Is the U.S. Government's Mining of Commercial Data Contributing to an Erosion of Trust in Government?

Carter Manny, Associate Professor of Business Law, University of Southern Maine

Abstract

Following the terrorist attacks of September 11, 2001, the executive branch of the U.S. Government turned to data mining practices for the avowed purpose of protecting public security. Relying on a combination of legislative authorization and cooperation by the private sector, federal institutions have obtained access to information in commercial databases collected largely from routine business transactions by ordinary people posing no particular threat to public order. Much of the data mining has occurred without safeguards like prior court authorization and limitations in the Privacy Act of 1974. In the absence of these safeguards designed to protect individual liberty, data mining appears to have contributed to an erosion of public trust in government. Government surveillance following September 11, like responses to other crises in U.S. history, is motivated by fear. While many members of Congress have supported greater restraints on data mining, their efforts tend to be overridden by fear-based justifications for surveillance.

I. Introduction

Several days after the September 11, 2001, attack on the U.S., Hank Asher, founder of a Florida-based commercial data broker company known as Seisint, ran a new data mining system through the company's 20-billion-record database. He came up with a list of names of 120,000 people the system had identified as having a "high terrorist factor." Those names were then reduced to a "1 percent list" of 1,200 people deemed to be the biggest threats. The names of five of the nineteen September 11 hijackers were on the list. When Asher demonstrated Seisint's system to officials from the FBI and other law enforcement agencies, they were greatly impressed.[1]

While this after-the-attack search of a commercial database raised some exciting possibilities in the minds of those interested in protecting public security, it also raised questions about the potential threat to civil liberties posed by government access to the billions of items of personal information held in commercial databases. Although some of the information, like names, street addresses, phone numbers, voter registration records, court records, marital records, and real estate records have been publicly available on paper for decades, recent

[1] *See* Jeffrey W. Seifert, *Data Mining and Homeland Security, An Overview, available at* http://www.fas.org/sgp/crs/intel/RL31798.pdf (last visited July 19, 2007); ROBERT O'HARROW JR., NO PLACE TO HIDE 98-102 (2005).

advances in computer technology have made it economically feasible for data brokers to compile electronic dossiers on most of the people in the U.S. Moreover, through information collected through a host of consumer transactions, it is possible to combine a wide variety of non-public data with public records to provide a detailed account of someone's life. Non-public personal information can include e-mail addresses, financial information, travel history, employment history, subscriptions to publications and membership in organizations. The data can be linked with information about other people in the household. Although the credit reporting industry, dominated by Equifax, Experion and Trans Union, has been subject to privacy and other restrictions under the Fair Credit Reporting Act since 1970, the data broker industry, currently dominated by ChoicePoint, Acxiom and LexisNexis, is subject to far less regulation.

These developments raise some important questions about government's response to the threat of terrorism. What about the 1,195 people on Hank Asher's "1 percent list," branded as possessing a "high terrorist factor," who were not part of the September 11 attacks? Were they unfairly identified? Is a data mining system based on some of the known characteristics of the hijackers, including ethnicity, pilot training, age and gender, along with other factors including social security number anomalies, credit history and connection with "dirty" addresses and phone numbers, likely to be effective at identifying potential future terrorists? Do security concerns justify this type of data mining? Are civil liberties being threatened? Do the answers to these questions indicate that data mining is contributing to an erosion of trust in government?

Ii. Privacy, Ethics and Society

Privacy is a complex concept with many different definitions. It is characterized as a human right in the United Nations Universal Declaration of Human Rights and has been

enshrined as a fundamental right in European law.[2] It is connected with liberty and personal autonomy. Alan Westin, in his influential 1967 book, Privacy and Freedom, explains how privacy arises out of nature.[3] Privacy has also been analyzed from a harm-based approach.[4] For example, publication of an embarrassing photograph can injure one's sense of dignity, even when no economic or psychological harm can be demonstrated. Lack of privacy also can affect behavior. People understandably will feel more inhibited when they know they are being observed. While this can be beneficial in promoting order in a crowded public place, the uninvited scrutiny of others can put a damper on creative activities like art, musical composition, and scientific inquiry. Lack of privacy can reduce security. The availability of someone's street address can increase the likelihood that the person will be targeted by a stalker, kidnapper or thief.

Privacy can also be viewed from the perspective of moral principles of justice. For example, restrictions on the dissemination of certain types of personal information, like religion or economic background, can help promote equality by reducing the likelihood that a prospective employer will use these criteria to reject the person's employment application. In other words, privacy can help promote equal treatment. Privacy can also help promote fairness in economic exchanges. For example, if a potential buyer of a house knows that the seller needs money quickly to pay for a kidney transplant for a sick child, the buyer might have an unfair advantage in negotiating a low purchase price. Similarly, if a seller knows that a buyer is wealthy, the seller may be less likely to be flexible in agreeing to a reduction of the asking price.

---

[2] *See* United Nations Universal Declaration of Human Rights (1948), art. 12, *reprinted in* THE PRIVACY LAW SOURCEBOOK 2003, 318, (Marc Rotenberg, ed.); Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (Nov. 4, 1950), art. 8, *reprinted in* THE PRIVACY LAW SOURCEBOOK 2003, 325, (Marc Rotenberg, ed.)

[3] *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 8-11 (1967)(documenting the need that animals have for seclusion.)

[4] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

Societal changes also profoundly affect notions of privacy. Prior to the twentieth century, much of the information about an American's private life could be discovered through physical objects, including documents, located in one's home. With industrialization, urbanization, electronic communications and finally computer technology, most of those details now are located in records held by businesses and other large institutions. Financial institutions, communications companies, credit reporting bureaus, commercial data brokers, government agencies, health care providers and educational institutions now possess massive amounts of electronic information about the lives of most Americans. The shift of personal information from the home to large, third party custodians has made it easier for government to get access to personal data.

