



ALJAZEERA.NET

Mobile biometrics to hit US streets

Despite fuzzy legality, US law enforcement will soon be able to perform mobile iris scans and fingerprinting.

D. Parvaz Last Modified: 02 Aug 2011 16:25



With new mobile gadgetry, suspects will no longer have to be taken to police stations for their fingerprints and irises to be scanned and recorded [GALLO/GETTY]

We're fast approaching a time when law enforcement will no longer need to ask you for your identification - your physical self, and the biometric data therein, are all that will be required to identify you.

A gadget attached to a mobile phone can photograph and plot key points and features on your face (breaking the numbers down into biometric data), scan your iris and take your fingerprints on the spot.

This gizmo doesn't exist in a futuristic world - it's already been prototyped and tested. By autumn, the Mobile Offender Recognition and Information System (MORIS), which will allow 40 law enforcement agencies across the US to carry out such biometric diagnostics, will be rolled out. So far, the 1,000 units on order - at \$3,000 and 12.5 oz per device - will be going to sheriff and police departments.

Proponents of the technology figure the deployment is a plus - having biometric data available almost instantly might prevent an officer from mistakenly identifying someone (via, say, a driver's license, which could be forged) and

unnecessarily hauling them in for processing.

Scans taken on the road are checked against a database of stored scans from those who have in the past been or are currently incarcerated. Essentially, the idea is to see if a suspect has a prior record.

It's accurate. It'll keep us safe. It'll help law enforcement do its job.

But given that two of the three functions of the MORIS could legally be considered to be the sort of "search and seizure" covered by the US Constitution's Fourth Amendment (meaning that a person could, in theory, decline to have their iris scanned or fingerprints taken), law enforcement's ability to use them as intended seems questionable.

"The collection of personal biometric data has many privacy and civil liberties concerns attached to it, including scalability, reliability, accuracy, and security of the data collected," said Amie Stepanovich, national security counsel for the Electronic Privacy Information Center (EPIC), a Washington DC-based public interest group focused on privacy and civil liberty issues.

A key concern, said Stepanovich, is that this technology was essentially developed for a military environment and not for domestic use.

"The potential of this technology for use to track and monitor innocent individuals' personal information cannot be overshadowed. To prevent misuse, warrant requirements must be strictly enforced."

Looming legal questions

Does this gadgetry provide Americans with greater protection or does it allow the state - or unscrupulous law enforcement officials - to take advantage of loopholes left by laws and a Constitution drafted in a more technologically simple age?

While Sean Mullin, the president of the Massachusetts-based BI2, the maker of the **MORIS device**, said that the constitutional issues surrounding such mobile search devices "have already been addressed" by the courts. He told Al Jazeera that he did not anticipate any problems with the technology, though he did submit that policy issues connected with the use of the device would have to be determined by lawmakers.

"This technology, though remarkable, does not change 200 years of constitutional law in the United States," said Mullin.

Legally speaking, there are grey areas when it comes to if and how road-side iris scans and fingerprinting can be carried out by law enforcement.

The Fourth Amendment in the US Constitution offers protection against "unreasonable" searches - this typically includes fingerprints.

But where does an iris scan fit in?

"An iris scan is almost certainly a 'search' within the meaning of the Fourth Amendment's protection against unreasonable searches and seizures. The closest analogy is of course a fingerprint," said Laurence Tribe, professor of constitutional law at Harvard Law School.

Tribe said that even the ways in which an iris scan could be distinguished from fingerprints - it is newer technology that does not require physical contact with the suspect - weren't constitutionally relevant, as using an iris scan would still be used to "provide accurate non-public information about the person's true identity" while obtaining "information that is not as accurately obtainable by mere observation of what an individual chooses to expose to the world at large".

EPIC's Stepanovich also says that certain constitutional protections are attached to the process of being taken into police custody, and that law enforcement ought not be able to bypass those protections by carrying out searches outside of the police station.

