Ethics of Data Mining and Aggregation

Brian Busovsky

Introduction: A Paradox of Power

The terrorist attacks of September 11, 2001 were a global tragedy that brought feelings of fear, anger, and helplessness to people worldwide. After sharing this initial reaction, Hank Asher, founder of Seisint, a private company that maintained a massive database filled with personal information records about individuals worldwide, had an idea. Just days after 9/11, Asher realized that he had the ultimate resource for identifying the terrorists at his finger tips: a massive database filled with detailed information about the traits, actions, and tendencies of 450 million people (No Place to Hide). After realizing the power of the database, Hank developed a set of complex search algorithms for the purpose of searching the database to identify individuals whose records contained certain attributes, events, or pattern of events. Two of the traits specified in the algorithms were male individuals of Muslim descent (No Place to Hide). Thus, Asher's supercomputer searched for the potential terrorists and quickly narrowed the list of suspects from four hundred and fifty million individuals to four hundred and nineteen, five of which were later found to be directly involved with the attacks (No Place to Hide). At first glance, Asher's database and algorithms appeared to be an incredible tool in the war against terrorism and, as a result, received federal funding and became known as The MATRIX (The Multistate Anti-TeRrorism Information eXchange). The database and the search techniques made it possible to organize and search troves of data for potential terrorists and terrorist threats. Consider, however, that four hundred and fourteen of the individuals that showed up on Asher's list had no readily apparent connections to the terrorist attacks. They simply had a certain set of traits and events in their records that matched those that were being searched for by the queries. Despite their innocence, they have undoubtedly been identified as potential threats and are being watched carefully by the government. The MATRIX and similar government programs, such as Total

Information Awareness, have an undeniable power to improve national security. At the same time, however, they have an unheard of ability to gather and sort information from nearly every aspect of an individual's life which can subsequently be used to categorize and potentially condemn them. This paradox of power has created one of the most heavily debated ethical dilemmas of our time: personal privacy versus national security.

The Growth of Database Use

The use of databases to harness the power of data has grown and continues to grow rapidly for three primary reasons: databases can transform data into information, an increase in the amount of available data, and significant improves to both the hardware and software components of database technology. First, organizations are beginning to understand that databases have the power to sort through massive amounts of meaningless *data* and turn it into understandable and useable *information*. Companies are using them to sort and analyze consumer data and transaction data to uncover trends that will enable them to more successfully target market their customers. Amazon.com, for example, stores information about which items an individual views, which items she buys, and which items she sells. This helps the company to uncover patterns and correlations between certain items, thus enabling the company to improve their target marketing and their bottom line (Associated Press). The database technologies make it possible to eliminate existing paper-based systems and digitize data, which ultimately makes it significantly easier to manage and effectively utilize it. As organizations have come to realize this power, the use of databases has grown significantly.

The second factor that has brought about increased use of database technology is the development and widespread use of new consumer technologies such as the Internet and cell phones. These widely used items have increased the amount of data available for organizations to store, query, and use to their advantage. The data from these devices, such as "cookies" from Internet browsing and call logs from cell phones, can be added to a database, sorted into existing personal records, and searched to uncover new patterns. There have also been significant developments in non-consumer-use devices, such as security cameras and RFID (Radio Frequency Identification) chips, which can be used by government entities to track and monitor individuals or by companies to track inventories

and monitor employees. Companies can use the data to enhance their services and bottom lines by improving their supply chain management and reducing employee theft. The government can use the data from these technologies to uncover patterns of activity, identify suspicious individuals, and monitor them. The power of both varieties of technology (consumer and non consumer) to increase the amount of data available has been furthered by an interesting and unusual cost trend. Rather than seeing increasing costs for enhanced devices, there is a general pattern of decreasing costs. For example, as a microchip becomes smaller and more powerful it also becomes cheaper (Kelly). This has enabled new devices to become heavily deployed in our society, which has increased their ability to generate even larger amounts of data that companies and government entities can use to enhance the power of their databases.

