NSA phone spying program: a blueprint for mass repression

Patrick Martin
15 May 2006

In the wake of the May 11 revelation by *USA Today* of a massive telephone spying program by the National Security Agency, directed against nearly every American citizen, the media commentary has deliberately downplayed the sinister nature of the program. This is a deliberate cover-up of what is without question the most wide-ranging invasion of privacy by the federal government in US history.

The press coverage has sought to obscure the vast scale of the data-gathering, as well as the political purposes to which it can be used, in order to lend credence to the Bush administration's claim that the operation is targeted exclusively at suspected terrorists linked to Al Qaeda. There has not been a single serious media commentary questioning why a supposedly "narrowly focused" program should collect data on an estimated 225 million Americans. Nor has there been any suggestion that the real purpose of the spy program is to assemble a database on the political affiliations and activities of a wide range of American citizens.

Further details of the program have emerged, however, in scattered press reports as well as legal papers filed by civil liberties groups and lawyers acting for telephone company customers who object to their personal information being handed over to the federal government.

By these accounts, the computer programs being used by the NSA to analyze the phone call databases it purchased from the big telecommunications companies are a more advanced form of the "social-network analysis" software used by commercial and political marketing firms to profile potential advertising targets. Phone trees are traced to identify nodes and determine common interests and activities among those targeted.

In the case of commercial marketing, the purpose is to identify the best targets to receive a sales pitch. For the intelligence agencies, the purpose is to select targets for more intensive electronic surveillance, or arrest and (perhaps indefinite) detention.

The potential value of this information for purposes of political intimidation is enormous. Every person who has ever telephoned a 900 number, for instance, now has that fact permanently recorded in a government database, making him or her vulnerable to blackmail by federal agents. Likewise those whose phone records suggest problems with gambling, narcotics abuse, or even extramarital affairs.

The FBI regularly used such information for nefarious purposes during the notorious 50-year reign of J. Edgar Hoover, who kept special files on the sexual and other peccadilloes of congressmen and government officials. Now such information will be available on every American citizen.

The sheer size of the database makes the NSA surveillance program unique and truly Orwellian in character. AT&T, Verizon and BellSouth, the three telecommunications companies which supplied the data, provided the NSA with the calling records on 224 million land-line and cellular telephone customers, 80 percent of the land-line and 50 percent of the wireless users in the US. According to press reports, the three companies connected 500 billion telephone calls in 2005 alone, and over two trillion since 9/11. Information on all these calls—the number calling, the number dialed, the time and duration—is now in the NSA database, along with historical information of unknown but vast dimensions.

The Electronic Frontier Foundation (EFF), which sued AT&T earlier this year over its collaboration with the NSA, said that the AT&T call database alone spans 312 terabytes, the equivalent of more than 400,000 CD-ROMs. EFF attorney Kevin Bankston told the *Los Angeles Times*, "There is simply no legal process for this kind of wholesale invasion of privacy. What they claim to be doing with the data is irrelevant because the fact is they could do whatever they choose without any oversight."

No previous regime, no matter how dictatorial—not Nazi Germany, not Stalinist Russia—was able to compile such an all-encompassing record of the private activities of its citizens. (The Nazis had to make do with primitive card-sorting devices supplied, at a hefty profit, by IBM.)

The press reports claim that the NSA did not actually eavesdrop on the phone calls, collecting only external information. *Time* magazine, for instance, writes: "Officials insist that the NSA is not eavesdropping on millions of law-abiding Americans, but merely compiling what the telephone companies refer to as 'call detail' information, recording what number called what number, when and for how long. 'It's just digits,' insists a White House official."

Two points should be made. First, even if true, this is a gross violation of personal privacy, one that would, in an ordinary police investigation, require the showing of probable cause to obtain a court order. Second, and more importantly, there is no reason to believe that NSA program was confined to call detail records and involved no eavesdropping.

The *New York Times*, in a lengthy account Sunday, wrote that after the September 11 terrorist attacks Vice President Dick Cheney pressed the NSA to intercept purely domestic phone calls, although he was supposedly rebuffed by NSA lawyers, who cited longstanding constitutional and legal prohibitions on such spying. The *Times* reported that many domestic phone calls were nonetheless intercepted, and quoted a White House spokeswoman, Dana Perino, confirming the interceptions but denying that they were "intentional."

The media reports on the surveillance program invariably state, without any qualification, that the telephone company records were handed over to the NSA without the names and addresses of the customers, implying that there was an effort to preserve confidentiality. There have been repeated descriptions of the data as "anonymized," as though there was no way for the NSA to trace back from the telephone numbers to the identities of those making the calls. This is absurdly false.

Even the simplest Internet search can pull up individual names associated with particular phone numbers. And the federal government has access to many more databases than these search engines. As the *New York Times* pointed out in an editorial Friday, "By cross-referencing phone numbers with databases that link numbers to names and addresses, the government could compile dossiers of what people and organizations each American is in contact with." (The *Times* ended this editorial with

© World Socialist Web Site

the cynical suggestion that the Bush administration obtain permission from Congress to continue its warrantless telephone spying).

