

Roger, WILCO.

« Challenge us again

Go ahead, challenge us. »



# DefenseNews

[Log In](#) | [Register](#) | [Subscribe](#) | [Renew](#)

SEARCH

[Electronic Edition](#) | [NEW! List of RSS Feeds](#)

HELP

[HOME](#) | [AIR](#) | [LAND](#) | [NAVAL](#) | [EUROPE](#) | [AMERICAS](#) | [ASIA & PACIFIC RIM](#) | [MIDDLE EAST & AFRICA](#) | [FEATURES](#)
[Features »](#) | [Technology Watch](#) | [Business Watch](#) | [Interview](#) | [Cover Story](#) | [Commentary](#) | [Special Report](#) | [Top 100](#) | [Online Show Daily](#)

ADVERTISEMENT

**2009 Integration Conference & Awards Banquet**  
October 19-20, 2009  
Arlington, VA

**Keynote Speakers Announced**

**Lieutenant General David A. Deptula**

**Vice Admiral Robert Harward**

**Register Now!**

## Double-Edged Sword

### U.S. Biometric Database Yields Rewards - and Risks

By [WILLIAM MATTHEWS](#)

Published: 24 August 2009

PRINT | EMAIL

Fingerprints, iris scans and other forms of biometric identification enabled U.S. troops to catch more than 400 "high-value individuals" in Iraq and Afghanistan in 2008, Lisa Swan said.

"We've been very successful at catching bad guys," said Swan, who is deputy director of the U.S. Army's Biometric Task Force.

After several years of compiling vast biometric databases that now contain identification information on more than 2.5 million Iraqis, the U.S. military is sold on the technology.

Fingerprints and irises are checked before Iraqis are allowed past checkpoints. Biometric identification is required before Iraqi and Afghan employees are allowed to enter U.S. bases. And "we take biometrics on all detainees to check and see where we might have encountered them before," Swan said.

Detainees' fingerprints and iris scans are checked against databases that contain the biometric identities of bomb builders and terrorists. There have been numerous matches.

Biometric checks have also identified insurgents among the applicants for admission to the Iraqi Police Academy, the Biometrics Task Force reports. They have even turned up Iraqis who have U.S. felony records.

Fingerprints lifted from bomb fragments and ambush sites are added to the database in the hope that some day they will match with prints of suspects in custody.

U.S. troops have ordered Iraqi men, women and children out of their villages and recorded their fingerprints and iris images before letting them return. "It has proven to reduce violence," Swan said. "It keeps the bad guys out."

"The use of biometrics has clearly thwarted security breaches and helped prevent unwanted activities by the enemy," the task force asserts.

#### RISKS FOR ID OWNERS

But as U.S. forces prepare to turn more responsibility over to the Iraqi military, the biometric databases have begun to raise concerns.

"There is precedent for identification systems being used in very bad ways," said Jim Harper, director of information policy studies at the Cato Institute. Identification cards in Rwanda that included photos and listed tribal affiliation were used by rival Tutsis and Hutus to identify their foes.

"They led to killing by machete," Harper said. Similar identification and slaughter "could easily happen in Iraq" if the U.S. military turns its databases over to Iraqis, he said.

The Electronic Privacy Information Center (EPIC) raised the same concern

ADVERTISEMENT

**Microsoft**

Now is the time to advance the mission... and stretch your budget. [LEARN MORE](#)

DEFENSENEWS MEDIA GROUP

MULTIMEDIA

#### Future Combat Systems "Spinout 1"

The Army's Future Combat Systems (FCS) program is ready to test a few components that soldiers may have in their hands by 2010.

[Watch](#)

#### C4ISR JOURNAL

##### Stopping IEDs

arming, training communities step up ...

[Full story](#) | [Related stories](#)

#### ARMED FORCES JOURNAL

##### Saving Afghanistan

Why the Iraq strategy isn't the answer

[Full story](#) | [Related stories](#)

#### TSJ ONLINE

##### Defusing a shifting threat

Counter-IED training is moving target for tech firms

[Full story](#) | [Related stories](#)

~~two years ago in a letter to Defense Secretary Robert Gates.~~

"The massive aggregation of secret files on Iraqis, linked to permanent biometric identifiers, creates an unprecedented human rights risk that could easily be exploited by a future government," EPIC director Marc Rotenberg wrote.