Finally, the third major factor that has influenced database use is the advancement of digital storage technology. Data storage devices, such as mainframes and hard drives, are decreasing in price, becoming physically smaller, growing in capacity, and becoming faster (Sadashige). This has enabled almost every company, large or small, to store information digitally. The subsequent development of advanced database software has made it possible to utilize the capacity by making it easy to effectively store, organize, and search the data held on the devices. Ultimately, the combination of these three factors (the realization of database power, increased number of data sources, and availability to all) has led to rapid growth in the use of databases and database tools by companies of all sizes. This paper will focus on government use of databases and will examine the ethical issues surrounding the implementation of government data mining programs, like The MATRIX, to gather and sort data about people.

Government Use of Databases

In an attempt to improve national security and prevent future terrorist attacks, the government has made several attempts to combine data from public and private sector databases to create a "grand, centralized database" that contains personalized information records that are composed of as much data as possible on as many people as possible (Democracy Now). Despite public declarations of anxiety about privacy infringement, the government has persisted in building a massive database and has used the factors

described above as their rationale. Companies nationwide are taking advantage of the new database technologies to assess and revamp their business models to increase profits. Each company uses their individual database(s) to store customer data that pertains directly to their company. Cell phone companies, for example, maintain huge databases of call records to prepare billing statements and to understand what pricing options they may be able to offer to attract more customers (Markoff). Similarly, Amazon maintains a database with information about the items that an individual has purchased, viewed, or sold. Individually, each of these databases poses only a minor threat to personal privacy as they only reveal a portion of the habits of the individual the information pertains to. The government is taking advantage of the wide use of databases by combining the information contained in each individual database in one "grand, centralized database". The privacy threat inherent in such a database comes from its ability to bring together the information held in previously autonomous databases into one massive database that contains significantly more in-depth records about each individual. By combining information from multiple databases, an administrator sitting in front of a computer screen in a government office can view intricate details of an individual's day-to-day life by simply typing in search queries, commonly known as data mining. Data mining is the process of extracting desired data from a database using a search language such as SQL. This is the *ultimate* privacy threat of our time and forces us to consider that the government is making a strong character judgment about the citizens of this country. The use of data mining suggests that federal agencies consider individuals to be inherently bad and that they must be monitored to avoid terrorism.

The government has embarked upon numerous large-scale data mining initiatives over the past several years. The first widely recognized attempt to combine information from multiple databases into a central database was called Total Information Awareness (TIA). The program was started by John Poindexter and the Defense Advanced Research Projects Agency (DARPA – the research arm of the Department of Defense) in early 2002. The objective of the project was to attempt to gather as much information as possible about individuals and store it in a massive database maintained by the government. The information in the database allegedly included information from online activity, credit card transactions, health records, academic institutions, bank statements,

phone calls, and a variety of other sources (Scheeres). Information for the database was also obtained from databases maintained by private companies, such as JetBlue Airlines and the Professional Association of Scuba Instructors (Sullivan). The ultimate goal of the program was to aggregate as much data as possible and use complex queries and algorithms to sort the data to identify patterns and, hopefully, uncover and deter potential terrorist attacks. Despite a strong attempt by supporters to build government trust in the program by renaming it to Terrorism Information Awareness and noting that it would be used primarily for foreign intelligence, lawmakers eventually decided to shut the program down in 2003. The opponents cited that the program was far too invasive, compromised personal privacy rights, and gave no guarantees of success (Hulse). TIA had presented an excellent opportunity to eliminate future terrorist attacks, but the public was simply not ready to sacrifice privacy in exchange for the promise of increased security. Despite public opposition to the program, TIA was not the last effort by the government to gather data about individuals to deter terrorism.

