GlobalResearch
Center for Research on Globalization

In the Name of Homeland Security, Telecom Firms Are Deluged With Subpoenas

By Miles Benson
Global Research, December 30, 2005
Newhouse News Service 30 December 2005

Region: USA
Theme: Police State & Civil Rights

WASHINGTON — Operating under new powers to combat terrorism, law enforcement agencies are making unprecedented demands on the telecommunications industry to provide information on subscribers, company attorneys say.

These companies and Internet service providers face an escalating barrage of subpoenas for subscriber lists, personal credit reports, financial information, routing patterns that reveal individual computer use, even customer photographs.

Behind the rising pressure for the fullest use of new technology and surveillance is homeland security. As police and intelligence agencies seek to deter future terrorist threats, the government is testing the limits of the expanded authority Congress provided when it passed the Patriot Act with broad bipartisan support in October.

“The amount of subpoenas that carriers receive today is roughly doubling every month — we’re talking about hundreds of thousands of subpoenas for customer records — stuff that used to require a judge’s approval,” said Albert Gidari, a Seattle-based expert in privacy and security law who represents numerous technology companies.

The Sunnyvale, Calif., headquarters of Yahoo, an Internet search engine used by millions, now has a voicemail prompt that refers law enforcement authorities to a special telephone number to which they can fax criminal investigation subpoenas.

“Everything is an emergency now,” Gidari said, though he believes “a lot of it is just fishing.”

Gidari’s clients include AT&T Wireless, AOL, the Cellular Telecommunications and Internet Association, Cricket Communications, Nextel, VoiceStream, Cingular Wireless, Rural Cellular Corp., Connexion by Boeing, Terabeam and Infospace.

At the FBI, spokesman Bill Carter referred all inquires about the volume of Patriot Act subpoenas to the Justice Department. At the Justice Department, spokesman Bryan Sierra said it might take “a long time” to determine how many subpoenas have been issued, and that it may not be possible to make the information public.

But clearly the heat is on.

“It’s not just volume but the scope of the subpoenas we are seeing, where instead of a rifle shot it’s more of a shotgun approach,” said Michael Altschul, legal counsel for the Cellular Telecommunications & Internet Association.

Altschul said carriers are struggling “as good citizens” to comply with complex and comprehensive surveillance demands that may sometimes “require adding three shifts around the clock.” The subpoenas are beginning to impose a financial burden on companies, Altschul said.

Gidari agreed, saying that companies “should be compensated for reasonable costs” and immunized from lawsuits claiming privacy rights were violated, and that new federal regulations should be drafted to spell out the rights and obligations of service providers.

Edward Black, president of the Computer & Communications Industry Association, said the industry is in “uncharted legal waters” — caught between customer expectations of privacy and government demands for information. “Either way we might appear to be breaking some kind of law.”

Particularly troublesome, Black said, is when law enforcement authorities move swiftly and “short-circuit” regular legal procedures. “I think we must be careful not to create a process whereby using a private company somehow empowers the government to do things they cannot legally do under the new laws,” Black said.

“In many respects authorities are doing what most Americans want them to be doing,” said Stewart Baker, law enforcement and national security specialist at Steptoe and Johnson, a Washington law firm. “In the long run, though, it does mean there’s an awful lot of information about people in law enforcement files, not because the police are bad or corrupt, but because an investigation has to track down a lot of leads.

“What happens to that information four or five years from now? The FBI doesn’t throw anything away.”

Technology has opened many new windows for law enforcement officers.

A typical subpoena to a cell phone service provider, Gidari said, can be used to identify all calls on a certain date between 10:15 and 10:30 a.m. by everyone in a small town, or within a few square blocks of a big city.

Prosecutors, acting under the authority of grand jury investigations, may issue subpoenas without prior approval of a judge. Critics complain that the Patriot Act makes it possible for CIA agents working with law enforcement officers to jointly draw up subpoenas, obtain information, and never have to appear in court to explain how the information was used.

Online booksellers can be forced to divulge lists of customers who have expressed interest in books about explosives, poisons or other subjects that arouse suspicion. The government is also collecting photographs of customers to include in databases for later matches against computerized facial recognition systems, Gidari said.

“Without a judge’s order, it used to be they could only get records of someone they suspected was acting on behalf of a foreign government or a terrorist organization,” said Kate Martin, director for the Center for National Security Studies, a nonprofit civil liberties group. “Now they can get the records of anyone if they simply say it is `in connection’ with a terrorism investigation.”

Under the Patriot Act, said James X. Dempsey, director of the Center for Democracy &

Technology and author of “Terrorism and the Constitution,” the FBI “can go into a public library and ask for the records on anybody who ever used the library, or who used it on a certain day, or checked out certain kinds of books.

“It can do the same at any bank, telephone company, hotel or motel, hospital or university — merely upon the claim that the information is `sought for’ an investigation to protect against international terrorism or clandestine intelligence activities.”