Iii. Legal Devices For Government Access To Information

A. Search Warrants

One of the grievances that led to the war of independence was the British government's use of general warrants authorizing indiscriminate searches of the American colonists' homes. In order to prevent such abuses, the Founding Fathers drafted the Fourth Amendment to guarantee that searches be based on particularized suspicion satisfying the standard of "probably cause" rather than on general authorization.[5] The Fourth Amendment's prohibition against "unreasonable searches and seizures," has generally been interpreted by the U.S. Supreme Court to require the government official to obtain a search warrant from a judge prior to the search. In a criminal investigation, the police must present the judge with enough information to establish "probable cause." For civil investigations by administrative agencies, the information presented to the judge is subject to a much lower standard. The Supreme Court, however, has interpreted

[5] The Fourth Amendment provides, "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

the Fourth Amendment to allow criminal and administrative searches without a search warrant under certain exceptions. For example, some types of warrantless criminal searches are permitted when evidence is in plain view[6] or when motorists are stopped at a properly administered sobriety checkpoint.[7] Warrantless administrative searches have been permitted for certain "closely regulated industries" like pharmacies, gun dealers and businesses which sell alcoholic beverages, as long as the inspection is done pursuant to a properly administered inspection program.[8] Today, for reasons explained below in the material on subpoenas, search warrants tend to be used primarily to search for physical evidence in homes and businesses.[9]

B. Electronic Surveillance

With the development of the telephone and radio, investigative methods expanded to include the ability to intercept phone calls through wiretaps and other conversations using wireless transmitters, commonly called "bugs." In 1928 the Supreme Court held that a wiretap did not require a search warrant because there was no physical trespass.[10] Almost 40 years later, in a pair of Fourth Amendment cases decided in 1967, the Supreme Court reversed itself and eliminated the physical trespass analysis with respect to electronic eavesdropping. One decision struck down a state law authorizing court approved police electronic eavesdropping on the ground that the law did not require the police officer to establish probable cause as required by the Fourth Amendment in order to get court approval.[11] In the other, the Supreme Court invalidated police use without a court order of an electronic listening device on the exterior of a pubic telephone booth.[12] The following year Congress passed comprehensive crime control

---

[6] *See, e.g.*, Washington v. Chrisman, 455 U.S. 1 (1982).
[7] See, e.g., Michigan v. Sitz, 496 U.S. 444 (1990).
[8] See, e.g., New York v. Berger, 482 U.S. 691 (1987).
[9] *See* Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 810 (2005).
[10] *See* Olmstead v. United States, 277 U.S. 438 (1928).
[11] *See* Berger v. New York, 388 U.S. 41 (1967).
[12] *See* Katz v. United States, 389 U.S. 347 (1967).

legislation with provisions regarding warrants for electronic surveillance.[13] Despite Supreme Court decisions and statutory responses, Fourth Amendment requirements with respect to electronic surveillance remain open to some interpretation.[14]

One controversial area that remains unsettled is whether electronic surveillance in the U.S. without prior court authorization is permissible with respect to national security. Because of abusive electronic surveillance of domestic groups during the Vietnam War uncovered by a committee chaired by Senator Frank Church, Congress passed the Foreign Intelligence Surveillance Act (FISA) in 1978.[15] Prior to engaging in domestic electronic surveillance when investigating foreign intelligence operations, the federal government is supposed to obtain authorization from a special court created by FISA. The proceedings of the FISA court are secret. Despite the existence of the FISA statute and court, the Bush administration secretly authorized the National Security Agency (NSA) to engage in surveillance of electronic communications in the U.S. without prior court approval. After the NSA surveillance program was reported by the press in late 2005, lawsuits were filed challenging both the program and the participation of phone companies in providing information.[16] In January 2007 the Bush Administration announced that it would obtain authorization from the FISA court for electronic eavesdropping under the one NSA program whose existence had become public knowledge,[17]

---

[13] *See generally* Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 82 Stat. 211, 18 U.S.C. §§2510-20.

[14] *See, e.g.,* Curtis Bradley, et al., *On NSA Spying: A Letter to Congress,* N.Y. REVIEW OF BOOKS, Feb. 9, 2006, *available at* http://www.nybooks.com/articles/18650 (last visited Aug. 14, 2007)(letter by legal scholars noting that the U.S. Supreme Court in United States v. United States District Court, 407 U.S. 297 (1972), "left open the question of the Fourth Amendment validity of warrantless wiretaps for foreign intelligence purposes.")

[15] *See* Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-62 (2000).

[16] In ACLU v. NSA, the U.S. Court of Appeals for the Sixth Circuit ruled in July, 2007, that the journalist and attorney plaintiffs lacked standing to challenge the NSA's warrantless interception of communications because they could not show that they were actually subject to surveillance. See *Sixth Circuit Rejects NSA Spying Challenge; Finds Journalists, Attorneys Lack Standing*, 6 PRIVACY & SECURITY L. REP. (BNA) 1081 (2007). Another set of cases consolidated in the U.S. District Court for the Northern District of California involve lawsuits by the U.S. Justice Department to block over 20 states from investigating cooperation by telecommunication companies with alleged NSA surveillance activities. *See, e.g., Multidistrict Panel Consolidates More Suits In Web of Claims Related to NSA Surveillance*, 6 PRIVACY & SECURITY L. REP. (BNA) 324 (2007).

[17] *See, e.g.*, Eric Lichtblau and David Johnston, *Court to Oversee U.S. Wiretapping in Terror Cases*, N.Y. TIMES, Jan. 18, 2007 at A1.

but there has been speculation that other secret electronic surveillance programs were also being run.[18] The following August, however, Congress passed temporary legislation allowing surveillance of telephone and internet communications without prior court authorization.[19]

C. Subpoenas

Prior court approval is not the only legal process for obtaining personal information in an investigation. In many instances, the production of documentary evidence is compelled by means of a subpoena. A subpoena can be issued by a court or other governmental institution ordering the recipient either to testify at a hearing, or to produce evidence. Unlike a search warrant which cannot be contested prior to the search, the recipient of a subpoena has the legal right to contest its validity in court before complying with the order to testify or produce evidence. In criminal cases, subpoenas are often used in connection with a grand jury investigation. Although a subpoena is a court document, as a practical matter it is filled out by the prosecutor who has some discretion to determine when it should be used. After the subpoena has been delivered, the recipient decides whether to comply with the subpoena or challenge it in court. A successful challenge will cause a court to modify or quash the subpoena. Someone who refuses to comply with a valid subpoena can be punished for contempt of court.[20]

