town, and who they were out with, shedding light on relationships between different factions.[9]

A major defender of Able Danger in Congress was Representative Curt Weldon (R-PA). Weldon testified before the Senate Judiciary Committee on September 21, 2005, that Department of Defense lawyers had ordered the data collected for Able Danger to be destroyed. An enormous amount of data had been collected from both classified intelligence sources and commercial data vendors. When erased in the summer of 2000, there were 2.5 terabytes of information in the data warehouse created by the program.

Able Danger reappeared as a controversy during and after the 9/11 Commission. Former employees argued that they had identified at least one of the September 11 hijackers, Mohammed Atta, a year before the attack and again in a chart presented to the Deputy National Security Adviser, Stephen Hadley, immediately after the attack. The Department of Defense ordered a number of these former employees not to testify at the September 21, 2005, hearings mentioned above. [10]

Total Information Awareness

In January 2002, the Defense Advanced Research Projects Agency (DARPA) established the Information Awareness Office (IAO) to bring together a variety of DARPA-funded projects that applied information technology to countering transnational threats to national security. Led by Admiral John Poindexter, the IAO started work on an experimental program called Total Information Awareness (TIA). Under Secretary of Defense Peter Aldredge explained the TIA program in a press briefing on November 2002 as follows:

> The war on terror and the tracking of potential terrorists and terrorist acts require that we search for clues of such activities in a mass of data. It's kind of a signal-to-noise ratio. What are they doing in all these things that are going on around the world? And we decided that new capabilities and new technologies are required to accomplish that task. Therefore, we established a project within DARPA, the Defense Advanced Research Project Agency, that would develop an experimental prototype -- underline, experimental prototype, which we call the Total Information Awareness System. The purpose of TIA would be to determine the feasibility of searching vast quantities of data to determine links and patterns indicative of terrorist activities.
>
> There are three parts to the TIA project to aid in this anti-terrorist effort. The first part is technologies that would permit rapid language translation, such as you -- as

---

[9] Patience Wait, "Data-mining offensive in the works," *Government Computer News* (October 10, 2005), http://www.gcn.com/print/24_30/37242-1.html.

[10] Wait; Louis Freeh, "An Incomplete Investigation: Why Did the 9/11 Commision Ignore "Able Danger"?" *Wall Street Journal* (November 17, 2005), http://opinionjournal.com/extra/?id=110007559.

> we have used on the computers now, we can -- there's voice recognition capabilities that exist on existing computers.
>
> The second part was discovery of connections between transactions -- such as passports; visas; work permits; driver's license; credit card; airline tickets; rental cars; gun purchases; chemical purchases – and events -- such as arrest or suspicious activities and so forth. So again, it try [sic] to discover the connections between these things called transactions.
>
> And the third part was a collaborative reasoning-and-decision- making tools to allow interagency communications and analysis. In other words, what kind of decision tools would permit the analysts to work together in an interagency community?
>
> The experiment will be demonstrated using test data fabricated to resemble real-life events. We'll not use detailed information that is real. In order to preserve the sanctity of individual privacy, we're designing this system to ensure complete anonymity of uninvolved citizens, thus focusing the efforts of law enforcement officials on terrorist investigations. The information gathered would then be subject to the same legal projections (sic) currently in place for the other law enforcement activities.[11]

The TIA program was embroiled in controversy from the start. The choice of Admiral Poindexter, who had been convicted for his participation in the Iran-Contra scandal (the conviction was subsequently overturned), to head the IAO made critics particularly uneasy. John Markoff published the first news story on the program in the *New York Times* on February 13, 2002.[12] Civil libertarians immediately expressed concern about potential violations of civil liberties. The American Civil Liberties Union joined forces with the conservative Eagle Forum. The Heritage Foundation and the Assocation for Computing Machinery also opposed the TIA.[13] On November 14, 2002, William Safire wrote a strongly critical editorial on the op-ed pages of the *New York Times*. Safire claimed that all U.S. citizens would be under surveillance if the program continued.[14]

Senator Russ Feingold (D-MN) introduced legislation on January 16, 2003, to suspend the TIA program. Senators Ron Wyden (D-OR) and Jon Corzine (D-NJ) were co-sponsors of similar legislation. In February 2003, Congress passed a bill suspending the actitivies of the IAO

---

[11] "Transcript of Pentagon Briefing on Poindexter's TIA Program," http://www.politechbot.com/p-04186.html.