Following the cancellation of TIA, The MATRIX program (The Multistate Anti-Terrorism Information Exchange) emerged and quickly gained recognition and funding from the federal government. MATRIX differed from TIA in that each state was given the option to join the program based on its ethical stance on the privacy issues at hand. The MATRIX was touted as less of a threat to privacy because it was run at the state level rather than the federal level and supposedly collected less information (creators refused to specify exactly what information was gathered). Further, supporters claimed that it simply computerized the existing paper sorting processes used before the growth of database technology and that the program only aggregated data that was already available to individual companies (The Matrix). Thus, essentially all the program did was combine the information in one database rather than keeping it distributed over several (The Matrix). The aggregation of this information into a single source is precisely the problem with these programs. As discussed earlier, dispersed information reveals a significantly smaller and less-detailed portion of the habits of an individual being analyzed. Aggregating data, on the other hand, enables an analyst to view a full and detailed picture of the day-to-day activities and habits of the subject under investigation. Thus, one of the primary arguments in favor of the programs is fundamentally flawed. Regardless of the

declarations of preservation of privacy by supporters, most states were leery of the program and chose not to join. At the height of its success in 2003, the program was being used in thirteen states, but six dropped out shortly after and the remaining seven began using the program for tracking criminals rather than identifying terrorists (The Matrix). Federal funding for the program ended in 2005 and the program was terminated later in the same year (ACLU Applauds).

Public opposition to the use of these programs has not deterred the government from continuing to make attempts to develop and maintain these databases. In fact, recent articles have reported that Total Information Awareness has continued to exist as a secret program being operated under the cloak of the National Security Agency (Democracy Now). This situation brings to light the government's ability to make secret that which it desires to keep from the public. Thus, the public is at the mercy of secret and public initiatives alike. Unlike public initiatives, society is unable to mount opposition to secret programs, which means that the ideals of the government will take precedence over those of the public. In essence, Americans are subject to the whims of the government. TIA and MATRIX are only the most notable and public examples of data mining efforts. TIPS (The Terrorism Information and Prevention System) and CAPSII (Computer Assisted Passenger Pre-screening System II) are similar government developments with similar objectives and ramifications. These program have simply received less public attention for a variety of reasons. The government has developed numerous programs for data mining and aggregation and, despite opposition, is continuing to utilize these programs to aggregate information to sort and analyze people.

Potential Implications of Data Aggregation

There are a huge number of potential consequences that may arise from these government programs. The first and most readily apparent outcome of the program is its intended effect: the identification and aversion of future terrorist attacks with the ultimate outcome of increased security and trust in government policies. It seems unlikely that increased trust in the programs will be a result. Recent government actions (i.e. – the war in Iraq, the poor handling of Hurricane Katrina, the passing of the Patriot Act, etc.) have already worked to degrade public trust in the government. Thus, the majority of

informed citizens are viewing these government programs with an eye of doubt and will need major evidence of their positive attributes to accept them. The nature of the programs, however, eliminates any evidence of an attack. Thus, the government can say that they have deterred the next 9/11, but there will be no way to prove the statement because the program will have allegedly stopped the event from occurring. Even if the program is able to eliminate some attacks, any failure of the program to stop terrorist activity will discredit any positive reputation the program has managed to gather. If the program fails to eliminate the terrorist threat, or even a single attack, the public will cry out and the government will have a multi-million dollar tool that can no longer be used for the intended purpose. In this event, there is a strong possibility that the database will be used for other, as of yet undefined, purposes. Ultimately, the program does indeed have the potential to eradicate terrorism, but it is more likely that it will continue to be viewed as an abuse of power and a violation of civil rights.