Another type of subpoena, an administrative subpoena, is available in many types of investigations by federal agencies. There are over 300 statutory provisions through which Congress has authorized federal administrative agencies to issue subpoenas.[21] As with grand jury subpoenas, administrative subpoenas can be challenged in court before the evidence is

---

[18] *See* comments by Peter Swire on the Public Broadcasting System television program *Frontline* titled "Spying on the Home Front" broadcast on May 15, 2007.
[19] *See* The Protect America Act of 2007, Pub. L. 110-55 (2007) (amending the Foreign Intelligence Surveillance Act for a period of 120 days beginning on August 5, 2007.)
[20] *See generally* FED. R. CRIM. P. 17.
[21] *See, e.g.*, Testimony of Rachel Brand, Principal Deputy Assistant Attorney General, U.S. Dept. of Justice, before the U.S. Senate Judiciary Committee, June 24, 2004, available at http://usdoj.gov/ olp/pdf/dojaag_brand_062204.pdf (last visited July 27, 2007).

produced. In order to have a court quash or modify a subpoena, the challenger must prove one or more of the following: (1) that compliance would cause an undue burden, (2) that the evidence is not relevant to an authorized investigation, or (3) that the evidence is protected by a legal privilege, for example the attorney-client privilege.[22]

Today, many administrative subpoenas are not a "first party" subpoena in which the target of the investigation is the recipient, but a "third party" subpoena in which the recipient is the custodian of information about a target. For example, a bank, phone company or Internet service provider might be the recipient of a third party subpoena seeking information about a customer. It is unlikely that anyone will go to court to quash or modify a third party subpoena. The target of the investigation will probably not know about the subpoena unless informed by the third party business. Even if there is some sort of notice, a challenge in court would be too late if the information has already been provided to the investigator. The third party business probably has little incentive to challenge the subpoena in court, unless the volume of information requested would be expensive to produce, thus meeting the "undue burden" legal standard. For economic reasons, it is unlikely that the third party would bear the expense of challenging a subpoena on the grounds that the information about a customer is not relevant to an investigation.

Even if a target customer learns about a subpoena, he will have difficulty challenging it on Constitutional grounds. The U.S. Constitution has been interpreted to provide the customer with little protection against third party subpoenas. The Supreme Court has held that there is no Fourth Amendment search protection in information which someone has provided to a third party[23] and that the Fifth Amendment privilege against self incrimination does not apply to

[22] *See* Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 806 (2005).
[23] *See* U.S. v. Miller, 425 U.S. 435 (1976).

business records.[24] The target customer could try to challenge the subpoena on the grounds that the evidence sought is irrelevant to an investigation, although this argument is unlikely to succeed in many types of investigations. A challenge based upon the contention that the information is protected by a legal privilege is even less likely to succeed, because there are no legal privileges in most commercial relationships.

The Constitution, and general provisions regarding subpoena power, provide few safeguards against government use of subpoenas to obtain documentary personal information from third party businesses like banks, phone companies and Internet service providers. Accordingly, investigators often use subpoenas to compel production of personal information in business databases. Of course, there would be no reason to use a subpoena if the business volunteers to provide information.[25]

D. National Security Letters

A National Security Letter (NSL) is a more powerful version of an administrative subpoena. There are several statutory provisions which authorize the FBI to issue an NSL to order production of documentary evidence held by communications providers, financial institutions, credit reporting bureaus and other organizations. Although most of the provisions existed prior to 2001, governmental authority to issue National Security Letters was greatly strengthened by the Patriot Act passed a few weeks after September 11. Authority to issue NSLs was expanded to include FBI field offices as well as FBI headquarters in Washington, D.C.

---

[24] *See, e.g.,* Hale v. Henkel, 201 U.S. 43 (1906).

[25] Newspaper articles published in June 2006 revealed that since shortly after September 11, 2001, the U.S. Treasury Department had been mining electronic financial data transmitted over a communications system operated by the Society for Worldwide Interbank Financial Transfers (SWIFT.) The newspaper articles contain information that in the immediate aftermath of September 11, SWIFT initially was very cooperative in providing data when it was approached by the U.S. Treasury, but after a period of months SWIFT had second thoughts, which may have caused the Treasury to use subpoenas to compel production of the information. Moreover, SWIFT's discomfort with government access to the data caused it to negotiate with the Treasury to add safeguards for protection of the data. *See* Eric Lichtblau and James Risen, *Bank Data Sifted in Secret by U.S. to Block Terror*, N.Y. TIMES, June 23, 2006 at A1; Josh Meyer and Greg Miller, *U.S. Secretly Tracks Global Bank Data,* LOS ANGELES TIMES, June 23, 2006 at A1.

Investigations to guard against international terrorism were added to counterintelligence as permissible purposes. Prior to the Patriot Act, the FBI could only issue an NSL when it had specific facts that the target of the investigation was a foreign power or its agent. The Patriot Act replaced the "specific facts" and "foreign power" limitations with a much lower standard allowing the National Security Letter to order production of evidence that is relevant to the investigation. The lowering of the standard to mere "relevance" arguably gives the FBI Congressional authority to order a business to make an entire commercial database available to government investigators, as long as there is some reason to believe it might contain information connected in some way with terrorist activity. Moreover, the National Security Letter statutes contain nondisclosure, or "gag," provisions, prohibiting the recipient of the NSL from disclosing its existence to anyone at any time. The gag provisions made it very difficult to challenge the validity of a National Security Letter in Court.[26]

However, two challenges to NSLs were brought by the American Civil Liberties Union in federal trial courts in New York and Connecticut. The court in the New York case held that National Security Letters violated the Fourth Amendment because they compelled searches which were effectively immune from any judicial process, and First Amendment protection for freedom of speech because the gag provision was so absolute that it lacked a process for it to be lifted by the FBI or a court.[27] The court in the Connecticut case also ruled that NSLs were invalid, but limited its reasoning to the same First Amendment rationale used by the federal court in New York.[28]

---

[26] *See* Charles Doyle, *National Security Letters in Foreign Intelligence Investigations: A Glimpse of the Legal Background and Recent Amendments*, *available at* http://www.fas.org/ sgp/crs/intel/ RS22406.pdf (last visited July 25, 2007).
[27] *See* Doe v. Ashcroft, 334 F.Supp.2d 471 (S.D.N.Y. 2004).
[28] *See* Doe v. Gonzales, 386 F.Supp.2d 66 (D. Conn. 2005).

