Report questions biometric technologies

October 5 2010, By Dan Vergano

Television cop shows love "biometric" technologies -- fingerprints, eye scans and so on -- but a blue-ribbon panel report calls for caution on widespread use of biological identification.

Released by the National Research Council, the "Biometric Recognition: Challenges and Opportunities" report, headed by HP Labs distinguished technologist Joseph Pato, concludes all biometric recognition technologies are "inherently fallible."

"A lot of things possible on a TV series just don't work that way in real life," says panel member Bob Blakley of Gartner, a computer security firm in Stamford, Conn. "While there are lots of good uses for biometric recognition, there are lots of ways to create systems that waste time, cost too much and don't work very well."

Fingerprints are the best-known example of biometric recognition markers -- physical traits that can serve to identify people reliably, such as facial features, voice, signature and even walk.

"Biometric recognition has been applied to identification of criminals, patient tracking in medical informatics and the personalization of social services, among other things," notes the report, released Sept. 24.

Federal agencies such as the FBI and the Department of Homeland Security are funding research in improved biometric screening, but the report cautions they're not doing basic research into whether the physical characteristics involved are truly reliable or how they change with aging,

disease, stress or other factors. None look stable across all situations, the report says.

Deployment of biometric screening devices at airports, borders or elsewhere without understanding the biology or the population being screened will lead to long lines, false positives and missed opportunities to catch criminals or terrorists, the report says.

"No system is infallible. There is no silver bullet," says Marc Rotenberg of the Electronic Privacy Information Center in Washington, D.C. "We have to test our security strategies carefully, or there will be a lot of taxpayer money wasted on systems that disappoint us."

Brandon Mayfield, a 44-year-old attorney from Oregon, is an example of the problem. A partial fingerprint from the 2004 Madrid subway bombing that killed 191 people was said by the FBI to match Mayfield's, which led to his arrest.

A judge later found the fingerprint match was only a slight one and for the wrong finger, ordering Mayfield released. The FBI apologized for the arrest, and Mayfield won $2 million in damages.

The FBI's nationwide fingerprint system has generally worked very well, leading to the arrests of fugitives, the report says. "But the key message is that even a very accurate technology can yield bad results if it is turned to the wrong problem," Blakley says, such as using time-consuming technologies to screen large numbers of people.

For that reason, the report calls for open and independent testing of biometric screening technologies before they are placed into widespread use. Cultural factors such as how long people are willing to wait in line for screening, as much as raw accuracy, will determine whether a particular kind of biometric recognition system will work.

"Too many false positives, and guards will just stop believing in the system and let the wrong people through," Blakley says.