BIOMETRICS
TASK FORCE

IN THE NEWS

The Washington Post

Post-9/11 Dragnet Turns Up Surprises

Biometrics Link Foreign Detainees To Arrests in U.S.

By Ellen Nakashima
Washington Post Staff Writer
Sunday, July 6, 2008; Page A01

FBI agent Paul Shannon led a team sent to Afghanistan in 2001 to fingerprint and interview foreign fighters for a database of known or suspected terrorists. Here, he takes Saddam Hussein's prints after his capture in 2003.

In the six-and-a-half years that the U.S. government has been fingerprinting insurgents, detainees and ordinary people in Afghanistan, Iraq and the Horn of Africa, hundreds have turned out to share an unexpected background, FBI and military officials said. They have criminal arrest records in the United States.

There was the suspected militant fleeing Somalia who had been arrested on a drug charge in New Jersey. And the man stopped at a checkpoint in Tikrit who claimed to be a dirt farmer but had 11 felony charges in the United States, including assault with a deadly weapon.

The records suggest that potential enemies abroad know a great deal about the United States because many of them have lived here, officials said. The matches also reflect the power of sharing data across agencies and even countries, data that links an identity to a distinguishing human characteristic such as a fingerprint.

"I found the number stunning," said Frances Fragos Townsend, a security consultant and former assistant to the president for homeland security. "It suggested to me that this was going to give us far greater insight into the relationships between individuals fighting against U.S. forces in the theater and potential U.S. cells or support networks here in the United States."

The fingerprinting of detainees overseas began as ad-hoc FBI and U.S. military efforts shortly after the Sept. 11, 2001, terrorist attacks. It has since grown into a government-wide push to build the world's largest database of known or suspected terrorist fingerprints. The effort is being boosted by a presidential directive signed June 5, which gave the U.S. attorney general and other cabinet officials 90 days to come up with a plan to expand the use of biometrics by, among other things, recommending categories of people to be screened beyond "known or suspected" terrorists.

Fingerprints are being beamed in via satellite from places as far-flung as the jungles of Zamboanga in the southern Philippines; Bogota, Colombia; Iraq; and Afghanistan. Other allies, such as Sweden, have contributed prints. The database can be queried by U.S. government agencies and by other countries through Interpol, the international police agency.

Civil libertarians have raised concerns about whether people on the watch lists have been appropriately determined to be terrorists, a process that senior government officials acknowledge is an art, not a science.

Large-scale identity systems "can raise serious privacy concerns, if not singly, then jointly and severally," said a 2007 study by the Defense Science Board Task Force on Defense Biometrics. The ability "to cross reference and draw new, previously unimagined, inferences," is a boon for the government and the bane of privacy advocates, it said.

An FBI Mission

The effort, officials say, is bearing fruit.

"The bottom line is we're locking people up," said Thomas E. Bush III, FBI assistant director of the Criminal Justice Information Services division. "Stopping people coming into this country. Identifying IED-makers in a way never done before. That's the beauty of this whole data-sharing effort. We're pushing our borders back."

In December 2001, an FBI team was sent on an unusual mission to Afghanistan. The U.S. military had launched a wave of airstrikes aimed at killing or capturing al Qaeda fighters and their Taliban hosts. The FBI team was to fingerprint and interview foreign fighters as if they were being booked at a police station.

The team, led by Paul Shannon, a veteran FBI agent embedded with U.S. special forces, traveled to the combat zone toting briefcases outfitted with printer's ink, hand rollers and paper cards. The agents worked in Kandahar and Kabul. They traversed the Afghanistan-Pakistan border. They hand-carried the fingerprint records from Afghanistan to Clarksburg, W.Va., home to the FBI's criminal biometric database.

As they analyzed the results, they were surprised to learn that one out of every 100 detainees was already in the FBI's database for arrests. Many arrests were for drunken driving, passing bad checks and traffic violations, FBI officials said.

"Frankly I was surprised that we were getting those kind of hits at all," recalled Townsend, who left government in January. They identified "a potential vulnerability" to national security the government had not fully appreciated, she said.

The people being fingerprinted had come from the Middle East, North Africa and Pakistan. They were mostly in their 20s, Shannon recalled. "One of the things we learned is we were dealing with relatively young guys who were very committed and what they would openly tell you is that when they got out they were going back to jihad," he said. "They'd already made this commitment."
One of the first men fingerprinted by the FBI team was a fighter who claimed he was in Afghanistan to learn the ancient art of falconry. But a fingerprint check showed that in August 2001 he had been turned away from Orlando International Airport by an immigration official who thought he might overstay his visa. Mohamed al Kahtani would later be named by the Sept. 11 Commission as someone who allegedly had sought to participate in hijackings. He currently is in custody at Guantanamo Bay.