[12] John Markoff, "Chief Takes Over at Agency to Thwart Attacks on U.S." *New York Times* (February 13, 2002), http://query.nytimes.com/gst/fullpage.html?res=9D00E0D61F3CF930A25751C0A9649C8B63.

[13] Julia Scheeres, "Bush Data-Mining Plan in Hot Seat," *Wired News*, February 6, 2003, http://www.wired.com/politics/law/news/2003/02/57568

[14] William Safire, "You are Suspect," *New York Times*, November 14, 2002, http://query.nytimes.com/gst/fullpage.html?res=9F0CE6D71630F937A25752C1A9649C8B63.

pending a report to Congress on the office's activities. On May 20, 2003, DARPA provided such a report, changing the name of TIA to the Terrorism Information Awareness program, attempting to reassure critics that it did not involve actual surveillance but was simply testing new technologies that might be used to detect terrorists in the future. Critics of the program were not reassured, Poindexter resigned, and the TIA program budget was zeroed out in the Defense Appropriations Act of 2004.[15]

Computer-Assisted Passenger Prescreening System (CAPPS II)

In 1996, the Federal Aviation Administration (FAA) provided a grant to Northwest Airlines to create a prototype system to screen airline passengers who might be hijackers. The result was the Computer-Assisted Prescreening System (CAPS or CAPPS I). Other airline adopted the system voluntarily, but in 1999 the FAA issued a rule mandating the use of CAPS for all U.S. flights. After September 11, the Transportation Safety Administration in the Department of Homeland Security began work on a Computer-Assisted Passenger Prescreening System (CAPPS II), to improve the screening of passengers. CAPPS II would color code all passengers as either green, yellow, or red. Green passengers would receive normal screening, yellow passengers would receive additional screening, red passengers would not be allowed to fly. The basic idea was to combine information provided by passengers voluntarily to the airlines with commercially available data on individuals and then apply data mining algorithms as a check on passenger identities. The TSA promised not to view directly or to store for long periods the information on individuals in its CAPPS II data warehouses.

Delta Airlines began testing CAPPS II in 2003. A consumer boycott quickly was mounted by consumer concerned about privacy. In September 2003, a news report revealed that JetBlue shared private passenger information with the Torch Concepts, a defense contractor, in September 2002, during a test of another data mining project. In January 2004, another news story revealed that Northwest had shared passenger data with the National Aeronautics and Space Administration in 2001 for yet another data mining project. The Senate Committee on Government Affairs held a confirmation hearing in June 2004 at which the acting director of the TSA, David Stone, revealed that four airlines and two travel reservations companies had provided passenger data voluntarily to TSA and/or its contractors.

Homeland Security Secretary Tom Ridge announced the dismantling of the program in July 2004. Critics in Congress focused on privacy concerns. They were supported by a variety of civil liberties groups. Ridge said that a new program in which travelers could "register" voluntarily would replace CAPPS II.[16] In August 2004, TSA announced officially the cancellation of CAPPS II and its replacement with a new system called Secure Flight. In early 2006, after spending more than $100 million on the project, TSA announced the cancellation of Secure Flight because it could not deal with the privacy concerns raised by Congress and civil liberties advocates.

---

[15] "Information Awareness Office," *Wikipedia*, *http://en.wikipedia.org/wiki/Information_Awareness_Office*.

[16] Mimi Hall and Barbara DeLollis, "Plan to Collect Flier Data Canceled," *USA Today*, July 14, 2004, http://www.usatoday.com/news/washington/2004-07-14-fly-plan_x.htm.

