WASHINGTON, DC -- Recent moves to beef up intelligence gathering in the wake of the September 11th terrorist attacks have civil libertarians concerned that law enforcement agencies will entangle many law abiding citizens and social justice groups in their surveillance missions. Intelligence networks are setting their sights on the Internet, which up to now has had no clear privacy guidelines. Under the provisions of the inaptly named anti-terrorism act, "USA-PATRIOT," the Federal Bureau of Investigation (FBI), National Security Agency (NSA), Central Intelligence Agency (CIA), and a number of other smaller law enforcement agencies are looking for ways to monitor the Internet and mine useful intelligence from it. And new technology makes it easier than ever to spy on the Internet.

Although law enforcement and intelligence agencies claim they are merely looking for information to counter future acts of terrorism, the definition of "terrorism" is being expanded to cover non-violent groups that have traditionally used the Internet to marshal resistance to corporate-inspired globalization. Politicians are already painting dissent as "unpatriotic" and therefore somehow linked to terrorism.

Meanwhile, a phalanx of software companies, consultants, and defense contractors stand to reap billions of dollars over the next few years by selling surveillance and information-gathering systems to government agencies and the private sector.

Technology Already in the Hands of Law Enforcement

Law enforcement agencies like the FBI already have at their disposal a massive information sharing network through which federal, state, local, and foreign police forces can exchange information on groups felt to pose a threat. The system, RISSNET, or Regional Information Sharing System Network, which existed before the September 11th attacks, recently got a boost when Congress authorized additional money for it in the USA PATRIOT Act.

RISSNET is a secure intranet that connects 5,700 law enforcement agencies in all 50 states, as well as agencies in Ontario and Quebec, the District of Columbia, Guam, the U.S. Virgin Islands, Puerto Rico, and Australia. According to sources close to the Washington Metropolitan Police, data on targeted local groups such as the Alliance for Global Justice, the anti-World Bank/International Monetary Fund activist organization, has been shared with other jurisdictions through RISSNET.
RISSNET has also been used to coordinate the monitoring of the activities of anti-globalization protestors in Seattle, Quebec City, Philadelphia, Los Angeles, Washington DC and Genoa. For example, when the FBI seized network server logs from Independent Media Center (IMC) in Seattle during the April 2001 anti-free trade protests in Quebec City, RISSNET was used to coordinate activities across jurisdictional boundaries. The IMC, founded during the 1999 WTO protests, allows activists and independent journalists to post directly to its site.

State and metropolitan police intelligence units also monitor the web sites of activist organizations in their jurisdictions. All RISS intelligence is archived by an Orwellian-sounding entity called MAGLOCLEN or "Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network." There are other regional RISS intelligence centers around the country with equally mysterious acronyms. MAGLOCLEN, a nerve center headquartered in Newtown, Pennsylvania, distributes political intelligence to all police departments hooked up to RISSNET.

MAGLOCLEN allows police investigators to link various activist groups and members through the Link Association Analysis sub-system, a relational database that identifies the "friends and families" of groups and individuals. The Telephone Record Analysis sub-system can call up records of phone calls of targeted groups and individuals. A suspect group's banking and other commercial data can be monitored by the Financial Analysis sub-system. And through a system that would have been the envy of J. Edgar Hoover, police and federal agents can also call up profiles that provide specific information on the composition of organizations, including their membership lists. The Justice Department has instituted a project called RISSNET II, which directly links the individual databases contained within the various RISS centers.

The FBI also runs its own intranet called Law Enforcement On-line or "LEO," which allows it to communicate intelligence with select other law enforcement agencies. In the aftermath of September 11th, the FBI is under pressure to open up LEO to more police agencies so they can have access to more real-time intelligence. If Attorney General John Ashcroft lifts restrictions placed on the FBI's collection of political intelligence, undoubtedly information on the First Amendment activities of American citizens will wind up in the Bureau's computer databases.

"There has been no indication that the FBI needs expanded spying powers," says Center for Constitutional Rights attorney Michael Ratner. "We should learn from history; spying on dissent is not only unlawful but it is abusive."

This kind of surveillance is not new. In the 1960s and 70s, the FBI's Counter Intelligence Program, known as COINTELPRO, was used to gather personal details on the lives and habits of a wide array of activists ranging from public figures like Dr. Martin Luther King, Jr., actress Jane Fonda and noted pediatrician Benjamin Spock, to members of local anti-war and civil rights groups. This information was often used to disrupt lawful organizing and protest activities.

A modern-day FBI list might include any group deemed "terrorist" by any law enforcement agencies, the military, or criminal prosecutors. That could subject organizations as varied -- and unconnected to terrorism -- as Earth First, Greenpeace, the American Indian Movement, the Zapatista National Liberation Front, ACT UP, and their supporters to a wide array of high-tech surveillance and eavesdropping tools.

Chief among spy agency tools is an e-mail sniffing program known as
Carnivore. Changes brought about by USA-PATRIOT allow federal law enforcement officials to petition a secretive federal court called the Foreign Intelligence Surveillance Court for warrants to tap phones, read e-mail, or break and enter into homes or offices to conduct searches and plant bugging devices. These spy activities can be carried out without proof that an organization has links to terrorists or foreign intelligence agencies.

