# Consumer Privacy vs. Government Surveillance

Michael T. Turnley
BADM 590 – Trustworthy Computing
Final Project

This project investigates known *public* standards of consumer privacy and the surveillance practices of the American government. At the root of these issues is the evaluation of current civil liberties and laws in place and their applicability tin the face of technological advancement. The privacy issue in this analysis is concerned with both an individuals' communications and the tracking of their location and movement. This is accomplished by performing a state-of-the-art survey of current trends and practices. The technical aspects of this project are addressed by examining the following topics: technological means by which the US government tracks individuals, and practices the government uses to determine whom to investigate. The business aspects are addressed by looking into: proposed legislation for privacy, current laws, roles played by communications providers, and roles played by data resellers. The privacy issue evokes additional factors such as trust and safety, which will be addressed as well.

The emergence of terrorist-related issues has changed the lives of all Americans, and has renewed government interest into the daily lives of inhabitants in the US. Although most of these changes have been perceivable, such as the developments of the terrorist security threat level system and the Department of Homeland Security, others have been overlooked; namely those regarding our data personalities in the digital realm. Moreover, with the era of ubiquitous computing the issues of privacy and surveillance are slowly re-emerging and long accepted policies are being reevaluated. Measures to protect our alternate representations needs to be pushed to the fore so that we may make informed decisions regarding such information. This project is to serve as an informative, concise source that sheds light on a topic that affects all inhabitants of the United States.

***Privacy***

What is privacy? According to www.dicitionary.com privacy is defined as: "The quality or condition of being secluded from the presence or view of others." This definition, though simple is not restricted only to the physical realm. It has relevance in the digital world. A more concrete definition of privacy in the context of this project is an individuals right to:

- Control the information collected about them.
- Control how that information is used.
- Control who has access to the information
- The ability to access their personal information.

This definition adapted from a lecture [Thomas Kleyle, PriceWaterhouse] illustrates the varying aspects of the privacy issue and how it can be adapted to fit different contexts. It is this chameleon quality of privacy that instantiates elusiveness.

***Technology***

In today's technological society, our privacy has become a highly valued commodity that is collected, purchased and sold. There are numerous companies whose sole mission is to collect and distribute this private, sensitive information that was once solely controlled by the owner. As we turn to the Internet and other wireless technologies to perform everyday tasks in the digital world, we are putting the confidentiality of our lives in jeopardy.

***Internet***

Every day, Americans use the Internet and wireless services to access, transfer and store vast amounts of private data. Information usually stored in physical form (e.g. financial statements, photos, etc.) are now stored in digital form on networks and in databases. More and more of our lives are conducted online and more and more personal information is transmitted and stored electronically.

The Internet itself is a new communications medium for social organization. Because of its democratic, decentralized, and open nature, the Internet is the first

communications medium that allows users to reach and create communities of interest despite geographic, social, and political barriers.

Privacy is the main reason why non-users still avoid the Internet. The protection of privacy is becoming more of a concern amongst existing users. While privacy faces threats from both private and government intrusions, existing privacy laws and practices fails to provide comprehensive protection.

***Internet vs. Privacy***

Tools of varying types: legal, technical, and self-regulatory are being designed to address the privacy concerns of Internet users. Objectives to address this issue include: setting limits on government access, ensuring that new technologies are designed to protect rather than diminish privacy, and the development of federal legislation to set standards for consumer privacy.

Individuals using the Internet can use new tools to protect their privacy. From anonymous mailers and web browsers that allow individuals to interact anonymously, to encryption programs that protect e-mail messages as they pass through the network, individuals can harness technology to promote their privacy.

But it is not just individuals' self-interest leading us toward increased privacy protection. Faced with numerous surveys documenting that the lack of privacy protections is a major barrier to consumer participation in electronic commerce, businesses are beginning to take privacy protection more seriously. Both cooperative and company specific self-regulation efforts have emerged. A growing number of companies, under public and regulatory scrutiny, have begun incorporating privacy into their management process and actually marketing their "privacy sensitivity" to the public.