The Army concedes there is potential danger.

In a discussion with bloggers in 2007, Lt. Col. John Velliquette, a biometrics manager in Iraq, acknowledged that a biometric database is "very sensitive because essentially what it becomes is a hit list if it gets in the wrong hands."

"The biometric task force works diligently" to ensure that doesn't happen, a spokeswoman said. "Biometric data and associated biographic information is only shared with authorized users and partners," and it's "a top priority to ensure that such important personal information does not fall into the wrong hands," she said.

Rotenberg has another concern. As databases are compiled, the individuals whose information is stored in them have little or no opportunity to see what has been collected or to correct any errors, he said.

#### THE TOOLS

In Iraq and Afghanistan, biometric data is collected mainly with a Biometrics Automated Toolset (BAT) or a Handheld Interagency Identity Detection Equipment (HIIDE).

The BAT is a four-piece kit that includes a rugged laptop, a separate digital camera for taking photos, a fingerprint reader and an iris scanner.

Photos, fingerprints and iris scans are fed into the computer, where they can be compared against the biometrics of insurgents, terrorists and other wanted persons. The collected data eventually is transferred into a much larger military "biometrics data repository."

The HIIDE is also used to collect and compare fingerprints, iris images, photos and biographical data.

It looks a bit like an oversized digital camera, but has enough memory to store 22,000 "full biometric and biographic portfolios," according to manufacturer L-1 Identity Solutions. A portfolio includes two iris scans, 10 fingerprints, a photograph and 35 items of biographic information.

Troops use the collected biometric data to control access to bases, to screen job applicants, to restrict travel and to aid in forensic investigations, the Biometric Task Force said.

The task force has helped develop other specialized biometric hardware as well.

For the Navy, there's a water-resistant, vibration-hardened "mission-oriented biometric software jump kit" that's used for gathering biometric data on the crew members of ships that U.S. sailors board and inspect.

There are hand geometry readers - "not terribly accurate," but useful in certain situations, Swan said - along with iris scanners that unlock doors only for approved irises, and a high security lock that can be opened only by the correct fingerprint, an access card and a personal identification number.

Development goes on. The task force wants systems that are able to scan irises from a distance. If employed at a base gate, authorized personnel could be scanned and cleared for entry as they drive up. "You wouldn't have to stop," Swan said.

Over the course of a year, the task force has examined about 50 biometric identification systems, including some that identify individuals based on their gait, ear shape, vein patterns in fingers and palms, even by odor, said task force spokesman Greg Johnson.

Once-promising automated facial recognition remains a technology that falls

Services: [Help](#) | [About](#) | [Contact Us](#) | [Site Map](#) | [E-Newsletters](#) | [Current Issue](#) | [Register](#) | [Subscribe](#) | [Renew](#) | [Advertising](#) | [User Agreement](#) | [Privacy Policy](#) | [Terms of Service](#)

short

AP Content © 2009, Army Times Publishing Company

Although the Navy is experimenting with it as a means to keep tabs on prisoners as they move about in the brig in Charleston, S.C., widespread use of facial recognition technology is unlikely anytime soon, Swan said.

Computers cannot yet reliably compare faces captured by cameras with photographs in databases. Poor lighting, images taken from angles and individuals who approach the cameras too quickly all lead to identification errors, she said.

And some biometric technologies are simply considered too intrusive. For example, it is possible to identify individuals based on retina scans, "but we typically don't use the retina," Swan said. "It can tell us things about your health, and that is a privacy concern."

Retina scans can reveal symptoms of diseases ranging from diabetes to cancer. Disclosure of such data could make it harder for people to get jobs or qualify for insurance, Swan said. ■

E-mail: [bmatthews@defensenews.com](mailto:bmatthews@defensenews.com).

**WWW.DEFENSENEWS.COM**  
Available 0800 hrs. - Day of Issue (EST)

