washingtonpost.com

FBI Prepares Vast Database Of Biometrics

$1 Billion Project to Include Images of Irises and Faces

By Ellen Nakashima
Washington Post Staff Writer
Saturday, December 22, 2007; A01

CLARKSBURG, W. Va. -- The FBI is embarking on a $1 billion effort to build the world's largest computer database of peoples' physical characteristics, a project that would give the government unprecedented abilities to identify individuals in the United States and abroad.

Digital images of faces, fingerprints and palm patterns are already flowing into FBI systems in a climate-controlled, secure basement here. Next month, the FBI intends to award a 10-year contract that would significantly expand the amount and kinds of biometric information it receives. And in the coming years, law enforcement authorities around the world will be able to rely on iris patterns, face-shape data, scars and perhaps even the unique ways people walk and talk, to solve crimes and identify criminals and terrorists. The FBI will also retain, upon request by employers, the fingerprints of employees who have undergone criminal background checks so the employers can be notified if employees have brushes with the law.

"Bigger. Faster. Better. That's the bottom line," said Thomas E. Bush III, assistant director of the FBI's Criminal Justice Information Services Division, which operates the database from its headquarters in the Appalachian foothills.

The increasing use of biometrics for identification is raising questions about the ability of Americans to avoid unwanted scrutiny. It is drawing criticism from those who worry that people's bodies will become de facto

national identification cards. Critics say that such government initiatives should not proceed without proof that the technology really can pick a criminal out of a crowd.

The use of biometric data is increasing throughout the government. For the past two years, the Defense Department has been storing in a database images of fingerprints, irises and faces of more than 1.5 million Iraqi and Afghan detainees, Iraqi citizens and foreigners who need access to U.S. military bases. The Pentagon also collects DNA samples from some Iraqi detainees, which are stored separately.

The Department of Homeland Security has been using iris scans at some airports to verify the identity of travelers who have passed background checks and who want to move through lines quickly. The department is also looking to apply iris- and face-recognition techniques to other programs. The DHS already has a database of millions of sets of fingerprints, which includes records collected from U.S. and foreign travelers stopped at borders for criminal violations, from U.S. citizens adopting children overseas, and from visa applicants abroad. There could be multiple records of one person's prints.

"It's going to be an essential component of tracking," said Barry Steinhardt, director of the Technology and Liberty Project of the American Civil Liberties Union. "It's enabling the Always On Surveillance Society."

If successful, the system planned by the FBI, called Next Generation Identification, will collect a wide variety of biometric information in one place for identification and forensic purposes.

In an underground facility the size of two football fields, a request reaches an FBI server every second from somewhere in the United States or Canada, comparing a set of digital fingerprints against the FBI's database of 55 million sets of electronic fingerprints. A possible match is made -- or ruled out--as many as 100,000 times a day.

Soon, the server at CJIS headquarters will also compare palm prints and, eventually, iris images and face-shape data such as the shape of an earlobe. If all goes as planned, a police officer making a traffic stop or a border agent at an airport could run a 10-fingerprint check on a suspect and within seconds know if the person is on a database of the most wanted criminals and terrorists. An analyst could take palm prints lifted from a crime scene and run them against the expanded database. Intelligence agents could exchange biometric information worldwide.

More than 55 percent of the search requests now are made for background checks on civilians in sensitive positions in the federal government, and jobs that involve children and the elderly, Bush said. Currently those prints are destroyed or returned when the checks are completed. But the FBI is planning a "rap-back" service, under which employers could ask the FBI to keep employees' fingerprints in the database, subject to state privacy laws, so that if that employees are ever arrested or charged with a crime, the employers would be notified.

Advocates say bringing together information from a wide variety of sources and making it available to multiple agencies increases the chances to catch criminals. The Pentagon has already matched several Iraqi suspects against the FBI's criminal fingerprint database. The FBI intends to make both criminal and civilian data available to authorized users, officials said. There are 900,000 federal, state and local law enforcement officers who can query the fingerprint database today, they said.