## TECHNOLOGICAL

Technology is rapidly becoming omnipresent; driving this information-based transformation is the movement to make computing more ubiquitous. One cannot go

about daily activities without being affected by technology. While it can be argued that technological advancements make everyday tasks easier to accomplish, one may also argue that for what we gain from these many conveniences we pay by disclosing information about ourselves that many times we think we still have control over; unfortunately we typically do not.

The issue arises when we relinquish control of this information, either voluntarily or involuntarily. Businesses rely on this information for marketing purposes, however, businesses are not the sole organizations interested in this information. The US government is also interested. Government agencies are more and more relying on the surveillance potential of consumer products as well as the development of their own technologies to perform improved data analysis and surveillance.

The government has vast technological resources at its disposal. Among several of the emerging technologies employed by the government are: data mining [in databases and email], cellular phones and global positioning systems (GPS), Keystroke loggers, and Echelon.

***Data Mining***

Data mining is concerned with the process of searching large volumes of data for patterns.

Key words commonly used in the data mining community are:

- Pattern-based – involves searches of large databases where the query does not name an identifiable data element (address, bank account, name, etc.), but instead seeks information that matches or departs from a pattern
- Subject based – these are queries that seek information about a particular subject already under suspicion based on previous information from traditional investigative means, this type of query uses identifiable data elements.
- Link analysis – this involves the process of finding relationships among individual subjects in or across a dataset(s). This analysis can be either subject based or pattern-based.

- Risk assessment – is a hybrid approach that draws together information from different databases, which can then be profiled in an attempt to identify specific patterns.
- Identity resolution – this involves determining whether information from various sources all correspond to the same subject.
- Screening – is the process of comparing a subject to source of data, similar to a type of approval process, it can also be performed by conducting a risk assessment with multiple factors.

These varying methods are used to mine data warehouses of information to find inferences and relationships between colossal amounts of information provided by data warehouses.

***Cellular phones & global positioning systems***

Location technology is becoming more popular because it offers the consumer added safety, security and convenience. One cannot deny the comfort felt by having a cellular phone at one's disposal. From the point of view of business, the market place opportunities provided by wireless devices is immensely vast. Cellular phones are by far the most popular; with global positioning systems and other wireless computing devices close behind.

When the power is on, cellular phones continuously search for nearby signal towers to send identification information. This information is then used to determine the location of the phone so that calls may be routed to the appropriate cell. This information can also be broadcast through the duration of a call. In this manner, a person with a cellular phone can have their locations traced. This transaction of information between the towers and the cellular phone can be logged and stored. As a result, anyone may be able to trace all previous movements of a cellular phone user. From a technological perspective, this technology implemented by the manufacturer alleviates the task [by government] of physically tracking individuals' movements.

Global positioning systems (GPS) offer its owners many innovating services. Included in these services are: stolen vehicle tracking, remote door unlocking, emergency roadside assistance, mapping capabilities, and directory information. These systems find location by GPS and then in conjunction with the service provider can establish two-way communication between the user and the service provider in the form of both data and voice. As with cellular phones, governmental and law enforcement agencies can request this information at any time.

***Keystroke Loggers***

Keystroke loggers are computer programs that record all keystrokes entered into the computer. Traditionally they have been used by employers to track the working habits of their employees, by parents who wish to monitor their children's Internet usage, and as a means of error detection in computer systems. The software can be installed both physically and remotely, and typically records additional information such as the program in which the keystrokes were entered as well as the time and date of the event. The government has taken advantage of this type of application. Because of the nature of the method, little is known concerning its development and deployment. The first public instance of its usage occurred in 2001 in the Supreme courts decision of *United States vs. Scarfo*. In this case the Federal Bureau of Investigation (FBI) gained access to the office of Nick Scarfo, a suspect and physically installed the software on his computer all without his knowledge. Of all the surveillance technology, keystroke loggers pose the most danger. Being that keystroke loggers are covert by nature, the monitoring of an individual can go on for an indefinite amount of time. Moreover, keystroke loggers record more information than just communications. Any information entered into the computer, not just what is transmitted to a third party is captured without knowledge of consent. This can have ramifications into what thoughts a person chooses to express, and with whom they wish to communicate with.