"Law enforcement officials must be clear with an individual about what they are consenting to - by performing these searches, which have historically been executed only at a police station, outside of police custody, many people may not be made aware of the scope of the search or their right to refuse. Well-accepted constitutional safeguards must be preserved," she said - adding that while a person can waive his or her Fourth Amendment rights, "it may be unclear to the individual what he or she is consenting to".

Expanded use

Mullin said that while, so far only sheriff and police departments have placed orders with BI2, there "has been a great deal of interest from the federal government, including the Department of Homeland Security".

The Department of Homeland Security did not respond to requests for an interview or for information on whether it had ordered any of the mobile biometric units, although Animetrics, the company selling facial recognition software (which can be used on the mobile device) promotes its products as being highly useful not only for police departments, but for the DHS - as well private security firms.

Paul Schuepp, president the New Hampshire-based Animetrics, readily acknowledges that private security firms, the US defence department and various local law enforcement agencies have purchased the facial recognition software, but remained tight-lipped when questioned specifically on whether the DHS or contractors such as Xe (formerly known as Blackwater) have ordered any of the handheld devices.

"That's a difficult one to answer ... those are the ones that I can't even talk about - there's high interest from intelligence agencies, which is all of the above," said Schuepp.

The company has a number of facial recognition **products** on the market - everything from a free phone app that allows people to see which celebrity they resemble the most (Schuepp says his own facial biometrics resemble those of Kevin Costner and George Clooney) to software currently being tested in Iraq and Afghanistan, where Schuepp says he hopes his company will score lucrative contracts.

As with the the iris scan, Animetrics' mobile applications would not store the biometric data of a person who is not already logged in some sort of penal system database.

While Mullin said private companies would not have access to the iris database, it's worth noting facial recognition is employed by private companies, who, Schuepp said, might want to keep a "white list" of those who ought to have access to their facilities and "black list" of those they'd like to keep out.

When it comes to his own moral position as a developer, putting technology that could be misused into the hands of the government and private sectors alike, Schuepp said he had faith in the system.

"I'm counting on our government being honest, whether it's law enforcement or the military, trying to find people who threaten our lives," he said.

Mullin, too, takes a pretty easy moral position on his company's product.

He said the only significant difference between the MORIS and what already exists is its "miniaturisation".

Still, Mullin acknowledged that there's nothing to stop an individual officer from misusing the device - coercing a suspect into submitting to a scan, for example - but said the device itself can only be used by authorised personnel, with five layers of verification and security to prevent "just anyone" from being able to access the iris database.

Indeed, the Pinal County Sheriff's Department is among the agencies that has ordered the handheld devices. Given that Arizona last year passed the most stringent **immigration law** in the country - one President Barack Obama said "threatened to undermine basic notions of fairness" - it seems worth examining how these devices might be used in



Massachusetts Plymouth County Sheriff's Department participated in BI2's promotional video [Youtube]

different jurisdictions.

The Pinal County Sheriff's department did not respond to numerous requests for an interview on its guidelines for using the device.

Constitutional watchdogs, as well as civil liberties groups such as the American Civil Liberties Union, have long had **issues** with the use of biometric data, even when collected at international borders, fearing that the data could be misused.

"There is a greater risk of abuse with greater technological functionality, including unconstitutional targeting of persons in specific religious clothing or attending controversial events, or instances where the technology is used to [further] the personal ends of a law enforcement officer," said Stepanovich.

"Wide spread data collection often turns up a few cases of people who may or may not be guilty of criminal activity, but if that is done at the cost of frequent surveillance of the general public then it is not in line with constitutional principles."

Building a biometric arsenal

We are living in the surveillance age. Google Street View vans roam our streets, mobile phone companies track our movements and most are even being watched by our social network, with Facebook allowing third parties to use facial recognition software to tag users without their consent.