Multistate Anti-Terrorism Information Exchange (MATRIX)
MATRIX was developed by a Florida-based private company, Seisint, in conjuction with the Florida Department of Law Enforcement (FDLE) to facilitate collaborative information sharing for counterterrorism. Some of the initial funding came from the Department of Homeland Security. MATRIX generated High Terrorist Factor (HTF) scores for individuals based on age, gender, driver safety records, proximity to "dirty" telephone numbers, credit bureau history, and ethnicity (among others). Seisint created a list of 120,000 names of individuals with high HTF scores and provided the list to the FBI, the INS, the Secret Service, and the FDLE.

The analytical core of the MATRIX project was an application called Factual Analysis Criminal Threat Solution (FACTS) that amalgamated state and public records on individuals. FACTS included, among other items, FAA pilot licenses and aircraft ownership records, property ownership records, information on vessels registered with the Coast Guard, state sexual offender lists, federal terrorist watch lists, bankrupty filings, etc.

Beginning in the early 1980s, a Regional Information Sharing System (RISS), with data accessible via a secured intranet called RISSNET, permitted a large number of state-level agencies to share law inforcement information. After the MATRIX project created FACTS, FACTS data were made available to state agencies that subscribed to the service via RISSNET.

Like TIA and CAPPS II, MATRIX came under withering criticism from civil libertarians. A number of states that had utilitized the FACTS data decided to opt out; some refused to participate from the outset. Federal funding of MATRIX ended in 2005 and the project was discontinued.[17]

Student Exchange Visitor Information System (SEVIS)
The Student Exchange Visitor Information System (SEVIS) is an Internet-based system that collects, manages, and distributes information about exchange students and foreign visitors during their stays in the United States. It is administered by the Bureau of Immigration and Customs Enforcement of the Department of Homeland Security.

The system was first initiated in July 2001 and expanded in January 2003 to include air flight schools, language training schools, and vocational schools, in addition to colleges and universities. The program is funded largely by fees charged to foreign students and visitors included in the SEVIS data base.[18]

Automated Targeting System (ATS)

---

[17] Seifert, pp. 12-16. See also Stephen E. Fienberg, "Privacy and Confidentiality in an e-Commerce World: Data Mining, Data Warehousing, Matching and Disclosure Limitation," *Statistical Science*, Vol. 21 (2006), pp. 143-154.

[18] Shannon R. Anderson, "Total Information Awareness and Beyond: The Dangeers of Using Data Mining Technology to Prevent Terrorism," Bill of Rights Defense Committee, Northhampton, Mass., July 2004, p. 7. Available at http://www.bordc.org/threats/data-mining.pdf.

The Customs and Border Protection office of the Department of Homeland Security developed the Automated Targeting System (ATS) for "targeting, identifying, and preventing potential terrorists and terrorist weapons from entering the United States."[19] ATS receives data in real time from the Automated Commercial System (ACS), the Automated Export System (AES), the Automated Commercial Environment (ACE), and the Treasury Enforcement Communication System (TECS). It collects data directly from commercial carriers in the form of a Passenger Name Record (PNE). ATS looks at inbound and outbound cargo and passengers, and private vehicles arriving by land.[20]

The above is just a sampling of the universe of U.S. government counterterrorist data mining efforts. Table 3 provides a listing of data mining programs, including others not described above, that may also be incomplete.

Table 3. List of U.S. Federal Government Counterterrorist Data Collection and Mining Programs

Name	***Administered by***	***Period of Operation***	***Scope of Operation***	***Types of Data***
Able Danger	Defense, SOCOM	1999-2000	Al Qaeda and Bosnia	Classified and commercial
TIA	Defense, DARPA	2002-2004	Research on new counterterrorism data mining techniques	Classified and commercial
CAPPS II	Homeland Security	2001-2004	Preventing hijacking and airline-based terrorism	Airline passenger personal information
MATRIX	Consortium of States	2001-2005	Targeting of potential criminals and terrorists	State public records and law enforcement data
SEVIS	Homeland Security	2001-present	Detecting terrorists in colleges, universities, and schools	Data on exchange students and foreign visitors

[19] Department of Homeland Security, *Privacy Impact Assessment for the Automated Targeting System*, November 2, 2006, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats.pdf, p. 2.

[20] Ibid, p. 2-8.

