Global Information Assurance Certification Paper

Sharon Pelaccio
Date 09/10/2002

Enforcing Privacy in an era of Heightened National Security: Dilemma of an Information Security Practitioner

Abstract

United States Security practitioners are entrusted with the ethical responsibility of ensuring the confidentiality, integrity, and availability of information. When it comes to ensuring privacy, they rely on the mandates of the constitution and its Fourth Amendment. In light of what happened on September 11 and the government's aggressive proactive national security agenda, however, security practitioners have to cooperate by acknowledging the fact that the FBI and CIA are using tools to monitor Internet exchanges of information between citizens. This paper attempts tracing the development of the government monitoring tools and the ensuing ethical dilemma of enforcing privacy in an era of heightened national security for the security practitioner.

Introduction

Is there a need to protect the American public from harm in this land of peace and tranquility? Of course, there is. A prudent government has the responsibility of protecting the life and property of its citizens from natural or man-caused disasters. Not only it should have a disaster recovery plan, but also must deploy national security controls to proactively prevent disasters like the September 11 terrorist attacks from ever happening again. After September 11's rude awakening, the United States Government is not taking any chances—it has taken several measures including establishing a cabinet-level Homeland Security Department.

When evaluating the certainty of the international terrorist threat and the vulnerability of the United States, the risk of September 11 repeating itself is extremely high. Because of the Afghan war, the all-time high anti-American sentiment among fanatic Muslims and other sympathizers is even higher posing a serious threat against mainland United States or US interests abroad. All four boarders of the United States are full of loopholes for terrorist intruders. The thousands of nuclear facilities, dams, bridges, and other public installations are easy targets for determined attackers. Even among the population, remnants of terrorist groups and new converts pose a huge physical and logical security problem that would deplete US resources—the richest nation on the globe. One of the ways of mitigating the terrorist risk is to proactively monitor the exchange of messages over the telephone, the mail, or the global Internet.

Though the national security risk is high, the United States is a nation of laws—laws that proclaim and protect the sanctity of personal freedom, the pursuit of happiness and

individual privacy. It is a constitutional mandate that neither Congress shall pass laws that curtail the enjoyment of personal freedom, the pursuit of happiness, or invade a person's privacy; nor shall the government conduct covert or overt actions that trespass the freedom and privacy of a person. To what extent is this true—even at the cost of national security? How can the dichotomy be reconciled so that the US can have "its pie and eat it, too?"

Post-September 11 US National Security Awareness

September 11 was a tragic day, and also a rude wake-up call that proved how porous our borders are, how lax our security controls are, and how hard the government needs to work to protect its citizens. While overt security controls are in place at airports, our borders, and other key security points, the government has embarked upon several covert-monitoring operations—the major one being Internet message monitoring.

The Private Internet

Though it has its origins in Federal computing institutions, it has been quite a long time since the private sector embraced, nurtured, and enhanced the Internet to be a truly private and free means of communication. There have been no rules and no limits in the global Internet. It has evolved into the "Wild West" of technology where the experts, the novice, the hacker, and cracker equally have their say and their day. One enters the world of the Internet at his/her own peril. Except for voluntary gentleman/gentlewoman etiquette, there are no rules on the Internet.

Nowadays, though, the noose is tightening—legislation has been passed that holds hackers and other lawless Internet players accountable for their malicious actions. Organizations are also required to shape up and protect private information of their customers from the prying eyes of intruders. Such laws as the Health Insurance Portability and Accountability Act (HIPAA) have brought in sweeping changes in protecting the privacy of patients. On the other hand, other regulations seem to be giving the government a free hand to invade the privacy of citizens.

The USA Patriot's Act and Internet Privacy

The most compelling regulation enforced since September 11 is the USA Patriot Act, which was signed into law on October 26, 2001. This law has many provisions; several, which are significant provisions that may impact privacy.