***Echelon***

Acknowledged as the world's most powerful tool for surveillance, Echelon is designed to intercept, analyze and dispense information. This is done through satellites that absorb every type of digital, wave-like communication in the atmosphere. From microwaves, fax transmissions, to cellular phone data it is all intercepted, filtered and sent to the base station that requested it. Echelon is run by several governmental agencies across the globe and is estimated to intercept up to 3 billion communications daily.

The National Security Agency (NSA) is the center for Echelon. Although much of the details concerning its design are secretive, Echelon in its most simple form mines data. The collected information is mined for key content through Echelon dictionaries. The content can be in the form of: phone/fax numbers, voice prints, and optical character recognition data. Each station has its own dictionary, maintained by a Dictionary Manager. This person has the only write access to the filters. Below are the satellites used to seize communications data.

| SATELLITE | NO. | ORBIT | MANUFACTURER | PURPOSE |
|---|---|---|---|---|
| Advanced KH-11 | 3 | 200 miles | Lockheed Martin | 5-inch resolution spy photographs |
| LaCrosse Radar Imaging | 2 | 200-400 miles | Lockheed Martin | 3 to 10 foot resolution spy photographs |
| Orion/Vortex | 3 | 22,300 miles | TRW | Telecom surveillance |
| Trumpet | 2 | 200-22,300 miles | Boeing | Surveillance of cellular phones |
| Parsae | 3 | 600 miles | TRW | Ocean surveillance |
| Satellite Data Systems | 2 | 200-22,300 miles | Hughes | Data Relay |
| Defense Support Program | 4+ | 22,300 miles | TRW/Aerojet | Missile early warning |
| Defense Meteorological Support Program | 2 | 500 miles | Lockheed Martin | Meteorology, nuclear blast detection |

Most often users supply information voluntarily when using the Internet. Several ways that is done include:

- Cookies – a block of text sent from the Website to the browser on a user's PC, where it is stored. Information that the cookie collects can be sent to the originating Website at a later time. Cookies enable customized interactions between a repeat visitor and Websites.
- Site Profiles – are sometimes required by websites to register users. They typically include contact information, demographic information, and possibly credit card information. They make it easier to match a user's history on a site with personally identifiable information.
- Web Bugs – small images, usually not visible. They allow the Website to eavesdrop on the user. When the user requests a page, a bug is activated and downloaded from the server. Bugs can also manage what additional websites a user has recently visited.
- ISP Monitoring – Internet Service Providers log and retain email and website traffic generated by their users. The USA PATRIOT Act allows government to obtain log information from ISP's without prior user permission or court order.

## BUSINESS

While Americans inadvertently provide information through Internet usage, registrations and warranties, the information is also being collected and resold in alternate forms without our explicit knowledge. The industry responsible for providing this type of information is data resellers. Data resellers collect purportedly non-personally identifiable information in order to gauge trends and for resell to businesses that may want to target certain markets.

Data sellers collect information in three forms:

- Public records – birth and death certificates, DMV records, civil case files, and property records
- Publicly available information – information typically not found in public records but available to the public: Internet websites, telephone directories, magazines or classified ads.

- Nonpublic information – product warranty information, information provided by businesses, etc.

***Information Resellers and Governmental Agencies***

One business that regularly buys information is the government. Recently these business affiliations have come under close scrutiny. The Government Accountability Office investigated several governmental agencies' use of reseller data. The organizations involved were: the Departments of Justice, Homeland Security, and State and the Social Security Administration. The report looked into the practices of these businesses to find out if the use of this personal data from resellers adhered and reflected best practices established by the Fair Information Practices, a set of widely accepted principles for protecting the privacy and security of personal data. The report also looked into the policies and practices of the involved agencies to determine whether they too were adhering to the Fair Information Practices once the information was collected.