Similarly, in 2004, an FBI team choppered to a remote desert camp on the Iraq-Iran border, home to the Mujahedin-e-Khalq (MEK), whose aim is to overthrow the Iranian government. The MEK lead an austere lifestyle in which men are segregated from women and material goods are renounced. The U.S. State Department considers the organization to be a terrorist group.

The FBI team fingerprinted 3,800 fighters. More than 40, Shannon said, had previous criminal records in the agency's database.

BIOMETRICS TASK FORCE IN THE NEWS

While the FBI was busy collecting fingerprints, the military was setting up its own biometrics database, adding in iris and facial data as well. By October, the two organizations agreed to collaborate, running queries through both systems. The very first match was on the man who claimed to be a poor dirt farmer. Among his many charges were misdemeanors for theft and public drunkenness in Chicago and Utah, a criminal record that ran from 1993 to 2001, said Herb Richardson, who serves as operations manager for the military's Automated Biometric Identification System under a contract with Ideal Innovations of Arlington.

Many of those with U.S. arrest records had come to the United States to study, said former Criminal Justice Information Services head Michael Kirkpatrick, who led the FBI effort to use biometrics in counterterrorism after Sept. 11. "It suggests there was some familiarity with Western culture, the United States specifically, and for whatever reason they did not agree with that culture," he said. "Either they became disaffected or put up with it, and then they went overseas."

Errors in matching, though rare, have occurred. In a noted 2004 case, Oregon lawyer Brandon Mayfield was erroneously named as a suspect in the Madrid train bombings that killed 191 people. FBI lab analysts matched a print lifted from a plastic bag at the crime scene to his fingerprints that were stored in the FBI's criminal database because of a 1985 arrest for auto burglary when he was a teenager. The charge had been dismissed. After a critical Justice Department Inspector General audit, the FBI made fixes in its system. A recent inspector general report found the FBI fingerprint matching to be generally accurate.

Worries About Watch List

Civil libertarians, however, worry that the systems are not transparent enough for outsiders to tell how the government decides who belongs on a watch list and how that information is handled.

"The day when the federal government can tell people the basis they've been put on the watch list is the day we can have more confidence in biometric identification," said Marc Rotenberg, executive director of the Electronic Privacy Information Center.

Vetting the data is the job of analysts at the National Counterterrorism Center, an office park-like complex in McLean run by the Office of the Director of National Intelligence. Analysts there scour intelligence reports to create the master international terrorist watch list.

"You cannot draw a bright red line and say that's a terrorist, this person isn't," said Russ Travers, an NCTC deputy director. "If somebody swears allegiance to Bin Laden, that's an easy case. If somebody goes to a terrorist training camp, that's probably an easy case. What if a person goes to a camp and decides, 'I don't want to go to a camp, I want to go home.' Where do you draw the line?"

Investigators are working on ever more sophisticated ways to evaluate the data. Analysts at the Army's National Ground Intelligence Center in Charlottesville, for instance, use software to scrutinize intelligence reports from sources such as electronic surveillance and informants. They then link the information to a person's biographic and biometric data, and look for relationships that might detect terrorists and plots.

For example, a roadside bomb may explode and a patrol may fingerprint bystanders because insurgents have been known to remain at the scene to observe the results

http://www.biometrics.dod.mil/

of their work. Prints also can be lifted off tiny fragments of exploded bombs, said military officials and contractors involved in the work.

Analysts are not just trying to identify the prints on the bomb. They want to find out who the bomb-carrier associates with. Who he calls. Who calls him. That could lead to the higher-level operatives who planned and financed attacks.

Already, fingerprints lifted off a bomb fragment have been linked to people trying to enter the United States, they said.

In a separate data-sharing program, 365 Iraqis who have applied to the Department of Homeland Security for refugee status have been denied because their fingerprints turned up in the Defense Department's database of known or suspected terrorists, Richardson said.

If Iraq and Afghanistan were a proving ground of sorts for biometric watch-listing, the U.S. government is moving quickly to try to build a domestic version. Since September 2006, Homeland Security and the FBI have been operating a pilot program in which police officers in Boston, Dallas and Houston run prints of arrestees against a Homeland Security database of immigration law violators and a State Department database of people refused visas. Federal job applicants' prints also are run against the databases. To date, some 500 people have been found in the database and thus are of interest to Homeland Security officials.

Steve Nixon, a director at the Office of the Director of National Intelligence, said the effort is key to national security.

"When we look at the road and the challenges, globalization and the spread of technology has empowered small groups of individuals, bad guys, to be more powerful than at any other time in history," he said. "We have to know who these people are when we encounter them. A lot of what we're doing in intelligence now is trying to identify a person. Biometrics is a key element of that."

Staff researcher Richard Drezen contributed to this report.