One provision of the Act can force a judge to issue a court order for recording the addresses to which a suspect sends messages, and from where the suspect gets messages from, that is if a prosecutor files papers certifying that e-mail is relevant to an investigation. Privacy advocates argue the law is far too open to interpretation of the relevancy of what constitutes an investigation. David Sobel, general counsel to the Electronic Privacy Information Center in Washington asked, "What is relevant, anything could be relevant." [1]

The USA PATRIOT Act contains other provisions that significantly diminish the Fourth Amendment guarantees. For example, the "sneak and peek searches" provision. The legislation allows law enforcement authorities to enter a home, office, or other private place and conduct a search, take photographs, and download computer files without notifying the person whose property is being searched until sometime after the search was conducted. This authority is not limited to anti-terrorism investigations but also extends to criminal ones. The justification law enforcement needs in order to enter without notice, is that the notice might seriously jeopardize an investigation or unduly delay a trial. This clause is adopted from existing law (18 USC 2705). [2]

Unlike many parts of the USA Patriot Act, these searches are not subject to the Sunset clause, which requires Congress to examine in four years whether the new Acts policy on American liberties have exceeded their authority or effectiveness. Congress has scheduled some, but not all procedures to the sunset clause, to expire on December 31, 2005. Congress has exempted from the USA Patriot Act any Sunset clause that states: "Foreign intelligence investigations that initiated before the Sunset date, or offenses that began or occurred before the sunset date." USA PATRIOT Act § 224. [3]

The USA Patriot Act is complex and powerful; it broadens the definition of terrorism, and increases the penalties for terrorism activity. The Act brings forward new surveillance tools that will create a range wide enough that e-mail, text chat, or Internet search inquiry can be subject to judicial action. Additionally, this law also increases cooperation within law enforcement and intelligence agencies to share information, become more involved in security, and more involved in oversight issues. Some of the more sweeping changes involve electronic surveillance on the Internet, which means there could be even less guarantee of privacy on the Internet.

Government Projects for Internet Monitoring

In recent years, both the FBI and CIA have invested heavily on Internet monitoring projects that would allow them to gather, filter, and siphon e-mail and other transactions over the Internet for analysis of any possible terrorist communications. The passing of the US Patriot Act will provide law enforcement and government intelligence agencies with more flexibility, and greater access to high-tech tools that includes: interception of e-mail messages, and the monitoring of Internet activity.

In order for US government agencies to thwart criminals and terrorists who may be plotting flagitious activity using computers, and the Internet, the FBI project Cyber-Knight, which is a spin off of Carnivore, is developing a tool called the Magic Lantern.

The CIA on the other hand is still functioning a nonprofit venture for the past three years with In-Q-Tel, located in Menlo Park and Arlington, Virginia. In-Q-Tel, in its effort to deliver cutting edge capabilities to the CIA, plans to introduce Inktomi Enterprise Search as a targeted search solution supporting multiple languages for its government clients, thus enabling them to more efficiently locate and access relevant information. Though

purpose of both efforts is to monitor, gather, and filter Internet transactions, their architecture, deployment, and functions, are not the same.

FBI's Magic Lantern

When rumors of Magic Lantern were first perceived, the Federal Bureau of Investigation (FBI) strongly denied that such a plan existed. Today the FBI unconditionally admits that they have devised a scheme called Magic Lantern in an effort to combat terrorism and future terrorist attacks. Magic Lantern is a plan by which the FBI by design infects computers with a virus or Trojan horse. This effort is intended to compromise a suspect's computer so that valuable information that can be used as evidence can be gleaned. This information was originally reported by MSNBC. [4]

Magic Lantern is an improved version of Carnivore; a software program designed to monitor secure encrypted email over the Internet. The FBI released a series of unclassified documents relating to Carnivore last year in response to a Freedom of Information Act request filed by the Electronic Privacy Information Center. The sections of documentation were heavily edited – blacked out. The documents included a document describing the "Enhanced Carnivore Project Plan," which was almost completely blacked out. [5] The edited portions of that memo mention Cyber Knight, which is described as a database that sorts and matches data gathered using various methods, like keystroking, which can match the files with the encryption keys.

The Magic Lantern effort resolves an important problem with the FBI's existing computer monitoring technology – the key logger system. Before Magic Lantern, using Carnivore alone destined investigators to break into a suspect's residence with a warrant and physically attach a device to a computer. Magic Lantern, however, can be installed over the Internet by misleading a person into opening an email attachment. Once the program is completely installed, it tries to hide itself on the task list by not showing any icon or indication that it is running. The entity controlling the computer uses a program that records keystrokes, copy email, and files.

The Magic Lantern program does not try to decrypt e-mail. Instead it records the characters as they are typed. With the collected information, the FBI can obtain a suspect's password and then the suspect's encryption key. The objective of using Magic Lantern is to catch the passphrase of an otherwise non-crackable cipher from a suspect's system.