Fair Information Practices

The Privacy Act of 1974 requires that the use of personal information be limited to predefined purposes and involve only information germane to those purposes. The provisions for the act are based on a set of principles for protecting privacy and security of personal information, known as the Fair Information Practices.

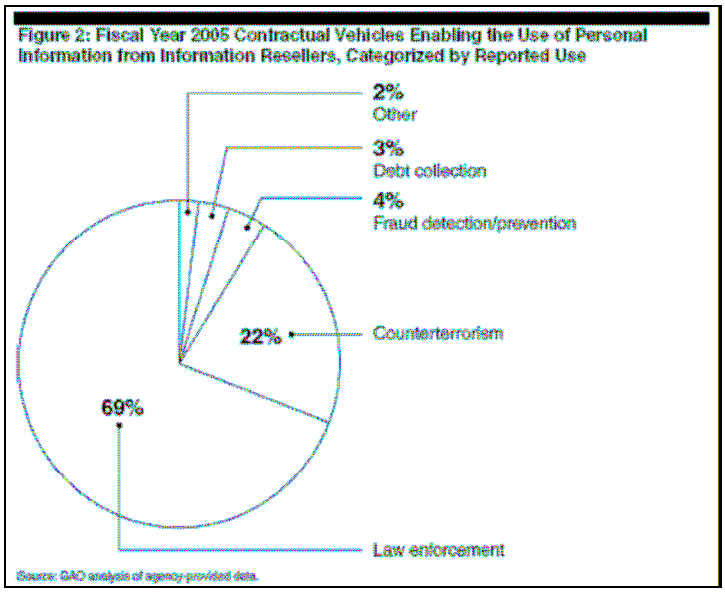
The principles are:

- Collection limitation – The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge and consent of the individual.
- Data quality – Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
- Purpose specification – The purposes for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to those purposes and compatible purposes.

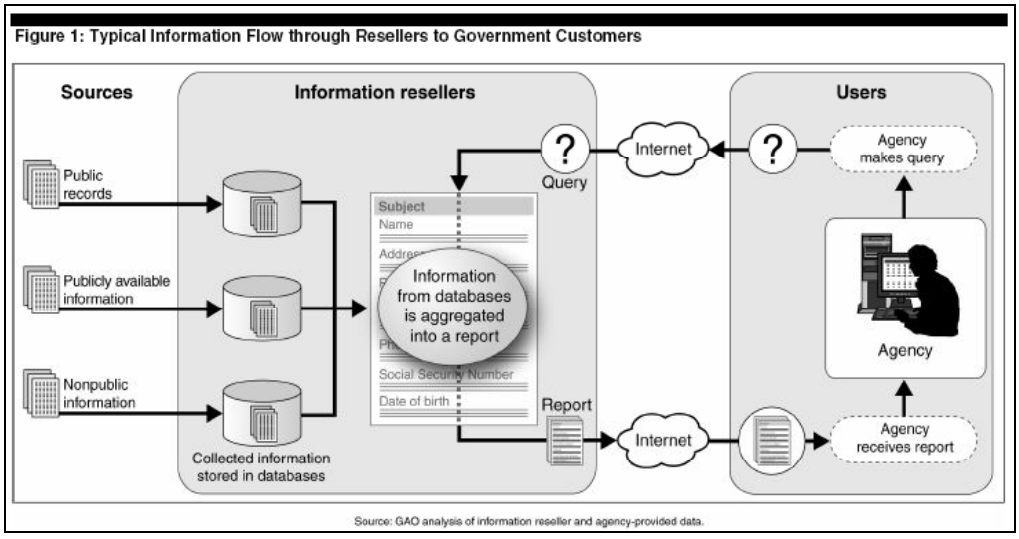
- Use limitation – Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
- Security safeguards – Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
- Openness – The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
- Individual participation – Individuals should have the following rights: to know about the collection of personal information, to request correction, and to challenge the denial of those rights.
- Accountability – Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

These practices are widely accepted and used by organizations in many countries including: Australia, Germany, New Zealand, and Sweden. The Organization for Economic Cooperation and Development (OECD), of which the US is apart adopted these practices in the 1980s.