As the government has continued to utilize and develop ethically questionable tactics and programs, there have been growing levels of doubt in the public that the government is acting in the best interests of the people. If the level of doubt reaches high enough, there may be a growth of hatred towards the government, which may lead to social unrest or rebellion. While it is unlikely that society will never reach the point of insurgence, it is almost inevitable that data mining initiatives will push society towards this end of the spectrum rather than the approving end. The programs may also result in the growth of social paranoia and the development of individual tactics geared towards preserving privacy (Simons). Those aware of the databases may work to maintain their privacy by avoiding things the government is tracking, such as cell phones, Internet usage, and credit card transactions, in an attempt to eliminate their paper and data trails. These tactics will work to safeguard privacy but will also hinder social interaction and result in an isolated and secretive society. This new model of culture may reverse economic development as services monitored by the government are boycotted (Simons). This has the potential to force huge numbers of companies into bankruptcy, which will increase unemployment rates, decrease per capita income, and reduce the standard of living. These developments will force Americans to become more reliant upon government assistance, which ultimately creates a vicious cycle that gives even more

power to the government. This internal situation does not even begin to examine or consider the impact of these programs on a global level.

In the current era, it is critical to examine how a new government program will influence foreign relations. An essential part of any government data mining program is gathering and querying information on foreign individuals. This suggests to foreign individuals, much like American citizens, and governments that the United States considers them to be threats to national security. This has a strong potential to create feelings of animosity towards the United States, which may lead to the degradation of foreign relations and the isolation of America from the rest of the world. This has major implications for the ability of our country to function in a world that is becoming increasingly dependant upon the global economy.

Finally, the information contained in the database may be compromised or distorted because large pools of information are natural targets for hackers and ill-intentioned computer geniuses. The ramifications of an attack on a centralized database are enormous and unpredictable. Two notable potential outcomes are hackers stealing and/or changing information in the database, both of which would compromise the integrity and the security of the information (Simons). Although the government has assured the public that the database is secure, there is no way to know how protected it is until a break in is attempted. The information in the database will be considered the master set, meaning that any information contained in the database will trump conflicting information from other sources. Thus, information that was covertly changed by a hacker may lead to false accusations of terrorist intentions. Ultimately, the negative consequences of data mining and aggregation programs drastically outweigh the potential benefits of the programs. It is reasonable to assume that the government has fully considered these possibilities and has decided in favor of pursuing the programs, which forces the public to consider where the priorities of the government lie.

Eerie Similarities

The government efforts to track and monitor individuals, along with a variety of other recent government actions, have eerie similarities to the society envisioned by George Orwell in his novel 1984. He described a country where individuals are monitored via "telescreens", devices that combine the functionality of a television and a video camera. These devices are placed permanently in homes, offices, cubicles, street corners, shop windows, and everywhere else people go. Individuals in the society live with the knowledge that they are being watched and that anything out of the ordinary (a strange facial expression, a different route home from work, a new purchase, etc.) may draw attention from the secret police (Orwell). Thus, they "had to live – did live, from habit that became instinct – in the assumption that every sound [they] made was overheard, and, except in darkness, every movement was scrutinized (Orwell)." They lived their lives in such a way that they wouldn't draw attention to themselves, generally meaning that they partook in the same ordinary events every day. In our society, individuals are at liberty to make almost any facial expression they please without fear of getting in trouble. With the advent of data mining, however, it has become necessary to be cognizant of the fact that our actions are being monitored and that a strange sequence or combination of events, even those that may not be considered to be out of the ordinary, may become a red flag for terrorist activity. If a data mining program becomes a fixture in our society, it will force individuals to alter their lifestyles and live in such a way that they intentionally avoid certain activities and interactions, regardless of their intentions, in order to avoid interrogation and harassment. This ability to influence society and force individuals to alter their lifestyles may be an ulterior motive of government data mining projects.