Based on media reports, Magic Lantern is a Trojan program. Keylogger Trojans log all of your keystrokes (including passwords), and then either save them on a file or Email them to the attacker occasionally. Keyloggers usually do not use much disk space and can masquerade as important utilities, thus making them very hard to detect. Some keyloggers can also highlight passwords found in text boxes with titles such as 'enter password' or just the word password somewhere within the title text. [6]

CIA and In-Q-Tel

Since September 11, the Central Intelligence Agency (CIA) has also been particularly active in developing software that can dig deep within the Internet to harvest information. The CIA relies on its wholly owned and operated company In-Q-Tel, to fund research and development Internet probing software. In-Q-Tel is a private, independent, enterprise funded by the CIA. Launched in 1999, In-Q-Tel's mission is to identify and invest in companies developing cutting-edge information technologies that serve United States national security interests. Working from an evolving strategic blueprint that defines the CIA's critical information technology needs, In-Q-Tel engages with entrepreneurs, established companies, researchers and venture capitalists to deliver technologies that pay out in superior intelligence capabilities for the CIA and the larger Intelligence Community. The CIA is planning to spend $38 billion in a vital restructuring for homeland security and defense. [7]

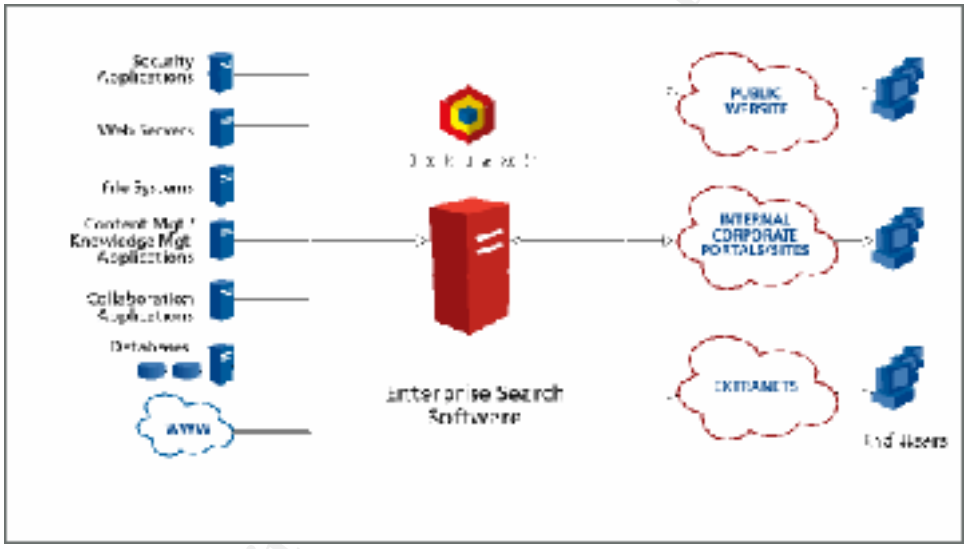

Figure 1: In-Q-Tel Security Architecture [9]

In-Q-Tel, delivers cutting edge capabilities to the CIA, and has plans to introduce Inktomis' "Enterprise Search" as a targeted search solution supporting multiple languages, which will enable the intelligence agency to more efficiently locate and access relevant information. "Leading edge search and retrieval technology is a top priority for In-Q-Tel because it is critical for accessing the vast amount of data available today, quickly and efficiently," said Gilman Louie, president and CEO, In-Q-Tel. "Inktomi has some of the most powerful enterprise intelligence tools in the commercial market. After a thorough evaluation, we selected Inktomi Enterprise Search for our government clients because its customizability and highly relevant multilingual search capabilities have the potential to deliver valuable improvements in open source information gathering." [8]

RISSNET

Law enforcement agencies like the FBI and the CIA have at their disposal a substantial information-sharing network through which federal, state, local, and foreign police agencies can exchange information on groups felt to pose a threat. The RISSNET and LEO systems have been in use since before the September 11, although information was not shared with all law enforcement agencies, since some of the information was controlled by government intelligence agencies.

The system, RISSNET, or Regional Information Sharing System Network, existed before the September 11 attacks, and has been in use by all law enforcement agencies. RISSNET is a secure intranet that connects 5,700 law enforcement agencies in all 50 states, including Ontario, Quebec, the District of Columbia, Guam, the U.S. Virgin Islands, Puerto Rico, and Australia. The information gathered using RISSNET is archived by MAGLOCLEN (Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network). There are other regional archives around the country, but MAGLOCLEN nerve center headquarters in Newtown, Pennsylvania, distributes political intelligence to all police departments, and intelligence agencies that are connected to RISSNET. [10]

LEO

The FBI runs its own intranet communication called Law Enforcement On-line or "LEO", which allows it to communicate intelligence with select other law enforcement agencies. [11]. LEO provides a state-of-the-art communication mechanism to link all levels of law enforcement, serving as a vehicle to educate law enforcement personnel on the best technologies and practices.

