

[Previous post](#)

[Next post](#)

Like 137

1

Share 5

# Your Local Cops Now Use Iraq's Iris Scanners

By [Spencer Ackerman](#) [Email](#) [Author](#)

December 20, 2010 |

10:19 am |

Categories: [Gadgets and Gear](#)

[Follow @attackerman](#)



In Iraq and Afghanistan, U.S. troops use handheld devices to take iris scans and thumb prints off of

detainees and put them in vast databases to distinguish insurgents from civilians. Now your local cops are getting in on the action.

L-1 Identity Solutions, a four-year-old company, makes the [Handheld Interagency Identity Detection System \(HIIDE\)](#), a mobile device that digitally records someone's iris, fingerprint and facial characteristics "to create a comprehensive database on the enrolled subject." The tool, which has [earned high marks in Iraq and Afghanistan](#), is marketed to cops, as a way to avoid taking suspects to booking stations, "where waiting time for results could be anywhere from three hours to three days" for a positive ID on warrant-jumpers.

Military technology has a tendency to trickle down to civilian applications, as evidenced by the fact that you're reading this story on the internet that Darpa helped create. Usually that takes time, but police departments across the country are fielding tools that the military developed to keep tabs on insurgents are now in place to see if you've got any outstanding arrest warrants. That's what the *Washington Post* found for the latest installment of its [series on the expanding surveillance state](#): Arizona's Maricopa County, for instance, keeps a database sized at "9,000 biometric digital mug shots a month."

Here's how the proliferation of biometrics works, as the *Post* discovers. The Department of Homeland Security wants more data points on potential homegrown terrorists. Through Federal-state law enforcement "fusion centers," federal grants help finance law enforcement's acquisition of ID tools like HIIDE, as well as powerful surveillance cameras and sensors. Police incorporate them into their regular law-enforcement duties, picking up information on suspects and using them to cut down on the time it takes to figure out who's evading arrest.

As the military learned, positive identification depends on having a large data set of known insurgents. Cops and the feds are going just as broad. Fingerprint information from crime records gets sent to a FBI datafarm in West Virginia, where they "mingle" with prints from detainees in Iraq, Afghanistan and elsewhere. Military and Homeland Security officials can search through the FBI database for possible connections to terrorists.

It's unclear if there are minimization procedures in place to void someone's fingerprints in the datafarm after a distinct period of time, or how serious a crime has to be to merit a bioscan getting sent to West Virginia. And in many cases, the technology at use here just accelerates the speed at which, say, prints from a police station get sent to the FBI, rather than making the difference between inclusion at the datafarm and remaining at the police station. But it certainly looks like there's not such a lag time between tech developed for a complex insurgency finding applications for crime-fighting at home.

*Photo: U.S. Army*

### **See Also:**

[Army Reveals Afghan Biometric ID Plan; Millions Scanned, Carded by ...](#)

[U.S. Scans Afghan Inmates for Biometric Database](#)

[U.S. Chases Foreign Leaders' DNA, WikiLeaks Shows](#)

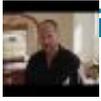
[Detainees Fill Pentagon DNA Databank](#)

[Search Top Secret America's Database of Private Spooks](#)

[You Might Like](#)

[Related Links by Contextly](#)





[Here: Go Behind the Scenes of Flying Lotus' 2001-Inspired Live Show](#)



[Whedon's Viral Video Calls Romney Perfect Leader for Zombie Apocalypse](#)



[X Dragon Splashes Down With Cargo, Including ... Frozen Blood?](#)



[Sale: Laptop With First Presidential E-Mail \(to John Glenn in Orbit\)](#)



[Broadcast Secret Video Feeds](#)

Danger Room senior reporter Spencer Ackerman recently won the [2012 National Magazine Award for Reporting in Digital Media](#).

[Read more by Spencer Ackerman](#)

Follow [@attackerman](#) and [@dangerroom](#) on Twitter.

Tags: [Biometrics](#), [Cops and Robbers](#), [Homeland Security](#), [L-1 Identity Solutions](#), [TIIDE](#)

[Post Comment](#) | [10 Comments and 0 Reactions](#) | [Permalink](#)

[Back to top](#)



[Reddit](#) [Digg](#) [Stumble Upon](#) [Email](#)

Comments for this page are closed.

Sort by popular now

**Showing 10 comments**



**xooloox**

## Two words: Minority Report

The problem is not this one issue (unless they are planning to or implementing scanning people at ordinary traffic stops or storing every scan they take beyond a criminal conviction-- WHICH THEY QUITE LIKELY WILL).

The problem is that it is just one in many issues that constitute a slippery slope on the way to a surveillance police state, which the U.S. is becoming, and already is in some respects. These stories are important because they demonstrate the ways in which the state can (and often does) go beyond their authority, in contempt of the people. They are guilty of insubordination. They are guilty of contempt of the people, who are the sovereign.

"WARNING: The government is armed, and should be considered extremely dangerous."

1 year ago

Like



**daprof**

So it seems that much of the security equipment used in Iraq is now being shipped back to the USA so that big brutha' can use it on their citizens?