Other recent actions suggest that our government may be on a path towards becoming the Big Brother organization proposed by Orwell. In 1984, the government is an all-powerful entity that rules without opposition. The individuals in the society believe, either forcibly or by choice, that the government represents supreme goodness and is always acting in the best interests of the public. Similarly, the government also believes that it is doing what is best. Orwell's government assumes that people are threats to the social order and decided that it was necessary to monitor them in order to maintain peace (Orwell). Readers understand how ludicrous it is to believe that the

policies enacted by Orwell's government are good for the people because they live in a society where the government is a representative of the desires of the people. If individuals are not careful, however, our society and the individuals in it will fall victim to an overbearing and powerful government that also genuinely believes that it is acting in the best interests of the people. By taking this consequence-based ethical approach of doing what it believes will benefit the greatest number of people, the government is bypassing duty ethics by disregarding its responsibility to be a representative of the people. Further, the government has begun carrying out questionable tactics in secrecy in order to avoid the negative effects of public outcry.

Classification of certain programs suggests that the government understands the questionable nature of the programs, but believes so strongly that the tactics are necessary to security that it is willing to act upon them without informing the public. Even further, the government is giving itself more power to make and enact decisions without public approval by weakening the laws surrounding the development of surveillance programs (Stanley). This gives the government increasing levels of power to carry out questionable initiatives that it deems necessary to national security without exposing them to the public eye. Ultimately, it is vital to constantly scrutinize government actions and remember that it is the duty of the government to represent the interests of the public rather than the interests of a select few heads of state (Vogt). This necessary scrutiny requires us to give heavy consideration to the data mining initiatives and decide if the government is indeed representing the best interests of the society or if it is pursuing the contents of an alternative agenda.

Resolutions

Based on the discussion of the data mining programs and their potential consequences, there are three basic courses of action that the American public can choose to embark upon with respects to the future of data mining and aggregation. The first of these is to accept data mining and diminished privacy in return for increased security. This option requires individuals to place faith in the government to do what is right for the society despite questionable government classification and secrecy. The second option is to strike a compromise wherein some of the government policies are accepted

and others are refuted. The final option is to rebel against data aggregation and mining programs in order to preserve our privacy. This option assumes that there are other ways to deter terrorist attacks or that the terrorist threat is not worth sacrificing privacy for. These options are the key players in the ethical debate over privacy versus security and, like most ethical dilemmas, there is no clear cut answer. Thus, it becomes the job of each person to weigh all sides of the debate and make an informed decision that they are willing to stand behind.

By accepting data mining, American society will essentially give in to the rise of an invasive and overbearing government. Alan Moore and David Lloyd's graphic movie, V for Vendetta, describes a society controlled by such a government. "Both [writers] were political pessimists, and decided that the world they wanted to portray…would be pretty grim, bleak and totalitarian (Boudreaux)." If the government is given the power to watch every individual's every action, any rights the public had or once believed they had would be in danger. The American people would indirectly be forced to forfeit any sense of privacy in hopes of gaining complete security from the government. The problem here is that the public would have no choice but to comply with the government rules of right and wrong and what they could and couldn't do, which would eventually lead to the disappearance of the country once defined as the land of the free. This option may become more acceptable if terrorism becomes rampant and widespread, but until then it seems to be the least likely of the outcomes described above.

The second option is to attempt to reach a compromise with the government regarding the use of data mining programs. This compromise could come in a variety of forms ranging from disclosure of details of the program to limitations on the type and amount of data that may be collected on a certain individual. Despite the alluring nature of this option, however, there are two fundamental flaws with the logic inherent in the proposal. First, recent government trends of secrecy and confidentiality will make it impossible for the public to know if the government is indeed holding up its end of the bargain. The actual nature of TIA is a prime example. The government claimed that the program had been dissolved, but it was in fact being operated secretly under a new name in a new agency. The government has extremely secret agencies, such as the NSA, that are able to keep secret any information they deem unfit for public knowledge, thus

making it impossible to reach a secure compromise. The second fundamental flaw with this option is that reaching a compromise will decrease the effectiveness of the program. If the public and the government agree to disclosure of information about the program, terrorists will be able to understand how the program works and develop ways to avoid detection. Similarly, decreasing the pool of information sources will decrease the ability to identify patterns that suggest terrorist activity. Ultimately, a compromise will force the government to lie or it will decrease the overall effectiveness of the program, thus leading to the sacrifice of certain amounts of privacy to a program that has less potential to positively influence security.