Congress, however, addressed the Constitutional defects identified in the two cases when it reauthorized provisions in the Patriot Act in 2006.[29] The 2006 reauthorization added provisions permitting judicial review of both the demand for production of information, and the accompanying gag provision. It added a mechanism for lifting the gag provision, and made clear that the recipient of a National Security Letter could consult a lawyer. It also required the Inspector General of the Justice Department to conduct audits of the NSL program and report the results to Congress. The first of those reports, issued in March 2007, found over 1000 FBI abuses of National Security Letters during 2003-05.[30] An internal FBI audit completed in June 2007 found an additional 1000 instances of abuse.[31]

Iv. Data Mining

Government has the ability to obtain access to commercial data, either through a compulsive device like a subpoena, or by purchasing access from members of the commercial data broker industry.[32] Once the government has access, there are differend methods of analysis, the two most prominent being link analysis and pattern analysis.[33] Link analysis looks for connections between different pieces of information. An example of link analysis in an antiterrorism investigation would be to use telephone company data to determine the phone numbers called by a suspect, and the phone numbers of the people who have called him. Link analysis is nothing new. It is an investigative technique that has been widely used in criminal investigations throughout history and can include links established by other methods of

---

[29] *See* USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. 109-177, §§115-19 (2006).
[30] *See* U.S. Department of Justice, Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters*, March 2007, *available a*t http://www.usdoj.gov/ oig/special/s0703b/final.pdf (last visited June 26, 2007).
[31] *See* John Solomon, *FBI Finds It Frequently Overstepped in Collecting Data*, WASH. POST, June 14, 2007 at A1.
[32] *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595 (2004).
[33] *See* Jim Harper, Testimony at U.S. Senate Judiciary Committee Hearing Entitled "Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs," *available at* http://judiciary. senate.gov/ testimony.cfm?id=2438&wit_id=5949 (last visited July 19, 2007).

communication, including postal mail, and even links established through face to face conversations. Computer technology, however, greatly expands the government's ability to discover connections between people. Link analysis, of course, has some limitations. Even though a suspected terrorist is speaking with someone by telephone, the link alone is insufficient to indicate that something sinister is taking place. The other party to the conversation might have nothing to do with planning an attack, like a landlord interested in collecting payment of rent, or a restaurant receiving an order to deliver a pizza. However, the identification of the links can cast suspicion on innocent parties.

Pattern analysis uses a different approach. Historical information is used to determine that certain types of behavior might lead to a particular event. If there is enough repetition of the behavior followed by the event, then detection of the behavior can be used to predict the event. The authors of a recent report have labeled this as "predictive data mining."[34] In the commercial context, predictive data mining can be a valuable technique. For example, data mining can be helpful in detecting possible fraudulent use of a credit card. The history of a customer's use of a card, combined with a bank's knowledge of the types of unauthorized charges made by thieves, can enable the creation of a system to alert the issuing bank when a card is used in a particular way. For example, the sudden appearance of charges of large purchases in Hong Kong, when the card holder resides in Ohio, can be a good indication that fraud is occurring. In this sort of commercial context, the large quantity of historical data about credit card use makes it possible to establish fairly reliable patterns, which helps the bank to be more vigilant. And in this example, fraud detection data mining is mutually beneficial to the customer and the business.

---

[34] *See* Jeff Jonas and Jim Harper, Effective Counterterroism and the Limited Role of Predictive Data Mining, *available at* http://www.cato.org/pub_display.php?pub_id=6784 (last visited July 27, 2007).

But how useful is data mining likely to be in predicting terrorist attacks? The same authors who coined the term "predictive data mining" conclude that pattern analysis is unlikely to be very useful. They provide three reasons. First, the small number of terrorist attacks do not provide enough information to establish a reliable historical pattern. Second, even if certain facts are connected to a potential threat, a data mining system which uses those facts can still lead to a large number of "false positive" instances in which the wrong people are identified. For example, when data mining expert Hank Asher created a data mining program in the days following September 11, the public then knew many of the hijackers' common characteristics. Because of this knowledge, Asher was able to create a data mining system that limited the search by age, gender, pilot training and ethnicity. Even using that kind of after-the-fact information, when his system came up with the narrowest list of people with a "high terrorist factor," it contained 1,200 names, only five of whom were hijackers. Over 99% of the people on the list were false positives. Third, predictive data mining could be based on "red teaming," in which the designers of the system would try to think like a terrorist and come up with a hypothetical plan for an attack. A data mining system could then be based on the probable activities than would be engaged in before carrying out the attack. But a data mining system based on "red teaming" also runs the risk of generating such a large number of false positives as to be ineffective. For example, one could assume that terrorists will carefully observe a target by taking photographs as part of the process of planning an attack. However, photography of buildings, bridges and airports is also consistent with the innocent behavior of tourists, amateur photographers and people interested in architecture and engineering.[35]

Despite these limitations, after September 11 the executive branch of the federal government has considered various forms of data mining as part of its efforts to combat

[35] *Id.*

terrorism. Some projects have been conducted in secret and caused quite a bit of controversy when exposed. Others were created in the open, even though some of their methods were not revealed. It is likely that some forms of data mining remain secret. The most controversial project was the Total Information Awareness (TIA) program run by the Defense Department and headed by Admiral John Poindexter who had been involved in the Iran/Contra scandal in the 1980s.[36] TIA, also known at Terrorism Information Awareness, considered the possibility of mining a large number of government and commercial databases to look for signs of possible terrorist activity. Because of public opposition largely fueled by privacy concerns, Congress canceled transparent funding for the project in 2003. However, Congress allowed unspecified components of the project to continue as part of the Defense Department's classified budget.[37]