In fiscal year 2005, governmental agencies reported that they used personal information obtained from resellers for a variety of purposes. These included criminal investigations, tracking down witnesses and fugitives, the detection of prescription drug fraud, and researching assets of subjects. Approximately $30 million was spent on contractual arrangements to enable the acquisition of such information. The break down was as follows: about 91 percent was for law enforcement (69 percent) or counter-terrorism (22 percent).




The data is stored in large data warehouses and is retrieved via queries processed through the Internet. In this manner, the involved agencies need not require physical warrants or subpoenas. Although there exist legislation against businesses that retain information, that legislation is not necessarily applicable for data retained in public warehouses.




The above figure depicts how information is collected, aggregated and sent in the form of reports to customers, including government agencies.

One major concern of consumers regarding privacy is how their information is handled when not under their control. GAO's report identified several problems related to

violations by governmental agencies in dealing with information obtained from data resellers. Their practices do not consistently reflect the fair information practices. The reports findings concluded that typically agencies policies and practices with regard to the principles of openness, purpose specification, and individual participation were uneven. This is attributed in part to the non-regulatory use of Privacy impact assessments (PIA) that were designed to ensure that the Fair Information Practices were being properly adhered to. Moreover, staff that had access to this information was not held liable for ensuring the appropriateness of accessing information. In summary, Fair Information Practices that were uneven between governmental agencies and data resellers were: *purpose specification* – records of governmental agencies lacked documentation noting the source of the information obtained, *openness* – policies were not established to specifically address the use of personal information, *individual participation* – because agencies neglected to divulge their information obtained from data resellers, individuals were not able to 'opt-out', and *accountability* – agencies do not monitor users usage of the data, they hold the user accountable for the information they view.

## GUEST SPEAKERS

An integral part of the course, Trustworthy Computing, was the component that included guest lectures. The lecturers came from various backgrounds and talked about varying aspects of Trustworthy computing. What these speakers added was a practical aspect to complement the material covered in the text and that outlined in the syllabus. Several speakers who influenced this project are: Mike Corn [Security and Information Privacy, UIUC], Thomas Kleyle [PriceWaterhouse Coopers], Dan Swartwood [Motorola], and Peter Siegel [CIO director, UIUC]. Below are synopsis of the speakers and their relevance to the topic of Privacy vs. Surveillance.

Speaker: Thomas Kleyle
From: PriceWaterhouse Coopers
Topic: Introduction to Privacy
Synopsis: Mr. Kleyle introduced the idea of privacy, and gave several defining features of privacy. These features included an individuals rights to: Control information

collected about them, Control how that information is used, Control who has access to the information, and the ability to have access their personal information.

Also covered were concerns raised by the events of 9/11. The tragedy has brought debate about the tradeoffs between liberty and security to a head. Topics of the lecture that influenced this project were:

- Concerns over terrorism, both foreign and domestic, and how their affects have begun to conflict with privacy needs.
- The fact that law enforcement is asking for broad new surveillance powers to monitor suspected terrorists.
- The introduction of new technologies that may infringe upon privacy rights of individuals.
- The fact that most Americans are unaware of the potential methods of surveillance.

Mr. Kleyle also addressed directly some of the probable methods of government surveillance including:

- Carnivore (DCS1000): email monitoring system
- Keystroke monitors: the Nicky Scarfo case
- Echelon

Questions that Mr. Kleyle proposed in his talk I attempt to address in this project:

- Do current privacy laws provide adequate protection in the face of new technologies?
- How does legislation deal with pen registers, trap & trace, roving wiretaps, and FISA

Speaker: Dan Swartwood, Motorola Privacy Protection Officer
From: Motorola
Topic: 21st Century Information Security: A Practitioner's Perspective

Synopsis: Mr. Swartwood's lecture addressed the role of technology in this privacy movement. His talked confronted the business of ubiquitous computing and its potential impact on privacy. Several highlighted topics of his talked centered on:

- Ubiquitous internet protocol-based technology,
- Almost everything connects to the net.
- Vulnerabilities are awaiting exploitation.
- Mobility of people, information, and devices

Speaker: Peter M. Siegel, CIO Director
From: University of Illinois Urbana-Champaign
Topic: Enterprise Information Security Issues: The Case of Higher Education
Synopsis: Mr. Siegel addressed several of the political movements made by legislation to enable the tracking of students.

