Biometrics - FAQs

Digital Fingerscans in Schools

In this world of ever increasing scrutiny from government and corporations, people are quite justified in having misgivings when new technologies emerge to help in the identification of the individual. Biometrics have been in the news for the last few years and many concerns have arisen over the rights of privacy and how organisations can use and abuse this information. Many people see any new technological advance in identification as another step towards the loss of the individual's privacy and freedom.

Every day we leave a trail of highly personal information as we go about our normal tasks. We leave fingerprints on everything we touch from door handles to a glass at the dinner table. We leave DNA from hair and saliva. Our images, time and location are recorded on hundreds of thousands of CCTV cameras up and down the country. Our cars are tracked by number plate and we are happy to leave our signature (the main source of identification for the last hundred years) on anything from delivery notes to Christmas cards. Our location can be tracked from our mobile phones, our emails can be intercepted, our web browsing styles analysed. Banks and shops know where we have been and what we have bought by tracking our credit card transactions. Even what we throw out can provide a rich array of information.

In contrast the controlled, confidential and secure environment in schools is ideal for hosting Biometric technologies without the concerns of privacy we battle with in our every day lives. The following questions and answers may help to dispel some of the myths and misinformation surrounding fingerscan systems used within schools.

Is my fingerprint stored in a database?
No, the image of an individual's fingerscan is never stored in a database or computer file. The image of the fingerprint is transferred from the fingerprint scanner into the computer via an encrypted data path. Feature extraction is then performed where unique points such as where ridges end or change direction are identified and their locations recorded. These form the feature template which is stored in the database for later comparison. Only the template is stored in the database. The number of unique features stored for each fingerprint can vary from ten to as many as forty depending on the complexity and quality of the fingerprint. It is impossible from this stored representation to recreate the original fingerprint image as virtually all the original information has been discarded during the template extraction phase.

Could the police use this stored information to identify and prosecute someone?
The amount of information retained is sufficient to identify an individual from a database of a few hundred or a few thousand using a special algorithm but is totally inadequate for forensic use and could not be used in a court of law to prove identity. The standards for forensic matching are very much higher and require the original fingerprint image.

If the government decided to create a national database of fingerprints is it technically possible for them to take this data from all the schools?
The system works exceptionally well when dealing with small groups of people from a few hundred to a few thousand. During enrolment a new template is created and compared against those already in the database. This is a controlled environment and only enough detail is stored to

distinguish this group of people from each other. There is not enough information stored about the characteristics of the fingerscan to scale this up to a national database.

When my child leaves the school how can I be certain their fingerscan data is removed?
Only one copy of the template is stored in the database and when the individual is deleted from the system the template is completely obliterated.

How do I know the school will keep my child's fingerscan data safe and confidential?
All the fingerscan data captured is the property of the school and is only stored on a computer within the school. Biometric data is classified as personal information under the data protection act and therefore must be treated in exactly the same way as other personal data. Schools already have systems and procedures in place to protect the significant personal information they hold on their pupils. In this controlled environment the security and privacy of an individual can be assured.

How is the treatment of this data affected by the Data Protection Act ?
Biometric data is personal data within the definition of the Data Protection Act, so the BioStore database is treated with the same care as any other personal data recorded by the school so as to conform to the data protection legislation.