Another form of communication on LEO is CHAT. This type of real-time online communication gives users the capability to join group discussions pertaining to specific law enforcement topics or have group meetings themselves. Using CHAT eliminates travel time to meetings and saves on the costs associated with traveling. LEO offers a feature called the Electronic Academy that provides hosted sessions with experts representing various disciplines within the law enforcement profession.

The calendar feature on LEO is an effective way of notifying users of upcoming seminars, conferences, training, or related meetings throughout the nation by posting events in the National Calendar or by particular state organizations using the State Calendar. This feature includes the dates of the event, point-of-contact, phone numbers, location, hotel accommodations, and many other features.

In the aftermath of September 11, the FBI is under pressure to open up LEO to more police agencies so they can have access to more real-time intelligence. Consequently, the FBI and CIA require secure sharable information, intelligence, and technology in order to combat terrorism.

Fourth Amendment Concerns

The ability to easily communicate with loved ones and co-workers, whether it is across the street or across the nation, is one of the best things about the Internet and e-mail. Moms in Madison County type e-mails to family members in Columbus or California when the kids are asleep. Salespeople send hundreds of e-mails in the course of a day in order to take care of business. Community groups organize volumes of volunteers with a few strikes on the keyboard. The options are plentiful. The freedom and privacy that accompany this technology should be too.

The right to privacy is one of the most important rights we enjoy as citizens of the United States. Assaults on our privacy may come from many directions such as aggressive marketers or computer criminals, but one would hope that the government is not part of that contemptible group.

At issue is the fundamental right under the Fourth Amendment, which grants United States citizens' prior notice when the government conducts a search and seizure. The Fourth Amendment of the US Constitution states:

> "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." [12]

The "Search and Seizure" provisions of the Fourth Amendment are all about privacy. Most people instinctively understand the concept of privacy. Is the freedom to decide which details of your life will be revealed to the public, and which will be revealed only to those you care to share them with. To honor this freedom, the Fourth Amendment protects against "unreasonable" searches and seizures by state or federal law enforcement authorities.

The flip side is that the Fourth Amendment does permit searches and seizures that are considered reasonable. In practice, this means that the police may override privacy concerns and conduct a search of your home, barn, car, boat, office, personal or business documents, bank account records, trash barrel or whatever, if:

- The police have probable cause to believe they can find evidence that you committed a crime, and a judge issues a search warrant, or
- The particular circumstances justify the search without a warrant first being issued.

Considering that today many people maintain their papers and effects on their computer hard drives, the expansion of pen register authority to include electronic communications and Internet usage can mean the collection of information more private than IP addresses, which are roughly the equivalent of phone numbers. The Government contends that it will concentrate its surveillance only on the target of the investigation, but in reality all conversations, including those conducted by third parties, will be wiretapped.

To use one example, if the government suspects that a particular target uses different pay phones at an airport, then the government would have the power to wire all the public telephones at that airport and the discretion to decide which conversations to monitor.

It is often said that ours is a government of laws, not those who inhabit high office at any given moment. Americans may trust or admire such individuals, but their enduring faith is reserved for certain fundamental legal principles and traditions that emanate from our Constitution. That the federal government is one of limited, enumerated powers; the Congress makes the law, the President executes the law, and the judiciary interprets the law; that criminal suspects are innocent until proven guilty and entitled to various procedural protections during the process of adjudicating guilt. Many of the new powers assumed by the President and his officers since September 11 run counter to these principles.

One reason for concern is that the new powers, especially many of the investigative tools in the USA PATRIOT Act, are not limited to the pursuit of terrorists. Even those that are reserved for terrorism investigations may be used in contexts that the drafters of the Act never contemplated. The label "terrorism" is notoriously elastic: it has recently come to light that the Department of Justice categorizes as "terrorism" such garden variety crimes as erratic behavior by people with mental illness, passengers getting drunk on airplanes, and convicts rioting to get better prison food.

Another reason for concern is that for months civil libertarians have warned that Americans' constitutional rights are being sacrificed in the name of the post-Sept. 11 push for improved national security. Now, a broad array of rights activists are attacking a Bush administration plan they claim would prod postal workers, utility employees, and others to spy on their fellow citizens.