Law enforcement officials have begun to press sources to deliver information without a formal subpoena, according to company lawyers. “Investigators have quickly learned that they don’t need to leave a paper trail anymore so nobody can judge the lawfulness of a request,” Gidari said.

At America Online, spokesman Andrew Weinstein said the company always insists on a court order, a subpoena or a search warrant before turning over information to the government.

But Peter Swire, a law professor at Ohio State University who served as a privacy counselor to the Clinton White House, said he is hearing complaints about “requests for cooperation from law enforcement agencies with the idea that it is unpatriotic if the companies insist too much on legal subpoenas first.”

Brent Scowcroft, who a decade ago was national security adviser to the first President Bush and who now serves as an outside adviser to the White House, acknowledges that homeland security requires “a kind of trade-off” of privacy and civil liberties.

“The war on terrorism is basically a war of intelligence,” Scowcroft said. “Every time they move, every time they get money or spend money, there’s a trace, somewhere. What we need to do is get as many of those traces as we can and put them together into a mosaic which will allow us to uncover the al-Qaida network.”

It is necessary to cast a wide net, Scowcroft suggested.

“There are a lot of things floating around that form a pattern that probably defies our own mental ability to put together, but the computer capacity we have now gives you great ability to link similar, apparently very disparate and unconnected patterns together,” he said.

There has been little public outcry against the trend, possibly because “there is something that people just haven’t grasped, though government investigators have,” Gidari said. “A network economy yields so much more information about personal lives that can be collected and manipulated in ways most people don’t understand.”

In fact, since Sept. 11, pollsters have tracked a dramatic shift in public attitudes about government and privacy. In a national survey March 28, pollster John Zogby found 55 percent in favor of allowing police to search their purses, handbags, backpacks or packages at random anywhere, while 48 percent would allow their cars to be searched, 36 percent would allow their mail to be searched and 26 percent said they would not object to having telephone conversations monitored by authorities.

Prior to Sept. 11, rights to privacy in such areas were “inviolable, the most cherished rights Americans had,” Zogby said.

While polls indicate widespread public support for vigorous government action to avert terrorist threats, some privacy experts and civil liberties advocates worry about the possibility of mistakes compounding in an overloaded information system and the long-term danger of abuses when intrusions become routine.

Some government officials and others say that the war justifies broad use of surveillance capabilities and new technologies, even at the cost of diminishing privacy and civil liberties.

“When you engage in this debate, you’re either going to fall on the side of saying, `I more or less trust law enforcement even if they don’t do the right thing 100 percent of the time, and I don’t mind them being empowered’ — or you’re going to say, `I don’t trust law enforcement, and I don’t think they should be empowered,”‘ said Robert Atkinson, formerly a senior analyst for the Congressional Office of Technology Assessment, now vice president of the Progressive Policy Institute, a Democratic think tank.

But it’s not simply a matter of trust, said Dempsey of the Center for Democracy & Technology, another Washington think tank.

“We endow government with tremendous power — power to arrest you, take away your property, take away your life, destroy your reputation, take your children away from you,” Dempsey said. “I think those powers in the hands of human beings, acting under pressure, with the best of intentions, facing time deadlines in a world of limited resources, those kinds of powers need to be surrounded with a thicket of rules.”

The problem that law enforcement and intelligence agencies face is not insufficient information — “they are choking on information,” Dempsey said. The deficiency is in targeting and analysis. The Patriot Act was based on “the assumption if you pour more data into the system, then the picture would become clearer, and I think that’s a false presumption,” Dempsey said.

The danger, said John Baker, a law professor at Louisiana State University, is applying the government’s war powers to domestic activities. “We’ve never had such a mix-up between the president’s wartime powers and law enforcement,” Baker said. “The president has wide powers under war and national defense, but the national government does not have wide powers for law enforcement.”

In the ’60s and ’70s, the FBI ran a massive program called COINTELPRO that included secret investigations, surveillance, infiltration and disruption of political activist groups that were not engaged in illegal conduct, including the civil rights movement, anti-war protesters and feminists.

Today, it is the accumulation of personal information about ordinary citizens that most disturbs civil libertarians, who believe the nation is commencing “the golden age” of wiretapping.

“Consumers should know that the information they give to America Online or Microsoft may very well wind up at the IRS or the FBI,” said Jeffrey A. Eisenach, president of the Progress & Freedom Foundation, a think tank that studies technology and public policy. “Security is not costless,” Eisenach said.

Writing in the American Spectator recently, Eisenach said high-speed data networks and new technologies “will indeed soon give governments the ability to monitor the

whereabouts of virtually everyone."

The aphorism "If you build it, they will come" is apt, said attorney Gidari. "And `they' are the law enforcement authorities."

(Miles Benson can be contacted at miles.benson@newhouse.com)