The FBI's biometric database, which includes criminal history records, communicates with the Terrorist Screening Center's database of suspects and the National Crime Information Center database, which is the FBI's master criminal database of felons, fugitives and terrorism suspects.

The FBI is building its system according to standards shared by Britain, Canada, Australia and New Zealand.

At the West Virginia University Center for Identification Technology Research (CITeR), 45 minutes north of the FBI's biometric facility in Clarksburg, researchers are working on capturing images of people's irises at distances of up to 15 feet, and of faces from as far away as 200 yards. Soon, those researchers will do biometric research for the FBI.

Covert iris- and face-image capture is several years away, but it is of great interest to government agencies.

Think of a Navy ship approaching a foreign vessel, said Bojan Cukic, CITeR's co-director. "It would help to know before you go on board whether the people on that ship that you can image from a distance, whether they are foreign warfighters, and run them against a database of known or suspected terrorists," he said.

Skeptics say that such projects are proceeding before there is evidence that they reliably match suspects against a huge database.

In the world's first large-scale, scientific study on how well face recognition works in a crowd, the German government this year found that the technology, while promising, was not yet effective enough to allow its use by police. The study was conducted from October 2006 through January at a train station in Mainz, Germany, which draws 23,000 passengers daily. The study found that the technology was able to match travelers' faces against a database of volunteers more than 60 percent of the time during the day, when the lighting was best. But the rate fell to 10 to 20 percent at night.

To achieve those rates, the German police agency said it would tolerate a false positive rate of 0.1 percent, or the erroneous identification of 23 people a day. In real life, those 23 people would be subjected to further screening measures, the report said.

Accuracy improves as techniques are combined, said Kimberly Del Greco, the FBI's biometric services section chief. The Next Generation database is intended to "fuse" fingerprint, face, iris and palm matching capabilities by 2013, she said.

To safeguard privacy, audit trails are kept on everyone who has access to a record in the fingerprint database, Del Greco said. People may request copies of their records, and the FBI audits all agencies that have access to the database every three years, she said.

"We have very stringent laws that control who can go in there and to secure the data," Bush said.

Marc Rotenberg, executive director of the Electronic Privacy Information Center, said the ability to share data across systems is problematic. "You're giving the federal government access to an extraordinary amount of information linked to biometric identifiers that is becoming increasingly inaccurate," he said.

In 2004, the Electronic Privacy Information Center objected to the FBI's exemption of the National Crime Information Center database from the Privacy Act requirement that records be accurate. The group noted that the Bureau of Justice Statistics in 2001 found that information in the system was "not fully reliable" and that files "may be incomplete or inaccurate." FBI officials justified that exemption by claiming that in law enforcement data collection, "it is impossible to determine in advance what information is accurate, relevant, timely and complete."

Privacy advocates worry about the ability of people to correct false information. "Unlike say, a credit card number, biometric data is forever," said Paul Saffo, a Silicon Valley technology forecaster. He said he feared that the FBI, whose computer technology record has been marred by expensive failures, could not guarantee the data's security. "If someone steals and spoofs your iris image, you can't just get a new eyeball," Saffo said.

In the future, said CITeR director Lawrence A. Hornak, devices will be able to "recognize us and adapt to us."

"The long-term goal," Hornak said, is "ubiquitous use" of biometrics. A traveler may walk down an airport corridor and allow his face and iris images to be captured without ever stepping up to a kiosk and looking into a camera, he said.

"That's the key," he said. "You've chosen it. You have chosen to say, 'Yeah, I want this place to recognize me.' "

Staff researcher Richard Drezen contributed to this report.

Post a Comment

View all comments that have been posted about this article.

You must be logged in to leave a comment. Login | Register

Submit

Comments that include profanity or personal attacks or other inappropriate comments or material will be removed from the site. Additionally, entries that are unsigned or contain "signatures" by someone other than the actual author will be removed. Finally, we will take steps to block users who violate any of our posting standards, terms of use or privacy policies or any other policies governing this site. Please review the full rules governing commentaries and discussions. You are fully responsible for the content that you post.