GlobalResearch
Center for Research on Globalization

Canadian think-tank sees danger in cross-border biometrics

Walsingham Institute discusses 'reactionary' moves by U.S

By Nestor Arellano
Global Research, May 18, 2007
itbusiness.ca 18 May 2007

Region: Canada
Theme: Police State & Civil Rights

Reports that face and fingerprint matching scanners are being left unused by U.S. frontier guards prove biometric technology is not appropriate for securing high-traffic environments according to a Canadian security analyst.

American officials acted rashly in deploying biometric technology right after the 9/11 attack, and Canadians are in danger of taking the same route said Alicia Wanless, director of the Walsingham Institute, an independent Toronto-based security think-tank.

“Implementation of biometrics at border crossings was reactionary at best,” said Wanless.

Shortly after the attack on the World Trade Centre in New York on Sept. 11, 2001, the American government went into high gear commissioning security equipment for the country’s entry points.

Biometric-based systems were touted as a sophisticated means of thwarting illegal entry into the U.S.

Biometric authentication uses technology to measure physical characteristics of a person’s face, fingers, hands, eyes or voice as a means of confirming identity.

A recent newswire report, however, revealed biometric scanners deployed at the U.S.-Mexican border are almost never used, because to do so would generate a huge backup in an area known for traffic jams that last for hours.

The report said the U.S. government spent “tens of millions of dollars” on issuing some 9.1 million visa cards to Mexican visitors that were embedded with the holder’s photo and fingerprint, but only about two per cent of the card holders are subjected to biometric screening.

The “laser visas” have an optical memory stripe that contains the personal identification information, a digitized photo and two fingerprints of the holder.

Cardholders crossing the border may be asked to press their finger against a lens and pose for a photo, while border inspectors swipe the visa through a machine to call up the holder’s personal data and photo.

The photo and fingerprints are automatically checked against a watch list for terrorist and

criminals. The process takes approximately 30 seconds per person.

Members of Congress who voted for the system in 1996 said the original intention was to use biometric screening for all entrants, according to the report.

Wanless said the deployment was done without adequate planning, and the negative press the U.S. government is getting over the implementation is giving biometric technology a "bad name."

However, she said the technology is good, if used in the right way.

According to the security expert, devices currently available are designed for scanning only a limited number of people and not the volumes normally encountered at border crossings or airports.

Ideally, biometric scanners should be employed in offices and government buildings.

"Authorities are using biometrics as they would a border guard – to determine a person's identity based on the documents he or she carries and information the system has in its database."

Canada, Wanless said, is deploying similar systems aimed at speeding security checks.

More than 5,000 people have signed up for the Nexus Air Card, which allows quick access to U.S.-bound flights through the Vancouver International Airport. The joint project of the U.S.-Canada immigration departments, employ cards that contain a digitized image of the holder's eye.

A kiosk-based machine scans the person's iris and matches it with what is contained in the database.

The iris scan is stored jointly by U.S. and Canadian authorities. The service is open to American and Canadian citizens with at least three years of permanent residency.

Toronto's Lester B. Pearson International Airport recently introduced the Clear Card program.

The card holds fingerprint and iris scan images, but the concept is similar to that of the Nexus program. The card was developed by Verified Identity Pass Inc. of Palm Coast, Florida.

Most biometric authentication methods, however, are flawed according to Wanless. "These fast-track kiosks and scanners run the risk of creating security breaches themselves."

For instance, she said facial recognition devices are notorious for high error rates since the technology is not yet at a level where it is able to give accurate readings.

Most operators are also not adequately trained to handle situations arising from false positive scans, she added.

The two biggest drawbacks of biometric devices, according to Wanless, are the "fluid nature of identity" and the technology's "failure to detect intent."

She said there are a multitude of ways available for a determined person to create or obtain

false personal information and documents.

The information can be easily slipped into government databases to thwart biometric scanning devices. “The ability to authenticate identity to an irrefutable degree is non-existent.”

Despite years of development, technology can not determine a person’s intentions, according to Wanless. “A machine can’t tell you if a person passing through airport security intends to blow up a building two weeks from now.”

“We still need properly trained border guards and security personnel who can detect subtle hints in body movements or speech that might betray possible harmful intent.”

Instead of spending millions of dollars in biometrics, Wanless advices that governments give more attention to improving border guard training, upgrade databases, as well as enhance information gathering and sharing.

Articles by: Nestor Arellano