This "Tag Suggestion" feature has attracted some negative attention, and at the behest of the Connecticut office of the attorney general, the social networking site earlier this month **agreed** to run adverts on its pages, informing users on how to opt-out of the tagging feature.

The uproar surrounding Facebook's facial recognition feature might be what has prompted Google to hold back on its facial recognition tool, although the company did not respond to a request for an interview.

But a type of biometric census has been in wide use by US and NATO forces, which have been using registering to millions of Afghans and Iraqis in their own countries for some time. It's not only the **criminals** who are processed and entered in these databases - it's **entire populations**, although the focus seems to be on males of "fighting age".

The New York Times recently reported that one in every 20 residents of Afghanistan has been registered in the massive biometric database. In Iraq, one every 14 have been entered.

Within the US, the database of iris scans and facial data is expanding too.

"In the fourth quarter of 2010 the system performed 3.2 billion – that's *billion*, with a 'b' - successful cross matches with one false accept [a false positive match]," said Mullin, of the iris database which is already employed in 47 states (the exceptions being Alaska, Hawaii and Delaware), although not in every jurisdiction in each state.

"The size of the database is growing very rapidly," said Mullin, who also said that the iris scanners are incredibly accurate and have a minute rate of "false accepts" - mistakenly matching an iris scan with one already in the database.

But not everyone is convinced of the accuracy of biometrics - a wide field that includes everything from voice and gait recognition to iris scans - as a whole.



The military has used different versions of iris and facial scanners in Afghanistan and Iraq for years [Reuters]

A 2010 **study** done by the National Academy of Sciences found that technologies behind biometric data gathering are "inherently fallible". "The scientific basis of biometrics - from understanding the distributions of biometric traits within given populations to how humans interact with biometric systems - needs strengthening particularly as biometric

technologies and systems are deployed in systems of national importance."

The study also highlighted that a subject might feel coerced into submitting to a scan due to "the possibility of negative consequences for nonparticipation", while instinctively wanting avoid a scan fearing "mission creep" - meaning that their data could be used for something other than the stated purpose.

Indeed, the notion of implied consent is where it gets sticky.

Tribe said that even within the context of what is considered a lawful **stop and frisk** that probable cause and a search warrant might still be required in order to compel someone to submit to an iris scan.

Scan first, apologise later?

The US isn't unique in it's use of on-the-go fingerprinting - UK police are also using mobile fingerprinting application, despite **objections** from civil and immigrations rights groups.

Still, use of such data continues to grow in the US.

Massachusetts, for example, was already using facial recognition software, and according to James Walsh, the executive director of the Massachusetts Sheriff's Department, the state is looking to expand its database with a recent \$250,000 grant from the US justice department.

Walsh was quick to point out that the grant did not include any MORIS units and that individual sheriff's departments in Massachusetts may have, independently, ordered some of the devices - but said he could not be sure.

They have.

John Birtwell, the director of public information and technology at the Plymouth County Sheriff's Department told Al Jazeera that the county will get "more than a handful ... at least three" of the devices.

But that's just about all the certainty Birtwell had to offer on the topic, as he seemed unclear as to whether officers would inform suspects of their Fourth Amendment rights to refuse to undergo impromptu fingerprinting and iris scanning.

He also seemed unsure as to what the protocol would be in the even that a suspect declined to be processed in such a manner.

"I'm dancing on the head of a pin here because I'm not a constitutional scholar," said Birtwell.

"The first or second time these devices are used, there would be some sort of appropriate constitutional test to make those bright lines [guidelines for field use] clear," said Birtwell, who said officers would be issued guidelines on when and how they could legally use the devices. He just wasn't sure when that would be - or what those guidelines would look like.

"All of these questions involve constitutional issues and protections and they should be addressed ... nobody wants to make a bad arrest, nobody wants to violate anybody's rights."

Follow D. Parvaz on Twitter: @DParvaz

Source: Al Jazeera