The plan is called "Operation TIPS" (Terrorism Information and Prevention System) [13] and is administered by the U.S. Department of Justice, and developed in partnership with several other federal agencies. In addition it is one of the five component programs of the Citizen Corps. Operation TIPS will be a national system for reporting suspicious, and potentially terrorist-related activity. The program will involve the millions of American workers who, in the daily course of their work, are in a unique position to see potentially unusual or suspicious activity in public places.

The Justice Department appears to be backing away from earlier, more aggressive and detailed descriptions of Operation TIPS, but groups such as the American Civil Liberties Union [14] and the National Lawyers Guild [15] claim the information-gathering initiative still represents a potential threat to Americans' civil rights.

Can the Dichotomy be Reconciled?

Privacy mandates proscribed by the constitution and its Fourth Amendment are being enforced to ensure citizens' privacy is protected. In addition to the Fourth Amendment privacy rights, Congress has enacted the HIPAA to ensure patients' medical information is kept with the strictest confidence, and to encourage patients to discuss their medical problems openly with their health practitioners. Because of the advent of Tele-medicine, medical doctors use the Internet in diagnosing patient's ailments remotely. In the presence of the FBI and CIA Internet monitoring tools, however, the purposes of HIPAA seem to be compromised. In addition, the proposed Operation TIPS initiative is now another in a series of questionable homeland security measures. How can the goals of privacy and national security be reconciled? What ethical standard should an information security practitioner apply to reconcile the dichotomy of privacy and national security?

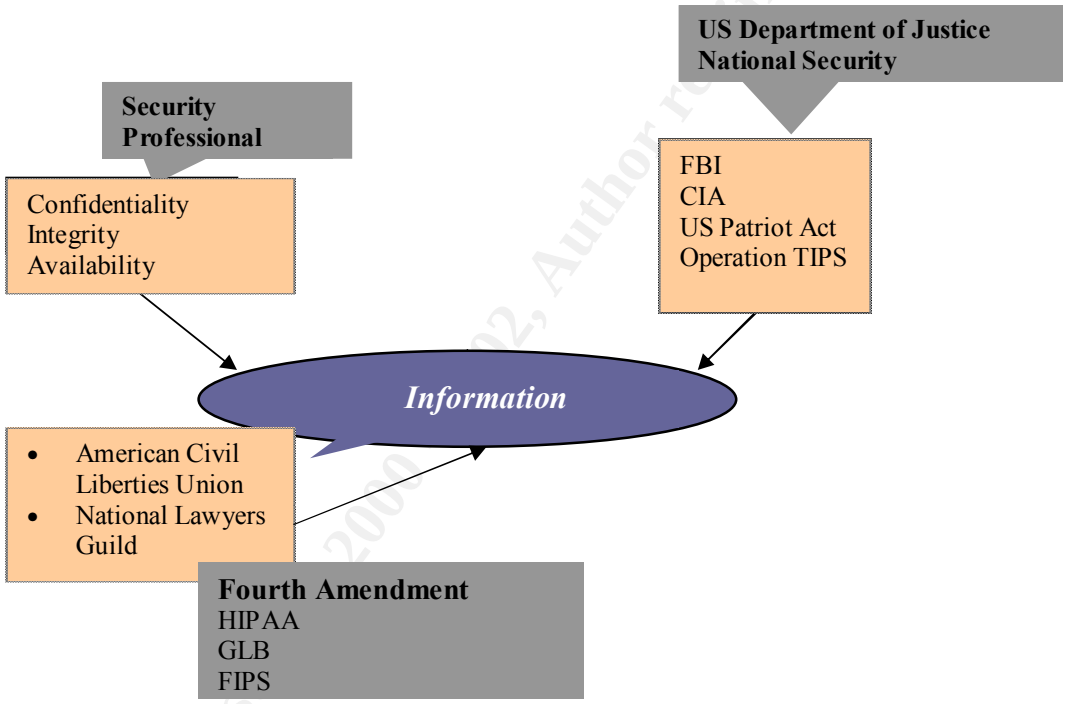

Figure 2: The Dichotomy: National Security vs. Citizens' Privacy

The security practitioner has the professional responsibility of ensuring the confidentiality, integrity, and availability of information assets he/she is entrusted to safeguard. This responsibility throws a heavy ethical burden of allowing government scrutiny in the guise of national security on one hand, and observing professional, constitutional, and regulatory mandates of ensuring privacy of information on the other. As a citizen-practitioner it is the national duty of the security practitioner to help and cooperate with all efforts intended to secure the nation. This is possible only if the practitioner maintains a "cool head" that will allow him/her to walk the fine line of national security and privacy demands. Though a tough job to do, it is the only best way to reconcile the dichotomy.