Another controversial project begun in the aftermath of September 11, the Multi-State Anti-Terrorism Information Exchange, also known as MATRIX, involved a database containing roughly 4 billion items of mostly publicly available information from government and private sources. It was initially developed by Seisint and originally included the "high terrorist factor" component mentioned earlier. MATRIX was operated as a pilot project which ended in April 2005. Although as many as 16 states were reported to have either participated in, or seriously considered participating in, MATRIX, only 4 states were actively involved when the project ended. States were reluctant to participate in MATRIX for a variety of reasons, including privacy concerns.[38]

Some data mining programs began covertly and were later exposed by the media. An example is the National Security Agency's program of surveillance of domestic phone calls

---

[36] *See* Jeffrey W. Seifert, *Data Mining and Homeland Security, An Overview* 5-8, *available at* http://www.fas.org/sgp/crs/intel/RL31798.pdf (last visited July 19, 2007).
[37] *Id.* at 8.
[38] *Id.* at 12-16.

which was exposed in December 2005. Controversy over the NSA project generated Congressional hearings and several lawsuits. Some of the lawsuits are directed at the NSA and seek to restrict or terminate the surveillance on Constitutional grounds. Others are by the federal government seeking to block state regulators from investigating the extent to which communications companies have provided customer information to the NSA.[39] Another example of a covert program exposed by the media is the Treasury Department's mining of international and domestic electronic financial data transmitted over a communications system operated by the European-based Society for Worldwide Interbank Financial Transfers, known by the acronym SWIFT. In Europe, officials of national data protection agencies, and the European Union's top privacy official, have concluded that SWIFT's actions in providing personal information to the U.S. Treasury were in violation of European data protection law. However, no enforcement action was taken, and an agreement between European and American officials permitting the transfers with some privacy safeguards was reached during the summer of 2007.[40]

Data mining has been a significant part of programs aimed at airline and border security. Proposed systems for computerized "prescreening" of airline passengers (before they experience the physical screening at the airport) have included use of commercial databases, as well as government "selectee" and "no fly" lists containing names of people who should be subjected to secondary physical screening, or who should not be allowed to board a flight unless cleared by law enforcement agents at the airport. One proposal, known as CAPPSII (Computerized Passenger Prescreening System II,) was canceled by the Department of Homeland Security (DHS) and replaced by another proposed system called Secure Flight. Both proposals were

[39] *Id.* at 18-20.
[40] *See, e.g.,* James Risen, *U.S. Reaches Tentative Deal With Europe On Bank Data,* N.Y. TIMES, June 29, 2007.

criticized because of privacy concerns. Implementation of Secure Flight was suspended by DHS in 2006 to allow officials to address privacy and other issues.[41]

After September 11, Congress passed legislation directing airlines to provide the Department of Homeland Security with access to information in airline reservation databases, known as passenger name record (PNR) data, for passengers arriving on international flights. The requirement has been a source of friction between European officials and the U.S. because European law requires a proper legal basis for all transfers of personal information from European Union countries to destinations whose privacy laws are not compatible with European standards. Because United States laws fail to meet those standards, European Union officials and officials from the Department of Homeland have negotiated several agreements that permit transfers with privacy safeguards. The agreements have been controversial in Europe. The first agreement was nullified by Europe's highest court in 2006. A second agreement was reached in the autumn of 2006, and was replaced by third agreement during the summer of 2007.[42] In addition to airline passenger reservation data, another system called the Automated Targeting System (ATS) uses data mining to assess risks associated with all people and cargo entering the United States.[43]

How can there be so much controversy over the privacy implications of these programs, especially with respect to government access to personal data in commercial databases, when Congress imposed duties on federal agencies to protect the privacy of individuals by passing the Privacy Act in 1974? Doesn't it provide sufficient safeguards? The simple answer is that

---

[41] *See generally* United States Government Accountability Office, *Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues Remain*, May 2007, *available at* http://www.gao.gov/new.items/d07346.pdf (last visited June 4, 2007).

[42] *See* Agreement Between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS), *available at* http://register.consilium.europa.eu/ pdf/en/07/st11/ st11595. en07. pdf (last visited Aug. 13, 2007.)

[43] *See* United States Government Accountability Office, *Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues Remain*, May 2007, 7, available at http://www.gao.gov/new.items/d07346.pdf (last visited June 4, 2007).

Congress did not anticipate the data mining techniques that currently allow federal agencies to use information from private sector databases. The Privacy Act is from a different era of computer technology, and was written to apply only to databases created either by the federal government, or on its behalf by private contractors.[44] Furthermore, Congress exempted data used for law enforcement or intelligence purposes from Privacy Act protection even when it comes from a government database.[45]

V. Privacy Principles And Trust In Government

What effect do these data mining activities have on public trust in government? A good starting point in this analysis is to look to general privacy principles with respect to the handling of personal information. Many of those principles were developed in the 1970s in the U.S. and Europe, and received international approval through guidelines adopted by the Organization of Economic Cooperation and Development. They were the foundation for the Privacy Act in the U.S. and comprehensive data protection legislation in Europe and elsewhere. The core principles recognized in the U.S. and elsewhere provide that individuals should be able to determine the existence of databases containing personal information, that an individual should be able to find out what information about him or her is in the database, that the individual should have the right to correct inaccurate information, that there should be no secondary use of the data without the individual's consent, and that the database should contain accurate information and be secure.[46] Additional principles recognized in Europe are that data should be collected fairly and for legitimate purposes, that the individual should be informed at the time of collection of the

---

[44] *See* 5 U.S.C. § 552a(m) (2000).
[45] *See* Jack Dempsey and Lara Flint, *Privacy's Gap: The Largely Non-Existent Legal Framework for Government Mining of Commercial Data*, *available at* http://www.cdt.org/ security/ usapatriot/ 030528cdt.pdf (last visited Aug. 15, 2007).
[46] *See* U.S. Dept. of Health, Education and Welfare, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973); OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), *available at* http://www.oecd.org/dsti/sti/it/secure/prod/PRIV-EN.HTM (last visited July 24, 2007.)

purposes for which the data will be used, and that data collection should be "proportional," i.e. not excessive.[47] Taken together, these principles probably are a good indication of public concerns regarding the use of personal data and how violations of those principles can diminish trust.

