INTERNATIONAL
BIOMETRICS & IDENTIFICATION
ASSOCIATION

Biometric Identity Assurance for School Children: Enhancing child security, safety and privacy

Overview

In today's world, virtually everything is dependent on knowing with a high degree of assurance 'who' we are dealing with. This is especially the case in our schools where children, our most vulnerable population, spend most of their days. For many critical purposes – foremost, the security, safety, and privacy of our children and also the productivity and the efficiency of our schools – we need to identify with a high degree of assurance 'who' is entering our schools, using school facilities, attending classes, eating school lunches.

At its simplest, biometric identification is the purest and most non-discriminatory form of personal identification. It is based on an individual's unique physical attributes. For this reason, it is the only way to positively identify an individual. The result is enhanced security and safety, school productivity and efficiency, and student privacy.

Other means of identification – cards, PINS, passwords, visual inspection of students – are ineffective for obvious reasons. Cards can be lost, or stolen, or shared; ID numbers and passwords are easily forgotten, especially for younger students, or shared. As for relying on visually looking at students, no one can remember all the students that come and go in a school.

School uses of biometric identification

- School cafeterias. Its use increases speed and efficiency so that students have enough time to eat; curtails bullying and theft of lunch money; protects the privacy of students on free or reduced cost government lunch programs; and ensures auditable and accurate record keeping for reimbursement from the federal government's $13 billion food programs.
- School security. Its use at school entrances can ensure that those entering the schools belong there; can match authorized parents or guardians with children to prevent kidnapping; and can ensure that children board the correct buses and get off at their correct stops.
- School efficiency. Its use facilitates accurate recordkeeping and compliance with federal requirements, thus saving administrative time to be dedicated to the students.

Biometric use is not a privacy threat; it enhances privacy

- The data that needs the most protection is one's biographic data – name, address, date of birth, sex, social security number etc. – not biometrics. In all of the highly publicized thefts of identity, the data that were used were biographic and NOT biometric.
- Biometric data is already protected. In the difficult and unlikely case that a person hacks a biometric database, all the hacker receives is the digital representation of the biometric (a string of ones and zeros). This digital representation does not provide access either to the biometric image or the biographic data, contrary to hacking into a database of personal biographic data.
- As a best practice to protect student privacy, IBIA recommends storing only the biometric templates, which should be deleted when a student leaves the school. Student privacy is further enhanced because templates CANNOT be used to search law enforcement biometric databases.