The final option is to rebel against data aggregation and mining programs in order to preserve individual privacy. This option would force the government to utilize other potentially less invasive tactics to identify and deter terrorist threats. Not only would this be a much more publicly supported solution (depending, of course, on the new tactics), but it would most likely lead to increased public trust in the political decision makers of the country. If the government recognizes and responds to public skepticism, there will hopefully be widespread feelings of confidence, trust, and cooperation. Government response will lead to the development of a united society wherein the government and the public are on a cooperative team devoted to the protection of the country. The new solution would potentially provide two primary benefits: (1) Increased trust in the government and (2) preservation of individual privacy. The new solution would eventually lead to the highest amount of utility provided to the greatest number of people. By providing increased utility to society as a whole, the standard of living would go up (other things equal), national security would be improved, and public rights would be sustained. Ultimately, this option will foster the growth of cooperation within the nation and will enable the government and the public to work together to create terrorism avoidance techniques that sustain privacy and improve national security.

Closing Remarks

The combination of the growth of databases and fear of terrorist attacks are making the society and government presented in 1984 a distinct possibility. The future of our democracy depends upon our ability to judge government actions and consider if they

are indeed what is best for society. The government is frequently telling the public what it believes it wants to hear while concurrently developing questionable programs outside of the public eye. These initiatives are creating major modifications to our society and the lives led by individuals in it without public approval. Thus, it is becoming an increasingly important duty of the people to examine the words of spokespersons and to understand the real issues at hand to decide if the government is indeed doing what is right. A centralized database is a huge violation of individual privacy regardless of government guarantees that its use will be limited and heavily monitored. There is no way to know how a tool with such vast capabilities will be used by the government and its slew of secretive agencies. Further, there is no way to know if our information is being scrutinized and watched or if it is one of the millions sitting idly. Many Americans have claimed that they are willing to divulge their privacy rights slightly in order to increase national security simply because they have nothing to hide (Vogt). The average citizen, however, has no way of knowing what series of events, details, and interactions are considered to be indicators of terrorist activity. Thus, what is considered to be nothing by many may indeed be everything. Further, these databases are more than small intrusions into privacy. Rather, they represent the ultimate invasion; they give a single individual the power to sit behind a computer screen and view the intricacies of each and every one of our lives. This means that "nothing is [your] own except for the few cubic centimeters inside your skull (Orwell)," and recent technological projects are beginning to threaten this space as well (Murray). It is critical that the public heavily scrutinizes government actions and takes a stand against the proliferation of government tactics that threaten privacy. Americans need to discontinue their passive observations of government policy and let the representatives of the public know how they feel about the growth of the Big Brother ideal in this country.

Works Cited

"ACLU Applauds End of "Matrix" Program." American Civil Liberties Union. April 2005. 8 Mar. 2006 <http://www.aclu.org/privacy/spying/15324prs20050415.html>

Associated Press. "Amazon Knows Who You Are." Wired News. Mar. 2005. 20 Mar. 2006 <http://www.wired.com/news/ebiz/0,1272,67034,00.html>

Boudreaux, Madelyn. "An Annotation of Literary, Historic, and Artistic References in Alan Moore's Graphic Novel, V for Vendetta." Mar. 2005. 20 Mar. 2006 <http://www.stahl.bau.tu-bs.de/~hildeb/vendetta/annotations/v-for-vendetta.1.shtml>

Hulse, Carl. "Congress Shuts Pentagon Unit Over Privacy." The New York Times. Sept. 2003. 20 Apr. 2006 <http://www.nytimes.com/2003/09/26/politics/26SURV.html?ex=1146715200&en=7ee39a8d863b5044&ei=5070>

Kelly, Kevin. "New Rules for the New Economy." Wired Magazine (1997): 8-10.