## PROPOSALS

The topic of surveillance and privacy has been a very prevalent topic in the media recently. To address the growing concerns of Americans, several technological initiatives and organizations have been established so that those concerned have avenues to address their issues.

What has fueled the privacy debate is the fight against terrorism. Coupled with an information-based market, data analysis techniques to handle this information are proceeding without a suitable legal framework. There exist legal constraints on the usage of commercial data, but they are incomplete, and unresponsive to the current uses of data and terror prevention analysis.

Surveillance law has been surpassed by technology. Following legislative developments, one finds that the while the growth of technology has been exponential; the growth in law has been practically horizontal. A secondary problem is that case law and statues make a distinction between historical data and real-time data. The government is seeking to

extinguish that distinction in a way that would open communications to government access without probable cause.

***Development of surveillance law***

- 1967: Supreme Court extends Fourth Amendment to wiretapping and bugging.
- 1968: Congress adopts the Title III, the Federal Wiretap Act.
- 1986: Electronic Communications Privacy Act (ECPA) extends Title III rules to cell phones and email in transit; stored email accorded lower protection.
- 1994: CALEA imposes design mandates on telephone companies; creates intermediate standard for some customer data; bars use of pens/traps for location.
- 2001: PATRIOT Act clarifies reach of pen/trap law; lowers standard for pen/traps in intelligence cases.

***Search Warrant vs. Subpoena: Terms***

- Search warrant - is issued by a judge if she finds, based on a sworn affidavit submitted by a law enforcement officer, that there is probable cause to believe that a crime has been or is being committed and that the search will uncover evidence concerning the crime.
- Subpoena - is issued without judicial approval, by a prosecutor or law enforcement official (such as an FBI agent) that claims that the information sought is relevant to an ongoing investigation.

A search warrant permits immediate seizure. With a warrant, the government can come in and go through your files and/or confiscate computer. A subpoena directs the recipient to bring forth the desired material at a future date. This gives the recipient time to go through their records and make copies.

Subpoenas can be challenged in court. However, many service providers often have no incentive to defend the privacy of their customers, especially if they need never be notified that their data has been turned over to the government. In many cases, the recipient of subpoena can, but is not required, to disclose the subpoena to its customers.

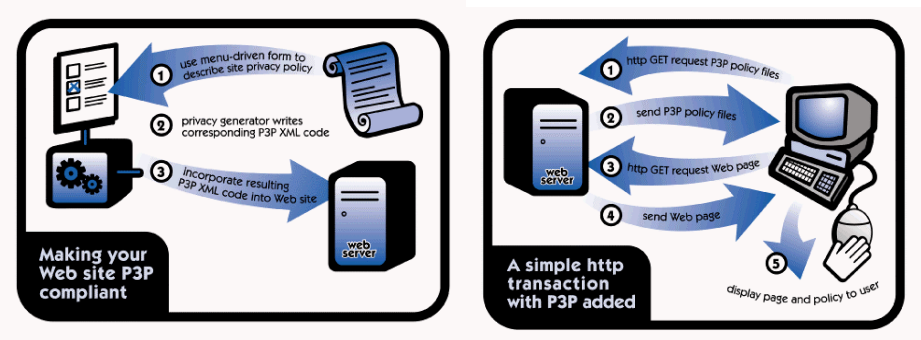
Probable cause is the highest standard for seizing evidence. It is also the standard for arresting someone or for bringing an indictment.

While designers and researchers are assessing the effectiveness of their applications, policymakers need to consider privacy and civil liberties associated with uses of data for combating terrorism. If the developers of information systems take privacy into account in the research phase, privacy protections can be built into applications. Taking this approach is more effective than trying to add on privacy protections after a project has been launched.