ATS	Homeland Security	Late 1990s to present, Expanded in 2001	Preventing terrorists and terrorist weapons from entering the US	Passenger and cargo data, especially, but also other data
US-VISIT	Homeland Security	2004-present	Tracking entrants to US	Photograph and finger-print data
Project Strikeback	FBI, Education	2001-2006	Tracking college aid money to potential terrorists	Financial aid records of individuals

It is worth noting that most of the data mining programs in Table 3 had been discontinued by 2005. The main criticisms of counterterrorist data mining were:

- Inability of the programs to meet their technical goals because of poor data, faulty algorithms, interoperability problems, and the generation of too many "false positives"
- Inability of the programs to adequately address privacy concerns
- The non-transparent combination of classified and open-source data in some programs
- The general lack of transparency in most of the programs
- The potential for other forms of abuse besides privacy violations, or "mission creep" (the use of data for purposes other than those originally stated).[21]

After 2005, controversies over warrantless searches displaced, to some degree, the ongoing debate about data mining. The main link between the controversies over data mining and warrantless searches is a shared concern about the tradeoffs between security and privacy.

Warrantless Wiretaps

Even before the death of the TIA, the Bush administration had pushed for giving the National Security Agency (NSA) a greater role in domestic surveillance. For many years, the various law enforcement agencies had been advocating an updating of the laws governing wiretaps to permit new forms of surveillance appropriate to the electronic age. NSA had already begun to ask telecommunications companies like AT&T to provide access to their central office switches so that the NSA could collect data on telephone calls and Internet usage. The Communications for Law Enforcement Act of 1994 mandated that telecommunications carriers design their equipment to permit surveillance by law enforcement agencies. In short, the carriers had to create "back doors" to their digital switches to facilitate government investigations.

An AT&T employee in San Francisco named Mark Klein blew the whistle on a San Francisco operation involving the NSA in 2005. Klein claimed that the NSA was basically copying and archiving all the data passing through the San Francisco switching station. Klein's information led to the filing in 2006 of a major class-action law suit, *Hepting v. AT&T*, that charged AT&T

[21] Seifert; Fienberg; Anderson; more to be added.

was illegally permitting and assisting the government to unlawfully monitor the communications of a large part of the US population.[22]

In February 2003, the Department of Justice drew up plans for a new law, the Domestic Security Enhancement Act (DSEA), that would expand the ability of law enforcement agencies to gather data from the Internet and other sources. Attorney General John Ashcroft believed that the existing law governing the gathering of intelligence, the Foreign Intelligence Surveillance Act (FISA) of 1978 was not well suited to the task of gathering intelligence on the activities of terrorists, particularly those operating within the territory of the United States.[23] The DSEA, also called Patriot Act II or Son of Patriot, would have permitted searches and surveillance without warrants or court orders. It also called for the creation of DNA data bases of suspected terrorists, immunity from civil liability for individuals and firms providing private information to the government, expansion of the list of crimes eligible for the death penalty, criminalization of the use of encryption technologies for protecting "incriminating communications," and the revocation of citizenship and deportation of U.S. citizens who support terrorists.[24] After the draft of the bill was leaked to the press, strong opposition from civil libertarians led the administration to search for other methods to achieve their aims.

In March 2004, Vice President Richard Cheney asked White House counsel Alberto Gonzalez and White House Chief of Staff Andrew Card to visit the hospital bed of Attorney General John Ashcroft who was recovering from gall bladder surgery to authorize the renewal of a secret surveillance program for the NSA that had been created soon after the September 11 attacks. The program permitted the NSA to monitor phone calls and e-mails between the United States and foreign countries without warrants. When he got wind of this visit, acting Attorney General James Comey rushed to the hospital to convince Ashcroft that he should not sign off. Lawyers at the Department of Justice had reviewed and questioned the legality of the program. Comey threatened to resign. FBI Director Robert Mueller was also opposed and threatened to resign.[25] As a result, President Bush intervened and the program was restructured to be consistent with the requirements of FISA.

