

Privacy vs. safety

Terrorist threat shifts priorities in online rights debate

By Stefanie Olsen and Evan Hansen
Staff Writers, CNET News.com
September 17, 2001, 11:25 a.m. PT

Last week's terrorist attacks on the World Trade Center and the Pentagon marked a significant turning point in the debate over computer and Internet privacy, giving new weight to calls for broader government surveillance powers.

Law-enforcement agencies in recent months have found themselves on the defensive over wiretapping and other intelligence-gathering technology, with Congress and the courts increasingly backing demands for greater accountability and restraint. But last week's terrorist assaults, the worst in U.S. history, may have instantly reversed that trend.

Political leaders last week rushed to assure Americans that civil rights and privacy laws would be upheld in the search for the perpetrators. Yet proponents of strict limits on the powers of law enforcement could face a powerful, lasting shift in public opinion over the balance of individual rights and national security.

"The bottom line is that for now, privacy will take a backseat to security," said Larry Ponemon, chief executive of the Dallas-based Privacy Council, a knowledge-management and technology company. "Because of (this) disaster, people aren't worrying about giving up too much information as long as a company is going to make the world a safer place."

Privacy advocates are concerned that government officials, swept up in an emotional tide of fear and anger, will undo years of lobbying and education in Washington and beyond. The Information Age has raised uniquely difficult issues of nuance and sensitivity that could be dismissed in fervent calls for public safety.

“
The bottom line is that for now, privacy will take a backseat to security.”

—Larry Ponemon, chief executive,
Privacy Council

The rush to defend the country by any means necessary could clear the way for a raft of controversial technologies, including Internet wiretaps, global communications-monitoring systems, online video cameras, and face-recognition and fingerprint-scanning devices. Some already have been tested and released despite concerns over potential abuse.

On Thursday the Senate passed by voice vote an anti-terrorism bill that includes an amendment allowing the government greater liberty to use surveillance technology, including Internet wiretaps, to combat terrorism. The amendment, authored by Sens. Jon Kyl, R-Ariz., and Orrin Hatch, R-Utah, broadens emergency powers for wiretaps, allowing any U.S. attorney to authorize the installation of "trap and trace" equipment for up to 48 hours.

"At this juncture of our history it is essential that we give our law enforcement authorities every possible tool to search out and bring to justice those individuals who have brought such indiscriminate death into our backyard," Hatch said, according to a transcript from the Senate hearing.

On a separate front, a hard-fought battle that successfully loosened laws banning the export of high-grade encryption products in the late 1990s could be back on, thanks to a terrorism backlash. On Wednesday, Sen. Judd Gregg, R-N.H., made a speech to fellow members of the U.S. Senate strongly urging international cooperation among encryption software developers and the government for technology that provides a backdoor for decoding by federal investigators.

Crossing the line

In the past year, privacy advocates, civil libertarians and lawmakers have spoken about the need to balance the government's use of technology to track criminals with the public's right to privacy. Here are a few of the technologies central to the debate:

The device: Carnivore, now renamed DCS1000

The use: The FBI has been using the technology — which allows it to tap communications that go through Internet service providers — for two years.

The latest: In July, the House of Representatives passed a bill requiring federal law-enforcement officials to release details about the use of electronic surveillance systems. The bill now goes to the Senate for approval.

The device: Echelon

The use: The U.S. surveillance network allegedly can scan e-mail and wireless communications in other countries for specific content.

The latest: The European Parliament released a report in May confirming the existence of Echelon, saying it has been capable of intercepting messages since 1978. U.S. officials have refused to comment on Echelon's existence.

Continued on next page >

Continued

Privacy vs. safety

“The public is going to demand that the government have more ability to conduct surveillance in order to monitor what dangerous people do,” said James Love, director of the Consumer Project on Technology. “That’s one thing we’re going to see happening. But are there ways of dealing with these issues that have any kinds of safeguards built in? What are the realities to prevent the predictable abuses?”

Attorney General John Ashcroft said at a press conference Monday that the Department of Justice will send a proposal to Congress in the next few days asking for expanded rights to conduct computer and telephone wiretaps to “identify, prevent and punish terrorism.”

Among the proposals, the Justice Department seeks to change wiretap rules to make it easier to track individuals. Currently, wiretap orders apply only to a single telephone number. Ashcroft said that limitation makes it difficult for investigators to monitor suspects who change phones frequently, citing the emergence of disposable cell phones to illustrate the problem.

He added that although the Justice Department seeks additional intelligence-gathering tools to conduct its terrorist investigations, it is “mindful” of protecting the privacy of Americans.

Some congressional leaders have sought to reassure the public that constitutional protections will be respected in the use of technology in anti-terrorism measures.

Sen. Patrick Leahy, D-Vt., chairman of the Senate Judiciary Committee, urged members of Congress last week to resist the temptation to abandon civil liberties in the face of terrorist threats. Leahy also chairs the Senate Democratic Task Force on Privacy, which was formed in January 2000 to protect the privacy of Americans’

“

I can’t think of anything that would better expedite the abuse of (surveillance) technology than what has just happened.”

—Coralee Whitcomb, president, Computer Professionals for Social Responsibility

medical and financial records and other personal information.

“When the facts are in and the facts are clear, the Judiciary Committee will look at law-enforcement surveillance capabilities and whether they are adequate or need to be strengthened consistent with the constitutional freedoms that are at the core of our national ideals,” Leahy said in a statement.