The most recent legislation to date to protect consumer information is the E-government Act of 2002. The E-Government Act of 2002 requires agencies to conduct privacy impact assessments (PIA). PIA's analyze how personal information is collected, stored, shared, and managed in a federal system. According to the E-Government Act, agencies must conduct PIAs (1) before developing or acquiring technology that "collects, maintains, or disseminates information that is in a personally identifiable form"; (2) "before initiating any new data collections involving personal information that will be collected, maintained, or disseminated using information technology if the same questions are asked of 10 or more people"; or (3) when a system change creates "new privacy risks", for example, by changing the use of personal information.

***Compliance Initiatives***

Several technological means have emerged to allow users to control what information their Internet browsers share. The platform for Privacy Preferences Project (P3P) is a standard that allows Websites to communicate their data privacy policies automatically to a Web browser when that Website is visited. A P3P-compliant browser can be programmed to interact with a Website in specific ways, depending on policies attributed to that Website. For example, it could reject any cookies from sites that do not have a policy that prohibits sharing of data with third parties. This technology has been built into both Internet Explorer and Netscape Navigator.




The figures above depict the communication between a users' computer and a P3P compliant website.

***Public Interests organizations***

The privacy vs. surveillance debate's growth has sparked the progress of special interest groups. Several of which are EPIC, CDT, and GAO.

One organization is the Electronic Information Privacy Center (www.epic.org). EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

A second organization is the Center for Democracy in Technology (www.cdt.org). The CDT was created in 1995 and is funded in part by companies including Google, Yahoo, AT &T, Verizon, HP and Microsoft. Its goal is "to promote democratic values and constitutional liberties in the digital age. With expertise in law, technology, and policy, CDT seeks practical solutions to enhance free expression and privacy in global communications technologies. CDT is dedicated to building consensus among all parties interested in the future of the Internet and other new communications media".

The government accountability office is an independent, nonpartisan agency that works for Congress. GAO is often called the "congressional watchdog" because it investigates how the federal government spends taxpayer dollars. GAO gathers information to help Congress determine how well executive branch agencies are doing their jobs.

# CONCLUSION

Individuals should be able to interact in modern society without losing control over their personal information. The modern right to privacy also entails, therefore, the right to control our personal information even after we disclose it to others.

Although there are strong laws to provide protection for communications in transit, the laws protecting the storage of communications are weak. The privacy and surveillance issues raise concern because of the inaccuracies, false positives, and possible misinterpretations or misuse of data. The consensus of the literature and surveys agrees that the government should be entitled to some data; however there should be in place a system of checks and balances. Individuals should be protected from fishing expeditions and government mistakes.

In addressing the conflict between terrorist activity and privacy one must first have the trust of the public. However, with mounting distrust from the public due to possibly covert government surveillance the government must assess what damage is possible to the national security goals.

The Internet and communications industry, users of technology, public interest organizations and the government need to communicate amongst each other to ensure fundamental rights of privacy and its protection in this the technological age.

## REFERENCES


- Dempsey, J. & Flint, L. "Commercial Data and National Security", 29 April 2006.
- Koontz, L., "Personal Information: Agencies and Resellers Vary in Providing Privacy Protections", 20 April 2006.
- Robinson, S., & Volonino, L., Principles & Practices of Information Security: Protecting Computers from Hackers & Lawyers, 21 April 2006.
- Schwartz, A., "Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology, Center for Democracy and Technology", 24 April 2006.
- Yancey, C. "ECHELON: The dangers of communication in the 21st century", 22 April 2006.
- URL: http://home.hiwaay.net/~pspoole/echelon.html (30 April 2006).
- URL: http://www.eff.org/Privacy/Surveillance/NSA/ (20 April 2006).
- URL: http://www.cdt.org/ (29 April 2006).
- URL: http://www.gao.gov/ (29 April 2006).
- URL: http://www.epic.org/ (29 April 2006).
- URL: http://www.cdt.org/publications/lawreview/1999nova.shtml (2 May 2006).
- URL: http://www.w3.org/P3P/ (29 April 2006).