Recent highly publicized events concerning government mining of personal data from commercial databases indicate how departures from these principles may be eroding public trust. The National Security Agency's warrantless surveillance program is a good example. Although some of the details of the program are still secret, it appears that the NSA has had access to information about U.S. telephone calls, and has been mining that data to detect evidence of planning of terrorist attacks. The program is contrary to the no-secondary-use-without-consent principle that personal data collected for one purpose (telephone billing records) should not be used for another purpose (government surveillance) without the individuals' consent. It also is contrary to the principle that the existence of a database should not be secret.

Another example, reported in a May 2007 television program titled "Spying on the Home Front," is the FBI's collection of information about hundreds of thousands of tourists in Las Vegas in late December 2003 in response to intelligence that a terrorist attack might be made in the city. Although the details of the data collection were not specified, probably because the information was collected using National Security Letters which prohibit recipients from disclosing the existence of the FBI demands, it appears that hotels, car rental companies and other businesses catering to visitors turned over all their information about customers during late December. Once again, this government activity violates the principles of no secondary use without consent, and no secret databases.

---

[47] *See* Council Directive 95/46, 1995 O.J. (L281), often referred to at the Data Protection Directive.

Privacy experts are alarmed by these and other examples. Law professor and former Clinton Administration privacy advisor Peter Swire has compared these instances of government acquisitions of massive amounts of data to the indiscriminate British searches of American colonists' homes under general warrants during the 1700s. Today, everyone is a suspect, in apparent contradiction of the Fourth Amendment principle that searches should be based on particularized suspicion.[48] Other privacy experts have expressed similar concerns during U.S. Senate Judiciary Committee hearings. These concerns have been raised across the political spectrum, reflecting that libertarian values can cross party lines.[49]

How is the average citizen reacting? An annual privacy trust study of the U.S. government surveyed 7,000 U.S. residents in 2007 to determine their level of trust connected with federal agencies' use of personal information.[50] Overall, trust in all federal government agencies declined from a rating of 52% in 2005 to 45% in 2007. The least trusted agencies in the 2007 survey, with the change from 2004 survey in parentheses, are:

National Security Agency:	19%	(-10%)
Central Intelligence Agency:	21%	(-06%)
Department of Homeland Security:	22%	(-05%)
Office of the Attorney General:	23%	(+01%)
U.S. Justice Department:	29%	(+05%)

Although the survey did not explore whether government mining of commercial data plays a role in determining levels of public trust, there appears to be a correlation between those agencies

[48] *See* comments by Peter Swire on the Public Broadcasting System television program *Frontline* titled "Spying on the Home Front" broadcast on May 15, 2007.

[49] Compare testimony of former Republican Congressman Robert Barr and statement of Democratic Senator Patrick Leahy at a U.S. Senate Judiciary Committee hearing titled "Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs" held on January 10, 2007, *available at* http://judiciary.senate.gov/hearing.cfm?id=2438 (last visited July 27, 2007).

[50] *See* Ponemon Institute, 2007 Privacy Trust Study of the United States Government, available at http://www.epic.org/privacy/pdf/2007ponemon.pdf (visited July 24, 2007). In 2007, the two most trusted federal agencies were the U.S. Postal Service at 83% and the Federal Trade Commission at 80%.

which have been publicly identified as engaging in data mining (the National Security Agency, the Department of Homeland Security, and the FBI which is part of the Justice Department) and low scores in the trust survey.

Vi. Fear, Civil Liberties And The Future

Of course, fear has played a large part in the government's response to the attacks on September 11. From personal experiences we all know that fear is a powerful motivator. Why? Security expert Bruce Schneier points to the human brain. In an evolutionary sense, one of the oldest centers of the brain, known as the amygdala, is responsible for processing emotions that come from sensory inputs, like anger, avoidance and fear. It is the area that controls the "fight or flight" response that instantly tells someone crossing the street to jump out of the path of an oncoming bus. The amygdala processes information very quickly and enables humans to survive when faced with sudden danger. A different part of the brain, the neocortex, whose evolutionary development is comparatively recent, is intelligent and analytic. It processes information much more slowly than the amygdala. It is the neocortex than enables humans to make a rational assessment of danger. Our brains have separate systems for responding to danger: the high speed, reactive, amygdala, and the much slower, rational, neocortex.[51]

Has human neurology been a factor in government responses to crises? Has fear led to an erosion of civil liberties? Consider some examples from U.S. history. In the 1790s the Federalist Congress enacted the Alien and Sedition Acts at a time when there was fear of revolutionary France's attacks on American ships, and concern that immigrants were supporting domestic political dissent that might destroy the U.S. government. Newspaper editors who were critical of the Federalists and supportive of then Vice President Thomas Jefferson were

[51] *See* Bruce Schneier, *Why the Human Brain Is a Poor Judge of Risk*, WIRED NEWS, March 22, 2007, available at http://www.schneier.com/essay-162.html (last visited July 27, 2007).

imprisoned for violating the Sedition Act, which today would almost certainly have been struck down as violating the First Amendment's protection of freedom of speech.[52] During the Civil War, the Lincoln Administration suspended habeas corpus, allowing the imprisonment without judicial process of people considered to be a threat to the Union. Although the suspension was probably justified in Maryland during the first few months of the war, when southern sympathizers had attacked federal troops on their way to defend Washington, burned railroad bridges and cut telegraph lines, thus threatening to isolate the nation's capital, the suspension was probably misused in other places later in the war.[53] During World War I, Congress enacted the Espionage Act and the Sedition Act, which were used to convict war critics for comments that today would almost certainly be protected by the First Amendment.[54] A series of bombings in 1919 led to mass arrests of innocent immigrants and U.S. citizens during the Palmer Raids in early 1920, orchestrated by U.S. Attorney General A. Mitchell Palmer.[55] In February 1942, during the early stage of U.S. involvement in World War II, President Franklin Roosevelt issued an executive order directing the internment of people with Japanese ancestry living in western states, most of whom were U.S. citizens.[56] In the late 1940s and early 1950s, a period often linked with the excesses of Senator Joseph McCarthy, Congress conducted heavy-handed investigations of people suspected of having ties to communism.[57] During the 1960s and 1970s,