This was not the end of warrantless searches, however. On May 11, 2006, an article published in *USA Today* reported that the NSA "had been secretly collecting the phone call records of tens

---

[22] Ellen Nakashima, "A Story of Surveillance: Former Technician 'Turning In' AT&T over NSA Program," *Washington Post*, November 7, 2007, p. D1. See http://www.eff.org/cases/hepting for the full text of the complaint and further documentation.

[23] FISA permitted a variety of surveillance techniques other than traditional phone wiretaps and bugging. For example, there was a section of FISA that permitted electronic surveillance, keystroke logging of computers, and the installation of spyware. All of these required warrants from the specially created FISA courts, however, but Ashcroft and other members of the Bush administration found this to be too cumbersome.

[24] For the full text of the proposed legislation, see http://www.loyalnine.com/DSEA2003_text_Patriot_Act_2.

[25] Dan Eggen, "Official: Cheney Urged Wiretaps," *Washington Post*, June 7, 2007, p. A3.

of millions of Americans, using data provided by AT&T, Verizon, and BellSouth."[26] In June 2006, the *New York Times*, *Los Angeles Times*, and the *Wall Street Journal* reported that the CIA and the Treasury Department had gained access to financial records from a vast international database housed at the Society for Worldwide Interback Financial Telecommunication (SWIFT) in Belgium.[27]

The story about the NSA resulted in the filing of over forty lawsuits against the government and the telecommunications agencies claiming violations of various privacy protection laws including the First and Fourth Amendments of the Constitution and the Foreign Intelligence Surveillance Act (FISA).[28]

The story about SWIFT resulted in a ruling by the Belgian government in September 2006 that SWIFT had violated both Belgian and European privacy laws by sharing data on cross-border wire transfers with the US government. The Belgian ruling was upheld by an EU committee, with the result that European authorities asked the U.S. government to cease and desist. U.S.-European and intra-European discussions were held. In November 2006, the *Wall Street Journal* quoted the negotiators as follows:

> U.S. diplomatic and law-enforcement officials have been meeting with their EU counterparts recently, including an unannounced meeting in Washington between Treasury Department officials and the EU's commissioner for justice, freedom and security, Franco Frattini, people familiar with the contacts said. Mr. Frattini is also vice president of the EU's executive body, the European Commission.
>
> "We have been engaged in an ongoing dialogue at senior levels with our EU counterparts, including with Vice President Frattini," said Treasury Undersecretary Stuart Levey. "This dialogue has focused on the value of the [financial intelligence program] in fighting terrorism globally, including its value to counterterrorism efforts in Europe. We have also discussed in detail the rigorous safeguards in place to protect the privacy of all citizens not engaged in terrorism."[29]

The Debate over the Renewal of the Protect America Act

The Foreign Intelligence Surveillance Act (FISA) of 1978 stipulates that all searches for the purpose of collecting foreign intelligence within the territory of the United States require a warrant from a secret FISA court. Between 1979 and 2006, a total of 22,900 applications for warrants were made to the court and 22,895 of them were approved. Yet, the Bush

---

[26] Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls," *USA Today*, May 11, 2006, p. A1.

[27] Josh Meyer and Greg Miller, "Secret U.S. Program Tracks Global Bank Transfers," *LA Times*, June 23, 2006, http://www.commondreams.org/headlines06/0623-06.htm; Eric Lichtblau and James Risen, "Bank Data Sifted in Secret by U.S. to Block Terror," *New York Times*, June 23, 2006, p. A1.

[28] Randy Gainer, "Lawsuits Challenge the NSA's Warrantless Data Mining and Surveillance Program," *The Privacy and Data Security Law Journal*, Vol. 1 (September 2006), pp. 897-908.

[29] Glenn R. Simpson, "U.S., EU Seek to Ease Banking Privacy Concerns," *Wall Street Journal*, November 21, 2006.

administration claimed that FISA created too heavy a burden on the agencies charged with counterterrorism and that the government had a right to authorize warrantless searches under CALEA and the Authorization for Use of Military Force (AUMF) Against Terrorists resolution of 2001.