Three years ago there was a political uproar when it was revealed that the Pentagon had established a data-mining program, entitled Total Information Awareness (TIA), to consolidate commercial records and government intelligence and criminal files into a central database that would be used, allegedly, to identify potential terrorist threats. The program was headed by Admiral John Poindexter, a convicted felon in the Iran-Contra affair who was later pardoned by the first president Bush. TIA was shut down after Congress cut off its funding.

The NSA program is far more sweeping and intrusive than TIA, but there has been no suggestion from any congressional quarter, liberal or conservative, Democrat or Republican, that it should be shut down. All the criticism revolves around demands that Congress be more fully informed of the program and given a say in how it operates—i.e., that Congress be a partner in the erection of the framework for an American police state, rather than a spectator.

For all the hemming and hawing in Congress and in media editorials, the lawless character of the Bush administration's telephone spying is unquestionable. The Fourth Amendment to the US Constitution spells out the right to be free of illegal searches in unmistakable terms: "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."

The *Chicago Tribune* interviewed Russell Tice, a former NSA analyst who was one source for the exposure last December of illegal NSA interception of international phone calls by thousands of Americans. Tice told the *Tribune*, "Everyone at NSA knew what they were doing was illegal, because it's drilled into our heads over and over that it's against NSA policy, that you do not do that. The choice is to speak out and get fired."

The response of Qwest, the lone telecommunications company to refuse the NSA request for phone records, demonstrates that the surveillance program was widely understood to be illegal. Former Qwest CEO Joseph Nacchio "concluded that these requests violated the privacy requirements of the Telecommunications Act," his lawyer said in a statement Thursday. Nacchio also cited the refusal of the NSA to obtain approval of the telephone surveillance from the special court set up under the Foreign Intelligence Surveillance Act (FISA).

The reference to the FISA court is especially revealing. FISA was adopted in 1978 after the exposure of illegal CIA, FBI, NSA and Pentagon spying on American citizens throughout the Vietnam War period. Thereafter, in the midst of the Cold War, US intelligence agencies were required to go before the FISA court to obtain approval to wiretap the communications of suspected foreign spies. Yet today, when the enemy is not a powerful industrialized state armed with thousands of nuclear weapons, but a small band of Islamic fundamentalist terrorists, the US government rejects the slightest democratic restraint on the activities of its police agencies.

Nacchio, the Qwest CEO, was repeatedly pressured by federal agents to comply. (He was later indicted on insider-trading charges, which he is currently fighting in court). His successor, Richard Notebaert, reached the same conclusion about the illegality of the surveillance program and ultimately broke off negotiations with the NSA in 2004.

Perhaps the most telling aspect of the Qwest-NSA discussions is that the agency consistently refused either to seek a court order or to present a directive from the US attorney general requiring the company's cooperation. Tacitly acknowledging that it had no legal authority, the NSA sought Qwest's voluntary cooperation, just as it had obtained the voluntary cooperation of AT&T, Verizon and BellSouth.

At least three other telecommunications firms, Verizon Wireless, Cingular Wireless and T-Mobile USA Inc. (a division of Deutsche Telekom), have denied participating in the NSA program, and the Internet companies Google, AOL and the MSN unit of Microsoft also declared that they had not supplied mass consumer information to the agency.

If the program was, as the Bush administration claims, absolutely vital for defending the American people from a new 9/11, how is the failure to enlist these companies to be explained? The reality is that the administration was well aware its requests were without legal authority, and it sought to conceal its mass snooping campaign from public scrutiny rather than seek court orders against non-complying companies.

There is ample reason to believe that the telecommunications companies themselves violated the law by handing over masses of consumer information to the NSA. An article in the *Los Angeles Times* Friday spelled out the legal precedents.

It noted that in 1986 Congress passed the Electronic Communications Privacy Act, in response to a 1979 Supreme Court decision, *Smith v. Maryland*, which allowed local police to obtain phone records without a warrant. The high court ruled by analogy to ordinary mail service, finding that the contents of the envelope were private, but the address written on the outside was not. Similarly, the court argued, there should be no expectation of privacy for the phone number dialed or the email address used to send an electronic message.

Congress specifically overturned this precedent in the 1986 law, which declares, in Section 2702, that providers of "electronic communications... shall not knowingly divulge a record or other information pertaining to a subscriber or customer... to any government entity." Since then, local police have been required to show probable cause and get a search warrant from a court to obtain the record of anyone's telephone calls. Companies that violate the law can be compelled to pay damages of $1,000 per violation per customer.

The first lawsuit under the 1986 law was filed Friday against Verizon in a Manhattan federal court. Bruce Afran, one of the lawyers, declared, "This is almost certainly the largest single intrusion into American civil liberties ever committed by any US administration. Americans expect their phone records to be private. That's our bedrock governing principle of our phone system."

The scale of the damages is staggering: with trillions of phone calls disclosed, at $1,000 each, any award that was proportional to the scale of the violation would bankrupt the corporations which collaborated with the illegal spying.

To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact

© World Socialist Web Site