---

[52] *See* SEAN WILENTZ, THE RISE OF AMERICAN DEMOCRACY, 75-83 (2005).
[53] *See* JAMES F. SIMON, LINCOLN AND CHIEF JUSTICE TANEY, 181-98, 236-40 (2006). Article I, Section 9, of the U.S. Constitution provides that the writ of habeas corpus shall not be suspended "unless when in Cases of Rebellion or Invasion the public safety may require it." The Constitution, however, does not specify whether the Congress or the president has authority to order the suspension.
[54] *See* DAVID M. KENNEDY, OVER HERE, THE FIRST WORLD WAR AND AMERICAN SOCIETY 75-88 (1980)
[55] *See* MURRAY B. LEVIN, POLITICAL HYSTERIA IN AMERICA: THE DEMOCRATIC CAPACITY OF REPRESSION, 31-75 (1971).
[56] *See* Geoffrey R. Stone, *Civil Liberties v. National Security in the Law's Open Areas*, 86 BOSTON U. L. REV. 1319-24 (2006).
[57] *See generally* DAVID CAUTE, THE GREAT FEAR: THE ANTI-COMMUNIST PURGE UNDER TRUMAN AND EISENHOWER (1978).

the FBI and other federal agencies secretly monitored the activities of civil rights and anti-Vietnam War activists.[58]

These examples provide evidence that in times of crisis, when fear is high, the federal government has reacted in ways which threaten civil liberties.[59] Presumably, the officials responsible for these measures were not much different from those who held office in more tranquil eras. Two of the presidents who participated in these reactions, Abraham Lincoln and Franklin Roosevelt, are regarded by historians as being among the best presidents in the history of the United States. Perhaps the explanation for these measures, many of which had public support when imposed, but in hindsight were clearly excessive, is that the neurology of the human brain can cause people to make bad decisions when motivated by fear. And this analysis can help explain why, in the aftermath of September 11, the federal government has turned to data mining projects that appear to threaten the privacy of ordinary people.

There have been signs, however, that government mining of commercial data could be subjected to greater restraints in the future. Some data mining projects have been canceled or suspended in response to privacy concerns. There is a very active and articulate privacy advocacy community in the U.S. which helps educates the public and puts pressure on government officials. Congress is becoming increasingly active in exercising oversight of federal agencies and is requiring reports on some data mining activities. Many agencies now have dedicated privacy officials who help shape new projects through privacy impact assessments and generally act to restrain abusive activities. Journalists have done good work increasing government transparency by informing the public of programs that affect personal privacy. And finally, there is traditional American skepticism of excessive governmental power

---

[58] *See generally* FRANK H. DONNER, THE AGE OF SURVEILLANCE: THE AIMS AND METHODS OF AMERICA'S POLITICAL INTELLIGENCE SYSTEM (1980).

[59] *See* Geoffrey R. Stone, *Civil Liberties v. National Security in the Law's Open Areas*, 86 BOSTON U. L. REV. 1315 (2006).

which can be a force restraining some of the more excessive forms of data mining. Many of these rational restraints, however, can be overcome by fear. Another major terrorist attack in the U.S. could quickly lead to even more intrusive data mining projects. Even without an attack, Congress demonstrated in August 2007 that it remains susceptible to arguments based on fear, when it temporarily amended the Foreign Intelligence Surveillance Act to permit some types of interceptions of electronic communications without prior authorization of the FISA court.[60]

Vii. Conclusion

Government mining of personal data in commercial databases for the purpose of detecting terrorism after September 11 is likely to have contributed to an erosion of public trust in government. Current law provides few restrictions on data mining, and allows broad-based examinations of personal data in apparent contradiction of the principle that government scrutiny of private lives should only occur when there is particularized suspicion. As in other periods of crisis in U.S. history, fear has led to government actions that reduce civil liberties. Although Congress has demonstrated that it is capable of acting as a restraining force, it remains susceptible to fear-based justifications for additional surveillance. Government reliance on data mining will probably increase in the near future. Another terrorist attack in the U.S., and the fear it would generate, would undoubtedly accelerate that trend.

References

Barr, R., 2007. Testimony of former Republican Congressman Robert Barr of Georgia at a U.S. Senate Judiciary Committee hearing titled "Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs" held on January 10, 2007, *available at* http://judiciary.senate.gov/ hearing.cfm?id=2438 (last visited July 27, 2007).

Bradley, C. et al., 2006. On NSA Spying: A Letter to Congress, *N.Y. Review of Books*, Feb. 9, 2006, *available at* http://www.nybooks.com/articles/18650 (last visited Aug. 14, 2007)

Brand, R 2004. Testimony of Rachel Brand, Principal Deputy Assistant Attorney General, U.S. Dept. of Justice, before the U.S. Senate Judiciary Committee, June 24, 2004, available at http://usdoj.gov/ olp/pdf/dojaag_brand_062204.pdf (last visited July 27, 2007).

[60] *See* Eric Lichtblau, James Risen and Mark Mazzetti, *Reported Drop In Surveillance Spurred a Law*, N.Y. TIMES, Aug. 11, 2007 at A1 (The article reported that the Bush Administration successfully argued that Congress should amend FISA because the process of obtaining court authorization for electronic eavesdropping was causing a reduction in the collection of intelligence. However, an opponent of the FISA amendment, Jane Harman, a Democratic U.S. Representative from California, was quoted as saying that the Bush Administration had "very skillfully played the fear card.")

