How can the privacy rights of U.S. citizens be balanced against the government's need to secure its citizens and their information assets?

A primary responsibility of the United States government is to protect its citizens and resources against the threat of terrorism. Americans value their security and have, at times, sacrificed certain liberties to protect it. The bombings at Oklahoma City, during the 1996 Olympic Games in Atlanta, and at the World Trade Center in New York are reminders of our vulnerability to acts of violence. In spite of precautionary measures in place at the time of these incidents, injuries and deaths occurred. In an increasingly global society where individuals and materials move across transparent international borders, the government and its citizenry struggle to find the proper balance between security and civil liberties.

How much further should the government go to safeguard its citizens?

Some have proposed that foreign students studying the United States be monitored more closely. Identifying potential threats early would increase the likelihood of stopping terrorist attacks before they happen. Is it right to target foreign students for closer scrutiny? Would students from some countries be monitored more closely than students from others? What about US citizens whose parents were from those foreign countries? Profiling and discrimination would certainly play a role. Where would it stop?

What role does the information age play in terrorist activities and prevention?

Technological enhancements to the delivery of information and services have enhanced our lives, but at a cost. The very systems that we turn to for efficiency and convenience are vulnerable to cyber attacks and other acts of terrorism. Computer viruses are delivered by email; thieves harvest credit card numbers and other personal information; hackers bring down 911 systems. Additionally, there is growing concern over the government's ability to "snoop" into the private lives of its citizens, while it secretly gathers information for purposes of national security.

One example of the US government's electronic surveillance is the Federal Intrusion Detection Network (FidNet), proposed by the Clinton administration in 1999 as "…a computer security system for government computers with the ability to detect computer viruses, and intrusion by hackers or terrorists." (1) Once detected, these patterns of intrusion would be sent to a central monitoring site at the Federal Bureau of Investigation. After negative reaction over possible misuse of information collected, a new plan was submitted to Congress. This plan limited the information/data collected and analyzed. The new plan/proposal reflects the concerns of critics, balancing efforts to safeguard national security with the need for privacy.

Another example, this one international, is **ECHELON**. The ACLU's *echelonwatch* describes **ECHELON** as "the most powerful intelligence gathering organization in the world." It "is the term used for an automated global interception and relay system operated by the intelligence agencies in five nations: the United States, the United Kingdom, Canada, Australia and New Zealand. It is believed that **ECHELON** is the code name for the portion of the system that intercepts satellite-based communications. The U.S. National Security Agency (NSA) takes the lead in working with other intelligence agencies of the other nations." (2) **ECHELON** serves as an example of the tenuous balance between civil liberties and the government's efforts to protect its assets and citizens. A powerful intelligence-gathering tool such as **ECHELON** can provide key information to help the government stop terrorism, cybercrime, and security breaches. On the other hand, it can also be used to violate the privacy rights and civil liberties of individual citizens. Are we comfortable with a secret intelligence-gathering tool that intercepts information communications and is controlled and monitored by the government?

How much personal information do these eavesdropping initiatives acquire from innocent citizens? Is the information used merely to protect against terrorist attack? How much is our privacy invaded and who can get access to the information? There have been numerous reports of attempts to access federal computer systems. If the US government keeps a central repository of information about each citizen, would that information be especially attractive (and vulnerable) to hackers? Would the information the US government has gathered on its citizens be open to inspection by the public due to the Freedom of Information Act? Would the government under any circumstances *sell* information it acquires to interested parties? For example, marketers of various products and services may pay a great deal to learn the habits of potential consumers. Would the information be used in place of voluntary polls to gauge citizen reaction to potential policies and legislation, thus influencing the course of government itself?

The debate continues as we attempt to balance issues of national security and the public's right to liberty and privacy. There are many concerns over how the government acquires its information, how it safeguards it and what it does with it. Yet, the threat to people, property and commerce is substantial. In such an atmosphere of risk and uncertainty, it is clear the U.S. government must move to improve its security measures. However, the question remains, in what manner and how strongly should the government act?

Questions for Discussion:

1. Commerce Secretary Daley has stated, “We’ve spent a great deal of time working on privacy and consumer protection concerns, but…an even more basic concern to consumers is the issue of security.” Not only government computers, but critical infrastructure computers, many of them private sector, such as the banking & finance computers that manage bank and credit card accounts, have come under increasing attack. It is no longer a question of protecting ourselves against foreign spies but against hackers and criminals stealing our money electronically. Do desperate times call for desperate measures? Should the government err on the side of consumer privacy or consumer security?

2. For the following scenarios, discuss whether this represents acceptable government or industry surveillance and intervention, as well as any rights being violated and any remedies or protections you feel the citizen(s) involved should have.

A. A computer science student prepares a research paper on how easy it is to penetrate ATM machines and steal passwords and accounts. He includes some sample code to accomplish this penetration. He posts this research paper on his personal web page, where it is discovered by a government knowbot that trolls the Internet for such information. The website, which includes personal information, including a name, address and the student’s plans for graduate school, is documented, indexed and stored electronically on a government computer system.

B. A man is arrested for bombing an abortion clinic, resulting in the deaths of a doctor, a nurse and three patients. He is a former member of an active abortion protest group. He claims in interrogation to have quit the group but criminal investigation determines that he maintains close contacts with the group. The group has never been associated with violent activity; although they protest actively at clinics across the nation. An FBI agent infiltrates a closed discussion list belonging to the group by spoofing the email address of another former member.

C. You attempt to access your VISA account at a strange ATM machine but you have forgotten your account and PIN number. You know you are just one or two numbers off, and you really need the cash, so you keep trying, over and over. Your multiple trials are registered and forwarded to a computer system jointly managed by government and industry, which in turn alerts the bank issuing your card. The bank contacts you about possible misuse of your card. You are impressed with their efficiency in safeguarding your account. The apparent “brute force” attack on your VISA account is stored, along with complete account information, for one year. If there are no more “attacks” on your account in that time, the information will be deleted from the server.