And if other countries such as Russia, China, and Pakistan next demand that you have your iris scan to enter their country, could they use your iris code to breach or misuse your identity? I am sure the Russian Mafia will pay big bucks for such valuable information.

What about the factor of Aging irises which may cause problems or whether eye disease such as astigmatisms, cataracts, inflammations could cause iris recognition systems to fail? I bet this consideration has not been well researched by the biometric folks.

And soon you also get your eyes analyzed by the DEA to make sure that you are not smoking any hippie herbs or doing some prescribed medicine without a valid prescription.

It has been well researched that different drugs have unique effects on the pupils which also may soon be used by the police to check for possible illicit drug use while driving your car, bike or simply walking down the street, but is it possible that you are taking some doctor prescribed medication that mimics the same response as some illicit drug and you get to spend time in jail until you can prove your innocence?

I even heard that testing is being done for pupil and drug reactions in the penitentiaries, can

anyone verify this?

The next step will be the insurance companies buying up all your iris scanned images to see if you have any health problems, on certain drugs (pharma and illicit), neurological diseases, syndromes which ponders the possibility of car/health insurance cancellation if you are too high of a risk. Google pupil diagnosis or check out some websites that claim to diagnose pupils from uploaded images from cell phones such as [pupilcheckup.com](http://pupilcheckup.com) that show what various pupil signs can indicate.

So I am having a few drinks waiting for my as usual delayed flight, oops, those five double scotch's may have been too much since my pupils are now very dilated which has changed my iris structure and now refused my flight.

Perhaps the new medications which either constricted or dilated my pupils thus changing my iris and pupil parameters won't allow me on the plane or take out any money from the iris scan atm to pay for my cab home..

If all fails you can always look forward to the new breed of cosmetic surgeons who will allow you to change your iris structure in case you need a new identity... ;)

1 year ago

Like



**Cantankerous**

I wonder how long it will take for these devices to work at range so it would be possible to log everyone walking down a street. Could it be possible to quickly log the identity of everyone that takes part in a demonstration or log the identity of everyone that walks through an airport.

1 year ago

Like



**drake006**

@daveschroeder "Or should they always be crippled so they don't work quite right, or are too slow or ineffective or unwieldy to reliably store and relate ALL of the information that may already be lawfully collected?" No, you are correct Sir, especially since they and the 75 + "Fusion Centers" all work out of immovable buildings that can easily be found on Googel earth ETC. ETC., God Bless America and her great Constitution.

1 year ago

Like

**Freddy**

Crime is at some of the lowest levels it's ever been so I argue that some of this technology potentially could have more detrimental effects on a free, equal and humane society than beneficial effects on crime prevention.

1 year ago

Like

**MingTheMerciless**

@ThisNameTaken: No, Orwell's 1984 was NOT suppose to be an instruction manual. "The Gulag Archipelago" is the instruction manual....

1 year ago

Like

**Shawnm750**

I'm all for protecting people's privacy, but I believe law enforcement should have this type of technology available at the patrolman level. I have to wonder how many truly dangerous criminals are sent on their way because the police don't have the resources to verify their criminal history without hauling to a station. Look at what would happen if they did take a suspect in and they were innocent. People would be upset about their civil liberties being infringed upon, etc. From what I understand, they're not stockpiling fingerprints from everyone they scan, they're just looking for hits in a database. So long as that's the case, I see no problem with it.

1 year ago

Like

**ThisNameTaken**

Orwell's 1984 was NOT suppose to be an instruction manual :(

1 year ago

Like

**jaymoney**

Well Dave, most people who get upset about law enforcement expansion do so because of the consequences that arise for the populace when those in charge abuse their capabilities. No legal construct can guarantee there will be no abuses of said capabilities... just look at the body scanner debacle.

1 year ago

Like



das

The thing that always puzzles me about these stories is that there's this implicit assumption floating in the air that it's somehow "wrong" for law enforcement to use technology to attempt to do its job better or more effectively — and even more wrong if it was developed and/or used by the military.

Why?

The Internet was developed in part by our nation's military apparatus; should law enforcement be enjoined from using it? There is all manner of technology that make the job of law enforcement easier: cameras, telephones, vehicles, computers, databases, wireless communications, binoculars, links to other law enforcement agencies, etc...should those be restricted?

It seems that these arguments are predicated on some sort of assumption that law enforcement should always be hindered. Mind you, I'm not talking about proper Constitutional limits here: I'm talking about the notion that even lawful expansion or enhancement of law enforcement capabilities is somehow "wrong". If a police officer may legally identify a person and store information on an arrest, what is wrong with attempting to ascertain and store that information more reliably (e.g., with biometric identification? If it is already appropriate to share information with federal entities, what is wrong with streamlining and automating those processes (e.g., via federated databases)?

Or should they always be crippled so they don't work quite right, or are too slow or ineffective or unwieldy to reliably store and relate ALL of the information that may already be lawfully collected? The power of aggregating information is not lost on me, nor is the potential for abuse of such databases. But if it's aggregation and/or abuse we wish to prevent, would it not be better to establish legal constructs in those areas, instead of handwringing that some technology that happens to have a military application also has a civilian application?

1 year ago

Like

 [Subscribe by email](#)  [RSS](#)

---