Caute, D. 1978. *The Great Fear: the Anti-Communist Purge Under Truman and Eisenhower*, New York: Simon and Schuster.
European Union, 1995. Council Directive 95/46, 1995 O.J. (L281), often referred to at the Data Protection Directive.
Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (Nov. 4, 1950), art. 8, reprinted in *The Privacy Law Sourcebook 2003*, 325, (Marc Rotenberg, ed.)
Dempsey, J. and Flint, L. 2004. *Privacy's Gap: The Largely Non-Existent Legal Framework for Government Mining of Commercial Data, available at* http://www.cdt.org/ security/ usapatriot/ 030528cdt.pdf (last visited Aug. 15, 2007).
Donner, F. J., 1980. *The Age of Surveillance: The Aims and Methods of America's Political Intelligence System*, New York: Knopf.
Doyle, C. 2006. *National Security Letters in Foreign Intelligence Investigations: A Glimpse of the Legal Background and Recent Amendments, available at* http://www.fas.org/sgp/crs/intel/RS22406.pdf (last visited July 25, 2007).
European Union and United States Department of Homeland Security, 2007. Agreement Between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS), *available at* http://register.consilium.europa.eu/pdf/en/07/st11/st11595. en07.pdf (last visited Aug. 13, 2007.)
Harper, J. 2007. Testimony at U.S. Senate Judiciary Committee Hearing Entitled "Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs," *available at* http://judiciary. senate.gov/ testimony.cfm?id=2438&wit_id=5949 (last visited July 19, 2007).
Hoofnagle, C. J. 2004. Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, 29 *North Carolina Journal of International Law & Commercial Regulation* 29:595-626.
Jonas J. and Harper, J. 2006. Effective Counterterroism and the Limited Role of Predictive Data Mining, *available at* http://www.cato.org/pub_display.php?pub_id=6784 (last visited July 27, 2007).
Kennedy, D. M. 1980. *Over Here, the First World War and American Society*, New York: Oxford University Press.
Leahy, P. 2007. Statement of Democratic Senator Patrick Leahy at a U.S. Senate Judiciary Committee hearing titled "Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs" held on January 10, 2007, *available at* http://judiciary.senate.gov/hearing.cfm?id=2438 (last visited July 27, 2007).
Levin, M. B. 1971. *Political Hysteria in America: the Democratic Capacity of Repression*, New York, Basic Books.
Lichtblau, E. and Johnston, D. 2007. Court to Oversee U.S. Wiretapping in Terror Cases, *N.Y. Times*, Jan. 18, 2007 at A1.
Lichtblau, E. and Risen, J. 2006. Bank Data Sifted in Secret by U.S. to Block Terror, *N.Y. Times*, June 23, 2006 at A1.
Lichtblau, E., Risen, J. and Mazzetti, M. 2007. Reported Drop In Surveillance Spurred a Law, *N.Y. Times*, Aug. 11, 2007 at A1
Meyer, J. and Miller, G. 2006. U.S. Secretly Tracks Global Bank Data, *Los Angeles Times*, June 23, 2006 at A1.
O'Harrow, R. Jr., 2005. *No Place to Hide*, New York: Free Press.
Organization for Economic Cooperation and Development, 1980. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at* http://www.oecd.org/dsti/sti/it/ secure/prod/ PRIV-EN.HTM (last visited July 24, 2007.)
Privacy and Security Law Report, 2007.
_____Multidistrict Panel Consolidates More Suits In Web of Claims Related to NSA Surveillance, 6:324
_____Sixth Circuit Rejects NSA Spying Challenge; Finds Journalists, Attorneys Lack Standing, 6:1081
Ponemon Institute, 2007. Privacy Trust Study of the United States Government, *available at* http://www.epic.org/privacy/pdf/2007ponemon.pdf (last visited July 24, 2007).
Schneier, B. (2007). Why the Human Brain Is a Poor Judge of Risk, *Wired News*, March 22, 2007, *available at* http://www.schneier.com/essay-162.html (last visited July 27, 2007).
Seifert, J. W. 2007. *Data Mining and Homeland Security, An Overview, available at* http://www.fas.org/ sgp/crs/intel/RL31798.pdf (last visited July 19, 2007)
Simon, J. F. 2006. *Lincoln and Chief Justice Taney*, New York, Simon and Schuster.
Slobogin, C. 2005. Subpoenas and Privacy, *DePaul Law Review* 54:805-45.
Solomon, J. 2007. FBI Finds It Frequently Overstepped in Collecting Data, *Washington. Post*, June 14, 2007 at A1.
Solove, D. J. 2006. A Taxonomy of Privacy, *University of Pennsylvania. Law Review* 154:477-560.
Stone, G. R. 2006. Civil Liberties v. National Security in the Law's Open Areas, *Boston University Law Review* 86:1315
Swire, P. 2007. Interview on the Public Broadcasting System television program *Frontline* titled "Spying on the Home Front" broadcast on May 15, 2007.
United Nations Universal Declaration of Human Rights (1948), art. 12, reprinted in *The Privacy Law Sourcebook 2003*, 318, (Marc Rotenberg, ed.)
United States, Federal Rules of Criminal Procedure, Rule 17.
United States Code
_____Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-62 (2000).
_____Omnibus Crime Control and Safe Streets Act of 1968, Title III, 82 Stat. 211, 18 U.S.C. §§2510-20.
_____Protect America Act of 2007, Pub. L. 110-55 (2007)
_____Privacy Act of 1974, 5 U.S.C. § 552a (2000).
_____USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. 109-177, §§115-19 (2006).
United States Department of Justice, Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters*, March 2007, *available a*t http://www.usdoj.gov/ oig/special/s0703b/final.pdf (last visited June 26, 2007).

United States District Court for the Southern District of New York, Doe v. Ashcroft, 334 F.Supp.2d 471 (S.D.N.Y. 2004).
United States District Court for the District of Connecticut, Doe v. Gonzales, 386 F.Supp.2d 66 (D. Conn. 2005).
United States Government Accountability Office, *Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues Remain*, May 2007, *available at* http://www.gao.gov/new.items/d07346.pdf (last visited June 4, 2007).
United States Deptartment of Health, Education and Welfare, 1973. *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*
United States Supreme Court
_____Berger v. New York, 388 U.S. 41 (1967).
_____Hale v. Henkel, 201 U.S. 43 (1906).
_____Katz v. United States, 389 U.S. 347 (1967).
_____Michigan v. Sitz, 496 U.S. 444 (1990).
_____New York v. Berger, 482 U.S. 691 (1987).
_____Olmstead v. United States, 277 U.S. 438 (1928).
_____U.S. v. Miller, 425 U.S. 435 (1976).
_____Washington v. Chrisman, 455 U.S. 1 (1982).
Westin, A. F. 1967. *Privacy and Freedom*, New York: Atheneum.
Wilentz, S. 2005. *The Rise of American Democracy*: New York: Norton.

Published by the Forum on Public Policy