Conclusion

On September 11, 2001 thousands of people lost their lives in a brutal assault on the American people. This tragedy requires all Americans to examine carefully the steps our country may now take to reduce the risk of future terrorist attacks. We need to consider proposals calmly and deliberately with a determination not to erode the liberties and freedoms that are at the core of the American way of life. We need to ensure that actions by our government uphold the principles of a democratic society, and international law, and that all decisions are taken in a manner consistent with the Constitution. We can, as we have in the past, in times of war and of peace, reconcile the requirements of security with the demands of liberty.

The coordination and information sharing contemplated by the USA Patriot Act between elements of the intelligence community, including the CIA and the FBI, appears to be consistent with existing law governing the activities of law enforcement and the intelligence community. In addition, although the method by which government officials conduct surveillance and gather information has significant implications on civil liberties, the simple sharing of information between two elements of the intelligence community, or between the intelligence community and the law enforcement community, does not necessarily compromise civil liberties.

In the end, the dichotomy may be reconciled by focusing attention principally on the techniques by which intelligence is gathered domestically, and not on whether other members of the intelligence community are permitted to view the intelligence gathered.

References

1. Port, Bob, "USA: FBI Software Records Each Keystroke", Seattle Times, December 18, 2001. http://www.corpwatch.org/news/PND.jsp?articleid=1092

2. LII, Legal Information Institute, US Code Collection TITLE 18, Part I, CHAPTER 121, Sec.2705, "Delayed Notice", Cornell Law School, Updated September 9, 2002. http://www4.law.cornell.edu/uscode/18/2705.html

3. THOMAS World Wide Web system, Federal Legislative Information Library, Updated September 01, 2002. http://www.ratical.org/ratville/CAH/Section224.html

4. Sullivan, Bob, "Magic Lantern' part of new 'Enhanced Carnivore Project", FBI software cracks encryption wall, MSNBC, August 20, 2001. http://www.msnbc.com/news/660096.asp#BODY

5. Electronic Privacy Information Center, "Questions about Enhanced Carnivore", November 16, 2000. http://www.epic.org/privacy/carnivore/carnivorequestions.html

6. Middleton, James, "FBI runs Trojan horse", vnunet.com UK technology news, November 21, 2001. http://www.vnunet.com/News/1127038

7. Internetnews.com, "In-Q-Tel Sounds Call to 'IT Warriors", INT Media Group, Inc., June 27, 2002. http://www.internetnews.com/ent-news/print.php/1378061

8. Singer, Michael, "CIA Taps Inktomi for Government Work, INT Media Group, Inc., April 24, 2002. http://siliconvalley.internet.com/news/article.php/3531_1015521

9. Yang, Jack, "INKTOMI ENTERPRISE SEARCH 4.5", Inktomi Corporation Home Page, 1996-2002. http://www.inktomi.com/products/search/enterprise.html

10. Gallagher, James R., "RISS PROJECTS: Their Impact On Analysis Over The Last Decade", Open Source Publishing, Incorporated, Originally appearing in the IALEIA Journal, September 1996. http://www.osint.org/osq/v1n3/riss.htm

11. Frank, Diane, Web links law enforcement nets, FCW.com Your Government IT Resource, August 20, 2002. http://www.fcw.com/geb/articles/2002/0819/web-leo-08-20-02.asp

12. FindLaw for Legal Professionals, "U.S. Constitution: Fourth Amendment – Search and Seizure", Copyright 1994-2002. http://caselaw.lp.findlaw.com/data/constitution/amendment04/

13. National Crime Prevention Council, Federal Emergency Management Agency. Updated July 20, 2002. http://www.citizencorps.gov/tips.html

14. American Civil Liberties Union Freedom Network, "Stop the Government from Turning Neighbor Against Neighbor!" Last updated July 24, 2002. http://www.aclu.org/action/tips107.html

15. Bauduy, Jennifer, "The Spy Who Reads Your Meter", Ashcroft's Plan To Turn your Neighbors into Snoops, Editor at TomPaine.com, Published August 26, 2002. http://www.tompaine.com/feature.cfm/ID/6027