FISA was amended with passage of the Protect America Act (PAA) of 2007 to permit warrantless surveillance of foreign intelligence targets "reasonably believed" to be outside the United States. The PAA was due to expire on February 17, 2008, so the White House pressed Congress to renew it. The Senate passed a version of the bill that President Bush found acceptable, because it included immunity from lawsuits for telecommunications companies that had participated with government surveillance in the past. The House, in contrast, passed a version that did not include guarantees of immunity. In addition, the House insisted that all searches for counterterrorism had to be conducted under FISA warrants, in this case a change from the original terms of the Protect America Act. According to the President:

> … the House bill could reopen dangerous intelligence gaps by putting in place a cumbersome court approval process that would make it harder to collect intelligence on foreign terrorists. This is an approach that Congress explicitly rejected last August when bipartisan majorities in both houses passed the Protect America Act. And it is an approach the Senate rejected last month when it passed a new -- new legislation to extend and strengthen the Protect America Act by an overwhelming vote of 68 to 29.
>
> Second, the House bill fails to provide liability protection to companies believed to have assisted in protecting our nation after the 9/11 attacks. Instead, the House bill would make matters even worse by allowing litigation to continue for years. In fact, House leaders simply adopted the position that class action trial lawyers are taking in the multi-billion-dollar lawsuits they have filed. This litigation would undermine the private sector's willingness to cooperate with the intelligence community, cooperation that is absolutely essential to protecting our country from harm. This litigation would require the disclosure of state secrets that could lead to the public release of highly classified information that our enemies could use against us. And this litigation would be unfair, because any companies that assisted us after 9/11 were assured by our government that their cooperation was legal and necessary.[30]

The defenders of the President's position argue primarily on the basis of the need for speed in catching terrorists and the need for cooperation from private firms. Critics argue that speed is not compromised by the existing FISA laws and that private firms should not have carte blanche to ignore the laws of the land in their dealings with the federal government.

The Tradeoffs between Privacy and Security

---

[30] "President Bush Discusses FISA," White House Fact Sheet, Office of the Press Secretary, March 13m 2008, http://www.whitehouse.gov/news/releases/2008/03/20080313.html.

To summarize, in the controversies over data mining and warrantless search since September 11 the two contesting worldviews stress, on the one side, security, on the other, privacy. The question raised by all this is to what extent legal privacy protections necessarily impair national security.

The extreme view in favor of privacy is that legal protection of individual rights and liberties could be undermined in a blind pursuit of total security, especially if that involves ambitious electronic surveillance that leaves very little room for government transparency and individual privacy rights.

The extreme view in favor of security is that rights and liberties will not be available to citizens if terrorists triumph, so whatever is needed to combat terrrorism is justified. The extreme advocates of security argue that the government can be trusted not to abuse the power that comes with the collection of highly detailed counterterrorist information.

Most of us are somewhere between these two extremes. The balance in the Bush administration since 2001 has been weighted heavily toward the security extreme (but it should be noted that individuals in the Department of Defense, the FBI, and the Department of Justice, for example, have weighed in from time to time in favor of privacy guarantees at the expense of some counterterrorism programs). One helpful approach suggested by technologists is to modify the technologies used for data mining and electronic surveillance so that they incorporate methods for protecting individual privacy.

It is unlikely that a permanent bargain will be struck between the political forces involved in these controversies. Nevertheless, there could be agreement on some of the goals for counterterrorist programs so that security could be enhanced in an incremental fashion without unduly threatening the rights of citizens. For example, the Total Information Awareness program, for all its faults, included some excellent ideas for creating rapid translation technologies and for building in privacy guarantees into data mining technologies. These programs were cut when the TIA was dismantled. Similarly, it is possible for different government agencies to share data electronically in an interoperable manner that is actually needed for counterterrorist operations but does not violate the privacy rights of U.S. citizens.

In conclusion, this paper shows how the efforts of the federal government after September 11, 2001, to implement counterterrorist data mining programs and to update electronic surveillance methods and techniques began a national debate about the tradeoffs between privacy and security. Such a debate would have occurred even in the absence of a precipitating event like September 11. The debate is our opportunity to address some of the problems that can occur when enormous amounts of information can be created, stored, transmitted, and processed easily and cheaply, including information about individual human beings. We need to rethink the rules governing the ownership and control over information and informational flows in light of the current debate.