"No Place to Hide." American RadioWorks. Narr. John Biewen and Robert O'Harrow, Jr. Transcript available at: <http://americanradioworks.publicradio.org/features/noplacetohide/index.html>

Markoff, John. "Taking Spying to a Higher Level, Agencies Look for More Ways to Mine Data." The New York Times. Feb. 2006. 17 Mar. 2006 <http://www.nytimes.com/2006/02/25/technology/25data.html?ei=5070&en=9716a9fe318e5875&ex=1145592000&adxnnl=1&adxnnlx=1145419581-9FGk2D+fWyB2GtJPfV7oYQ>

"The Matrix: Total Information Awareness Reloaded – Data Mining Moves Into the States." American Civil Liberties Union. Oct. 2003. 2 Mar. 2006 <http://www.aclu.org/privacy/spying/15694res20031030.html#attach>

Murray, Frank. "NASA Plans to Read Terrorist's Minds at Airports." The Washington Times. Aug. 2002. 30 Mar. 2006 <http://www.maebrussell.com/Articles%20and%20Notes/NASA%20to%20read%20minds%20at%20airports.html>

Orwell, George. 1984. New York: Penguin Books, 1949.

Sadashige, Koichi. “Data Storage Technology Assessment.” National Media Laboratory. Mar. 2003. 15 Apr. 2006 <http://www.imation.com/government/nml/pdfs/AP_NMLdoc_DSTAssessment.pdf>

Scheeres, Julia. “Bush Data-Mining Plan in Hotseat.” Wired News. Feb. 2003. 15 Mar. 2006 <http://www.wired.com/news/politics/0,1283,57568,00.html>

Simons, Barbara. The Association for Computing Machinery. Jan. 2003. 23 Apr. 2006 <http://www.eff.org/Privacy/TIA/acm-letter.php>

Stanley, Jay, Barry Steinhardt. “Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society.” American Civil Liberties Union. 2003: 9 - 10.

Sullivan, Bob. “Are Private Firms Helping Big Brother Too Much?” MSNBC. Aug. 2004. 18 Mar. 2006 <http://www.msnbc.msn.com/id/5737239/>

“Total Information Awareness Lives On Inside the National Security Agency.” Democracy Now. Feb. 2006. 18 Mar. 2006 <http://www.democracynow.org/article.pl?sid=06/02/27/1519235>

Vogt, Carlton. “Pentagon Data Mining: Just Say No.” InfoWorld. (n.d.). 4 Mar. 2006 <http://www.infoworld.com/articles/op/xml/02/11/22/021122opethics.html>

Suggested Readings

Bergstein, Brian. “In this Data-mining Society, Privacy Advocates Shudder.” Seattlepi. Jan. 2004. 22 Mar. 2006 <http://seattlepi.nwsource.com/business/154986_privacychallenge02.html>

“Data Mining: Federal Efforts Cover a Wide Range of Uses.” United States General Accounting Office (GAO). May 2004. 18 Mar. 2006 <http://www.gao.gov/new.items/d04548.pdf>

Granneman, Scott. “RFID Chips are Here.” Security Focus. June 2003. 20 Mar. 2006 <http://www.securityfocus.com/columnists/169>

Ramasastry, Anita. “The Safeguards Needed for Government Data Mining.” FindLaw. Jan. 2004. 27 Feb. 2006 <http://writ.news.findlaw.com/ramasastry/20040107.html>

“Total Information Awareness Resource Center.” 10 Mar. 2006. Collection available at <http://www.geocities.com/totalinformationawareness/>

Singel, Ryan. “Pentagon Defends Data Search Plan.” Wired News. May 2005. 26 Feb. 2006 <http://www.wired.com/news/privacy/0,58936-0.html?tw=wn_story_page_prev2>