Nevertheless, such calls for calm contrasted with the appeals of others eager to sacrifice the right to privacy—guaranteed under the Fourth Amendment of the Constitution—for the promise of greater security. One CNET News.com reader wrote: “If giving up my right to not have my e-mail read could have saved this tragedy from happening, then I say, ‘World, read my mail.’”

Such public sentiment could fuel a political backlash at a sensitive time in the privacy debate. Consumer advocates have recently begun to make inroads with lawmakers, some of whom have started to seek more information about government surveillance technologies.

Federal agencies have repeatedly defended the need for secrecy surrounding details of their eavesdropping technology. But some members of Congress have begun to grow impatient with apparent stonewalling by law enforcement about such activities.

Chief among these is the FBI’s Carnivore system, recently renamed DCS1000 for the sake of political palatability. Carnivore consists of specialized eavesdropping hardware installed directly in commercial systems that link consumers to the Internet, offering the ability to scan any e-mail that travels over the network. Before installing the hardware, the FBI must obtain a search warrant that may set a specific time frame for its use.

The device: face-recognition technology

The use: The biometrics technology can digitally analyze biological characteristics such as facial structure and iris patterns to compare faces with mug shots of criminals.

The latest: The most high-profile U.S. use of the technology came in January, when police scanned the crowd for criminals or terrorists at the Super Bowl in Tampa, Fla. Several months later, the Tampa Police Department installed 36 security cameras with face-recognition software in a downtown entertainment zone.

The device: key-logger system

The use: The technology captures the keystrokes made on a computer and can be used to discover encrypted passwords.

The latest: In *United States v. Nicodemo S. Scarfo*, a federal judge this month ordered prosecutors to show him documents describing how the system works. In closed session, the judge will decide whether the government is protected under the Classified Information Procedures Act, which prevents disclosure for reasons of national security.

Continued on next page >

Continued

Privacy vs. safety

This summer, Rep. Dick Armey, R-Texas, sponsored a bill that would require federal law-enforcement officials to be more forthright when answering questions about Carnivore and other electronic surveillance systems.

In an opinion piece published in June, Rep. Bob Barr, R-Ga., blasted the FBI's veil of secrecy over Carnivore in a demand for greater accountability.

"This computer system has the ability to sort through all e-mail correspondence between law-abiding American citizens traveling over any Internet service provider," he wrote. "To this day, and despite requests made by Congress and public interest groups, the extent to which this system has been used by the government remains unclear."

On Wednesday, however, his tone seemed decidedly less critical of the government's investigative tactics.

"I call on my colleagues to join with me in taking real steps towards untying the hands of our military and intelligence leaders so they are allowed all means necessary to fight this war against terrorism," he said in a statement. "We must give our government every tool at hand to combat those persons who threaten and destroy American lives, and commit terrorist acts across the world."

Armey and Barr were unavailable for interviews last week.

Barr has also led efforts to unveil details of another controversial system known as Echelon, though the U.S. government has not even confirmed its existence, according to the American Civil Liberties Union. The network is supposedly shared by U.S., British, Canadian, Australian and New Zealand intelligence agencies, capturing communications from a variety of sources, including satellite and undersea cable lines.

In an unprecedented move, the National Security Agency last year invoked attorney-client privilege in blocking a congressional inquiry seeking details about

Echelon. President Clinton then signed legislation requiring the NSA to report on the legal basis for Echelon and similar activities.

The courts have also recently weighed in with significant rulings affecting police surveillance powers. For example, a New York federal judge ordered the FBI to provide details of computer keystroke technology used in an investigation that led to the arrest of alleged mobster Nicodemo Scarfo.

Privacy advocates worry that momentum that had been tilting toward greater disclosure and accountability will now shift in the opposite direction.

"The terrorist attacks will cause the widespread use of Carnivore and at the very least an acknowledgment of the Echelon system," said Coralee Whitcomb, president of Computer Professionals for Social Responsibility, a 20-year-old public education group made up of computer scientists.

"The tragedy may soften our commitment to privacy as a public and allow for these technologies, once they are in place, to stay in place afterward," she said. "I can't think of anything that would better expedite the abuse of this technology than what has just happened."

Professor Harold J. Krent, of the Illinois Institute of Technology's Chicago-Kent College of Law, takes a longer view.

"We have a balance in this society to allow for security and freedom for privacy. That balance changes in such an event," said Krent, who was part of a team that assessed Carnivore.

"We are in a new cycle: We'll trade our privacy to be more collectively secure," he added. "We saw this with the Oklahoma bombing and in the Columbine shootings, where the government enacted zero-tolerance laws and parental-responsibility laws that both restricted the freedom of some schoolchildren. We'll see a similar cycle now." ■

The device: fingerprint scanning

The use: The biometrics technology prints and transmits fingerprints electronically to identify people.

The latest: The Alabama Bureau of Investigation said in July that it would use the technology to submit fingerprint and demographic records electronically during background checks.

The device: thermal-imaging system

The use: Police officers have used such technology, which can display pictures of invisible heat waves given off by objects, in criminal investigations.

The latest: In June, the Supreme Court ruled in *Kyollo v. United States* that using thermal-imaging devices without a search warrant would compromise privacy.

Editors: Mike Yamamoto, Julie Laing, Jennifer Balderama

Design: Ellen Ng, Jeff Quan

Production: Ben Helm

Comments on the piece?
letters@news.com

Comments on www.news.com in PDF?
production@news.com