To read e-mail the FBI can order an Internet Service Provider to place a special monitoring computer called Carnivore (now renamed Data Collection System 1000) on its network servers. The FBI can then select the e-mail of surveillance targets for capture and storage. Not content with this device, the FBI now seeks to expand its surveillance capability to the entire Internet.

Making a Buck off of Government Spying

Companies that are positioning themselves to help the government surveill the web came out in force at a recent Homeland Security Conference in Washington. They included Oracle, Microsoft, Information Builders, Choice Point, Man Tech, AMS, and Booz Allen & Hamilton. Government speakers from civilian and military agencies all stressed that they urgently need the technology to store surveillance-derived intelligence and exchange it with other agencies. If these corporations step up to the plate on developing new surveillance, monitoring, and biometric ID systems, they stand to make billions.

Companies like Top Layer Networks, Inc. of Westboro, Massachusetts, are developing ways for the FBI to install surveillance systems at a few key Internet hubs which would allow federal agents to remotely flip a switch and pound a few keys to begin monitoring the e-mail or web-based mail of any targeted group or individual. According to chief Top Layer engineer Ken Georgiades, the firm is working with a number of partners to develop new standards for the legal interception of communications at the Internet Service Provider level and at higher gigabit speeds.

The higher gigabit intercept equipment would be placed at major Internet backbone hubs in strategic locations like Washington, DC, the San Francisco Bay Area, Chicago, Dallas, and Los Angeles. Georgiades said that the 1994 Communications Assistance to Law Enforcement Act (CALEA) does not currently extend to the Internet and only applies to telecommunications companies. However, the fact that Top Layer and its unspecified partners are ramping up to deliver CALEA-like wiretapping services for the Internet indicates the FBI sees the power of CALEA growing beyond phone lines to the web. And Georgiades pointed out that foreign governments are under no such constraints and can use Internet snooping equipment under existing current wiretapping laws.

David Banisar, Research Fellow at Harvard’s Information Infrastructure Project, said such systems “set a dangerous precedent to allow law enforcement and intelligence agencies to run the communications system.” He added, “these agencies take an over-inclusive view of who they think are the enemies and its likely that civil and human rights groups will, again, be monitored for no legitimate reason.”

The large defense and intelligence consulting and engineering firm Booz, Allen & Hamilton has not only developed the FBI’s Carnivore capability but it has assisted the bureau in ensuring that all telecommunications companies engineer their systems to ensure they are “wiretap friendly.” The companies are required by the Communications Assistance to Law Enforcement Act to ensure the FBI has access to all forms of telecommunications, including cellular calls.
What if a target decides to use encryption to protect their e-mail from interception? That is not a problem for the FBI. Booz Allen & Hamilton has helped develop a system code-named Magic Lantern, which permits a virus containing a key logging program to be secretly transmitted to a recipient. After installing itself on the target's computer, any time the target types in a password to decrypt a message, that same password is immediately picked up by Magic Lantern and transmitted to the FBI. Essentially, the FBI has a virtual master key to break any encryption program used by a surveillance target.

A companion program to Magic Lantern, code named Cyber Knight, is a relational database system that compares and matches information from e-mail, Internet relay chats, instant messages, and Internet voice communications.

Not to be outdone by the FBI, the CIA has also been extremely active in developing software than can dig deep within the Internet to harvest information. The CIA has relied heavily on its wholly-owned and operated proprietary Silicon Valley company, IN-Q-TEL, to fund research and development for Internet snooping software. IN-Q-TEL's President and Chief Executive Officer Gilman Louie is to keynote a January 2002 Las Vegas seminar on the use of emerging intelligence technology to search and analyze the web. He is to be joined by Joan Dempsey, the Deputy Director of the CIA for Intelligence Community Management. IN-Q-TEL's web page describes the aggressive attitude the CIA is taking toward ensuring new technologies come complete with the spy agency's seal of approval, "IN-Q-TEL strives to extend the Agency's access to new IT companies, solutions, and approaches to address their priority problems."

Assisting the government in its goals to gather massive amounts of personal information on citizens and non-citizens, is a company that owes its very existence to the CIA. Oracle, Inc. Chairman Larry Ellison has offered to provide to the government free of charge the database software required to establish an interactive national ID card system. Oracle got its start when the CIA gave Ellison a contract in the 1970s to design a system to enable the agency to store and retrieve massive amounts if information in databases. Not coincidentally, the code name of that CIA project was "Oracle."

The rush by the government to monitor the Internet has the backing of a group of federal contract research facilities that have pounded out report after report warning about the threat of cyberspace to national security. These "think tanks" include Rand Corporation and Analytical Services Corporation (ANSER). They are assisted in this policy laundering effort by the Center for Strategic and International Studies, the K Street rest home for former Pentagon, intelligence, and State Department political appointees.

But all the technology in the world will not protect citizens from terrorist attacks, unless the government knows how to use the information effectively. As the government and a few selected companies and think tanks push for new surveillance laws and more monitoring of the Internet and telecommunications in general, the words of Mary Schiavo, the Transportation Department's former Inspector General and outspoken critic of lax airline security, are particularly poignant. Speaking in Washington on December 18, Schiavo pointed out that the "United States already had laws to prevent what happened on September 11th . . . they weren't being enforced."

Wayne Madsen is a Washington-based journalist who covers intelligence, national security, and foreign affairs. He is also a Senior Fellow of the Electronic Privacy Information Center (EPIC) in Washington, DC and author of